FIG. 1

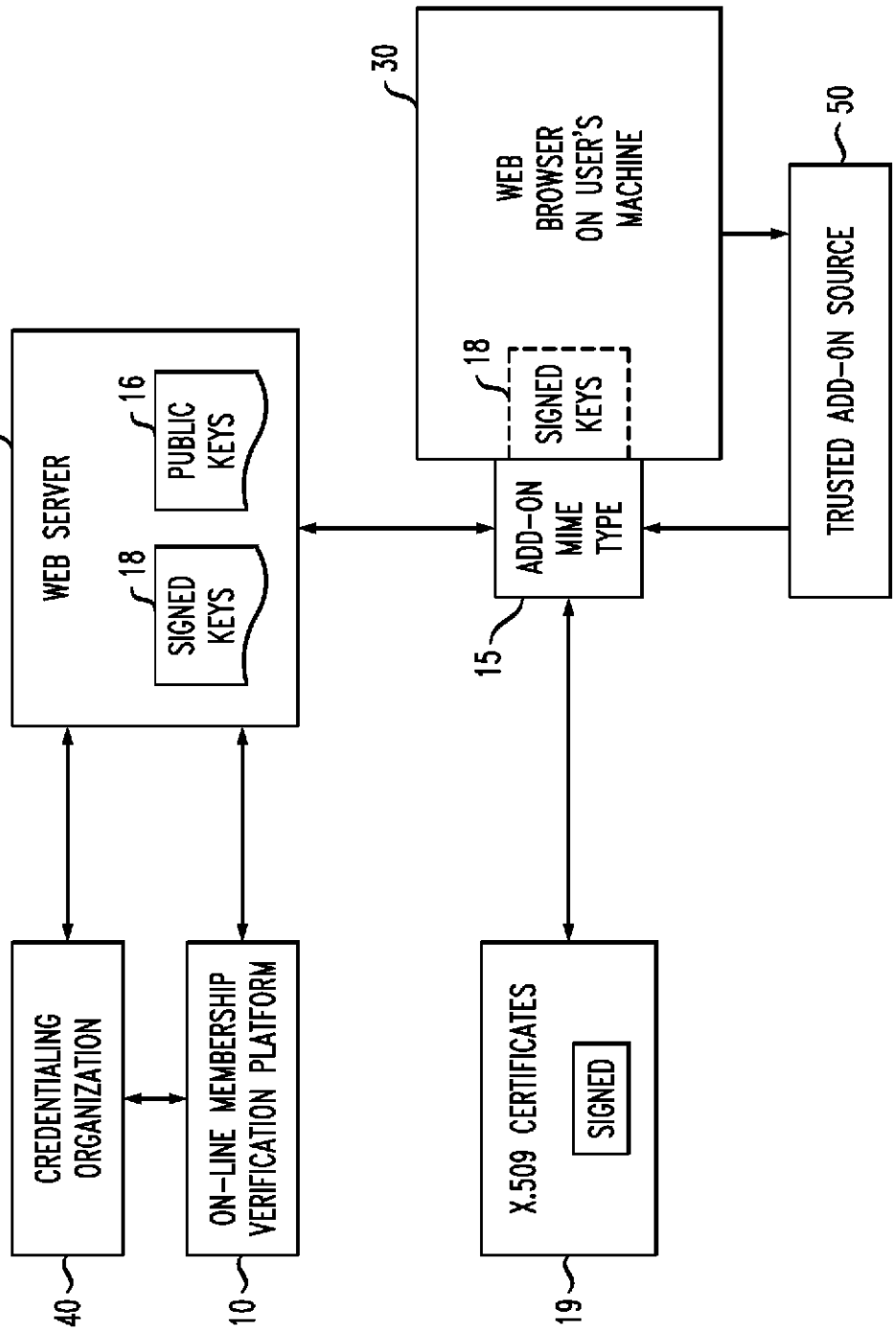

WEB SERVER
20
PUBLIC KEYS
16
SIGNED KEYS
18
WEB BROWSER ON USER'S MACHINE
30
SIGNED KEYS
18
ADD-ON MIME TYPE
15
TRUSTED ADD-ON SOURCE
50
CREDENTIALING ORGANIZATION
40
ON-LINE MEMBERSHIP VERIFICATION PLATFORM
10
X.509 CERTIFICATES
SIGNED
19

FIG. 2

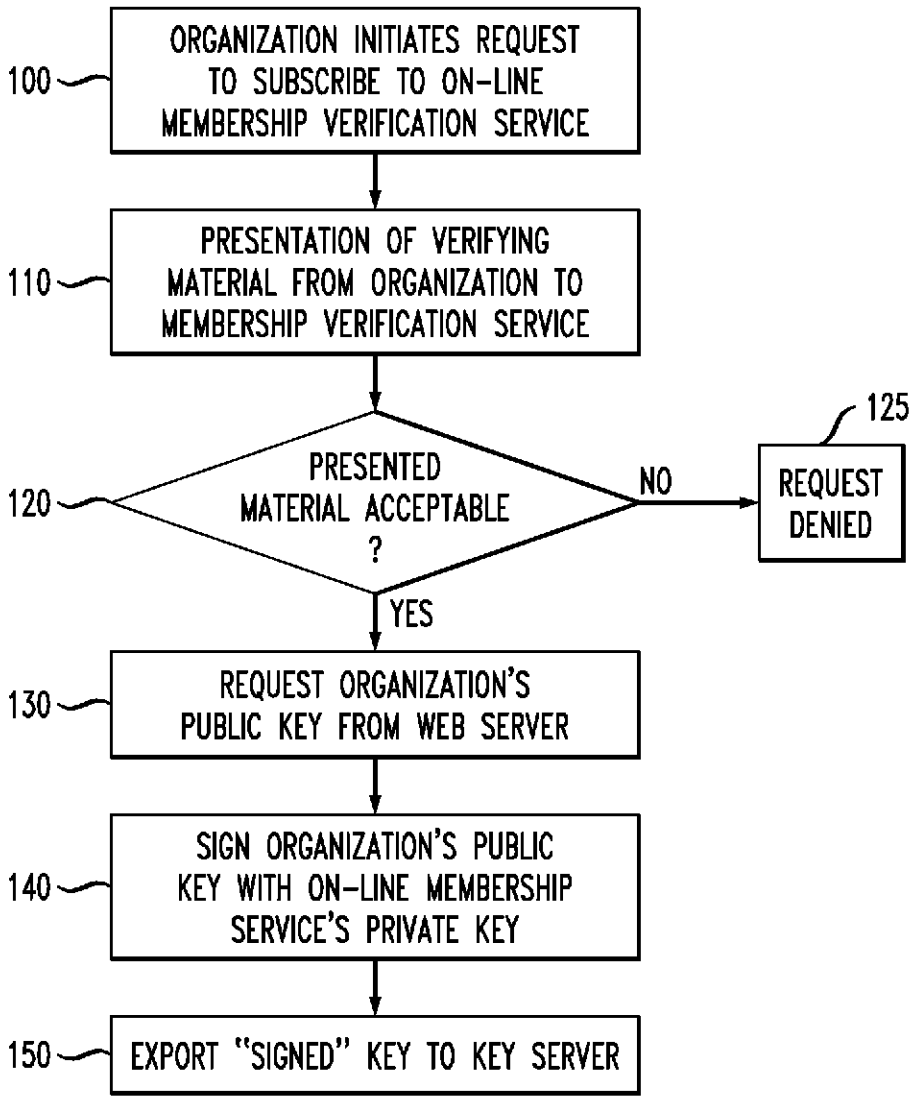

ORGANIZATION INITIATES REQUEST TO SUBSCRIBE TO ON-LINE MEMBERSHIP VERIFICATION SERVICE
100
PRESENTATION OF VERIFYING MATERIAL FROM ORGANIZATION TO MEMBERSHIP VERIFICATION SERVICE
110
PRESENTED MATERIAL ACCEPTABLE ?
120
NO
125
REQUEST DENIED
YES
REQUEST ORGANIZATION'S PUBLIC KEY FROM WEB SERVER
130
SIGN ORGANIZATION'S PUBLIC KEY WITH ON-LINE MEMBERSHIP SERVICE'S PRIVATE KEY
140
EXPORT "SIGNED" KEY TO KEY SERVER
150

FIG. 3

16

```
pub   1024D/0AD456D8 2008-08-01 [expires: 2012-07-31]
uid   Yale University (No comment) <admin@yale.edu>
sub   2048g/7DADADEB 2008-08-01 [expires: 2012-07-31]
```

FIG. 4

17

```
sec   1024D/46184333 2008-08-01 [expires: 2012-07-31]
uid   Online Membership Inc. (Basic registration address) <registrar@onlinemembership.com>
sub   2048g/95AA43B0 2008-08-01
```

FIG. 5

18

```
pub   1024D/0AD456D8 2008-08-01 [expires: 2012-07-31]
uid   Yale University (No comment) <admin@yale.edu>
sig 3 0AD456D8 2008-08-01 Yale University (No comment) <admin@yale.edu>
sig   46184333 2008-08-01 Online Membership Inc. (Basic registration address)
        <registrar@onlinemembership.com>
sub   2048g/7DADADEB 2008-08-01 [expires: 2012-07-31]
sig   0AD456D8 2008-08-01 Yale University (No comment) <admin@yale.edu>
```

FIG. 6

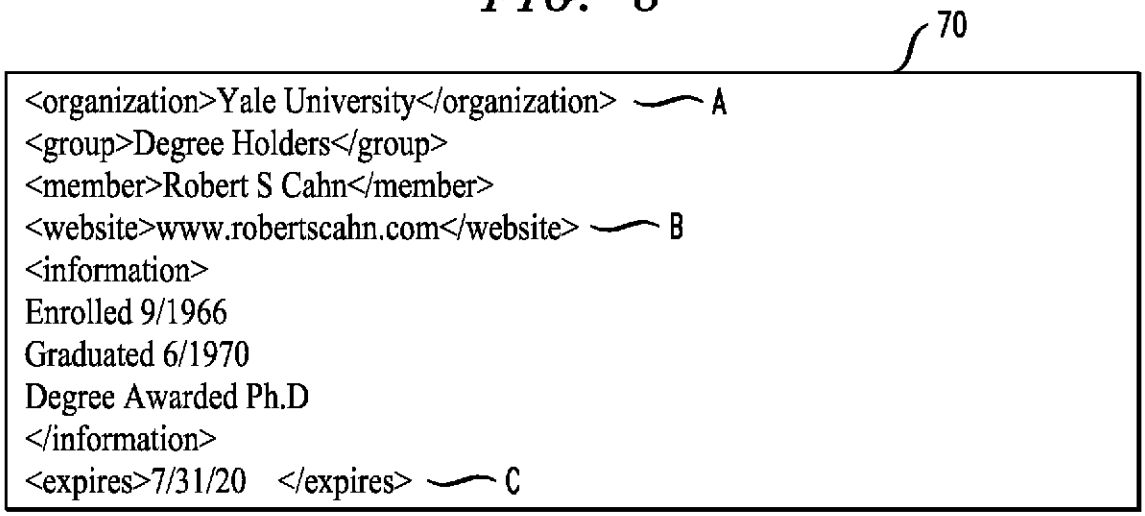

70
<organization>Yale University</organization> A
<group>Degree Holders</group>
<member>Robert S Cahn</member>
<website>www.robertscahn.com</website> B
<information>
Enrolled 9/1966
Graduated 6/1970
Degree Awarded Ph.D
</information>
<expires>7/31/20 </expires> C

FIG. 7

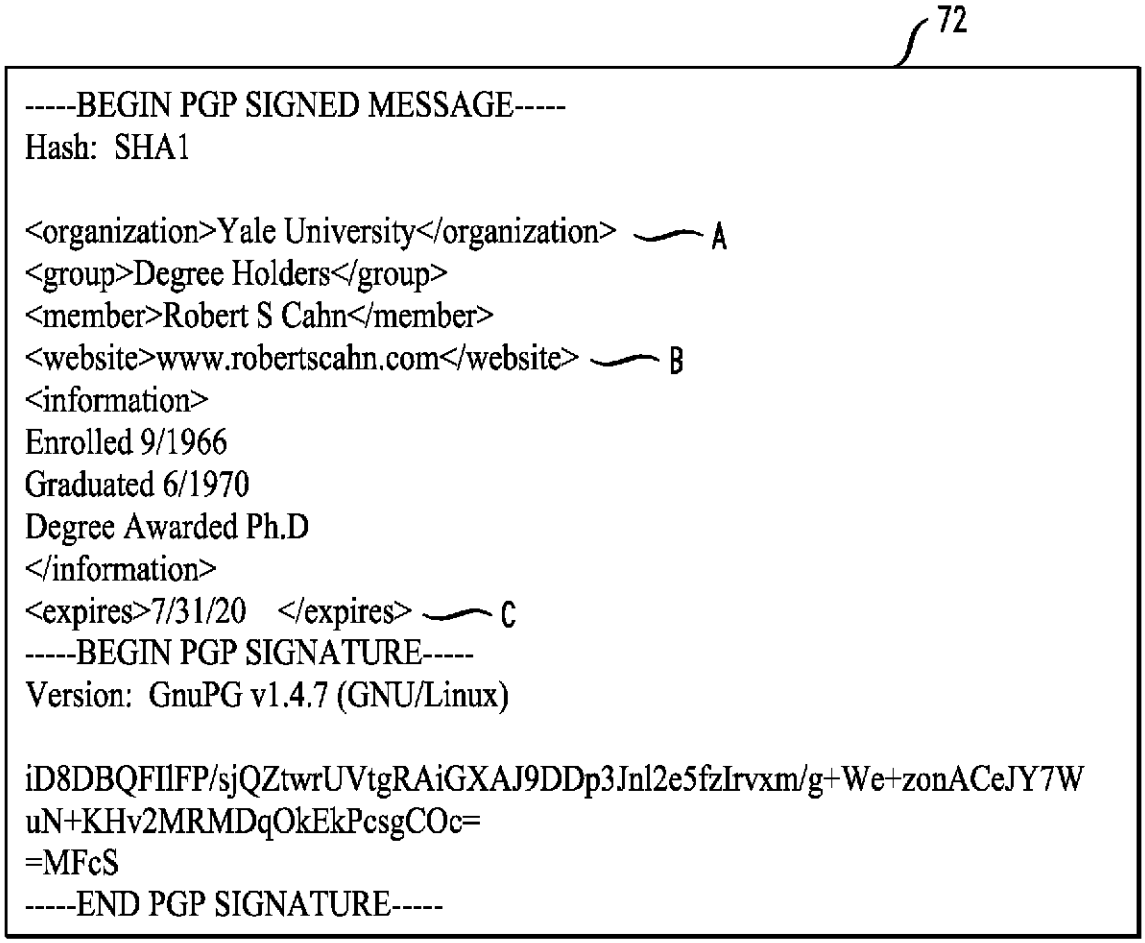

72
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
<organization>Yale University</organization> A
<group>Degree Holders</group>
<member>Robert S Cahn</member>
<website>www.robertscahn.com</website> B
<information>
Enrolled 9/1966
Graduated 6/1970
Degree Awarded Ph.D
</information>
<expires>7/31/20 </expires> C
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.7 (GNU/Linux)
iD8DBQFIlFP/sjQZtwrUVtgRAiGXAJ9DDp3Jnl2e5fzIrvxm/g+We+zonACeJY7W
uN+KHv2MRMDqOkEkPcsgCOc=
=MFcS
-----END PGP SIGNATURE-----

FIG. 8

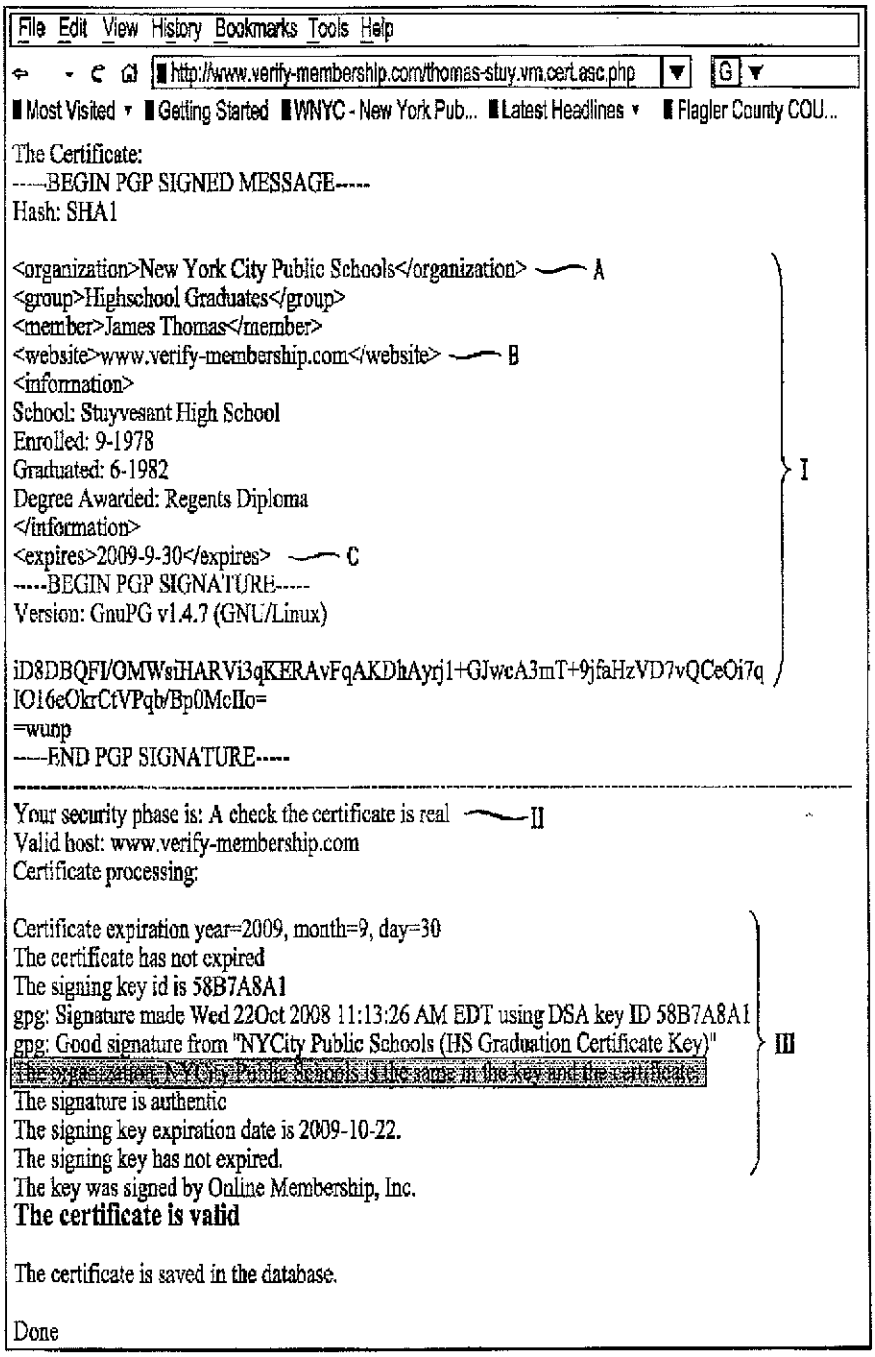

File Edit View History Bookmarks Tools Help
http://www.verify-membership.com/thomas-stuy.vm.cert.asc.php
Most Visited
Getting Started
WNYC - New York Pub...
Latest Headlines
Flagler County COU...
The Certificate:
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
<organization>New York City Public Schools</organization>
A
<group>Highschool Graduates</group>
<member>James Thomas</member>
<website>www.verify-membership.com</website>
B
<information>
School: Stuyvesant High School
Enrolled: 9-1978
Graduated: 6-1982
Degree Awarded: Regents Diploma
</information>
<expires>2009-9-30</expires>
C
I
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.7 (GNU/Linux)
iD8DBQFI/OMWsiHARVi3qKERAvFqAKDhAyrj1+GJwcA3mT+9jfaHzVD7vQCeOi7q
IO16eOkrCtVPqb/Bp0McIIo=
=wunp
-----END PGP SIGNATURE-----
Your security phase is: A check the certificate is real
II
Valid host: www.verify-membership.com
Certificate processing:
Certificate expiration year=2009, month=9, day=30
The certificate has not expired
The signing key id is 58B7A8A1
gpg: Signature made Wed 22Oct 2008 11:13:26 AM EDT using DSA key ID 58B7A8A1
gpg: Good signature from "NYCity Public Schools (HS Graduation Certificate Key)"
The organization NYCity Public Schools is the same in the key and the certificate
The signature is authentic
The signing key expiration date is 2009-10-22.
The signing key has not expired.
The key was signed by Online Membership, Inc.
III
The certificate is valid
The certificate is saved in the database.
Done

FIG. 9

App Path	/home/bob/mcstore
Sec Phrase	This certificate is real Bob
Sec Color	blue

FIG. 10

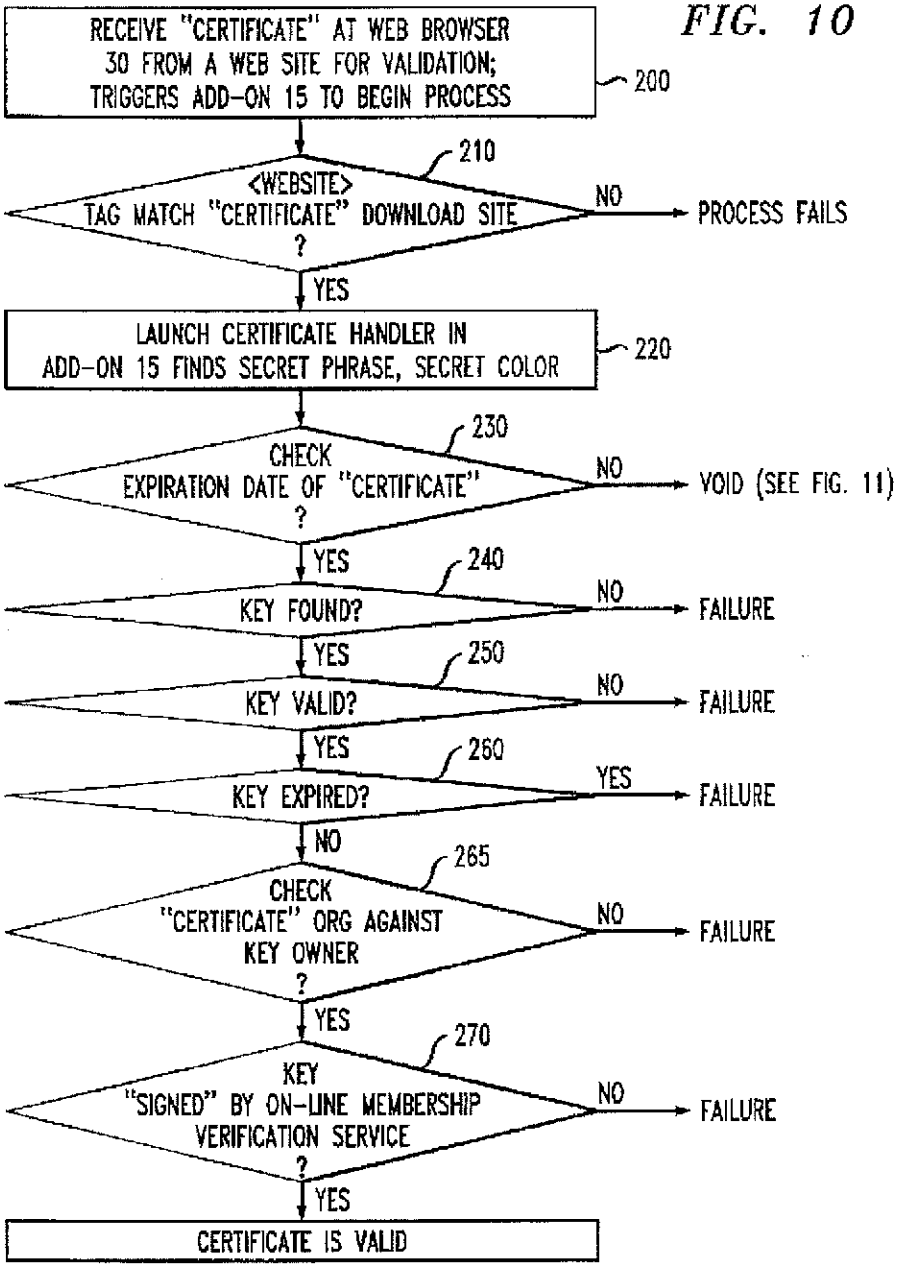


FIG. 11

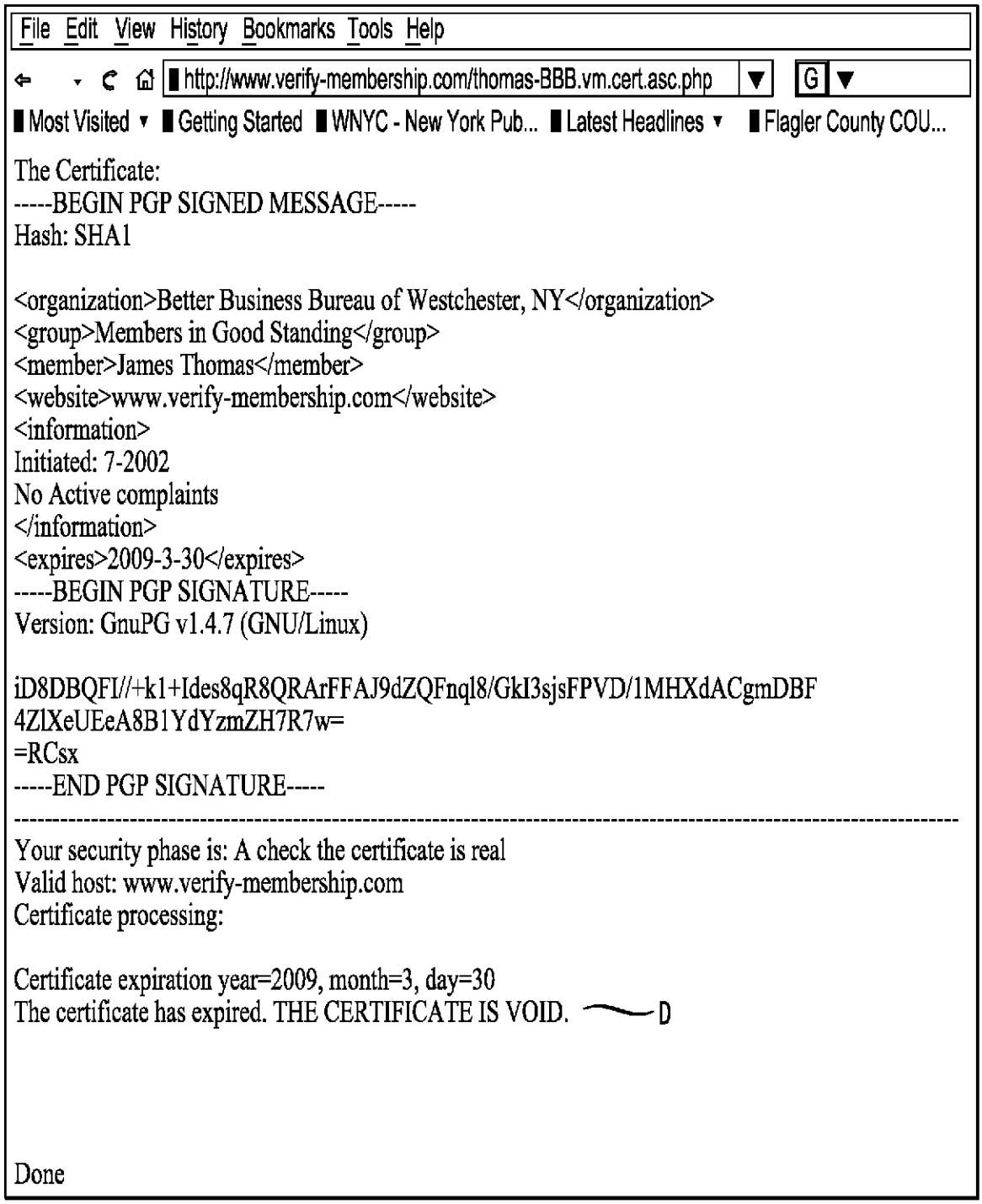
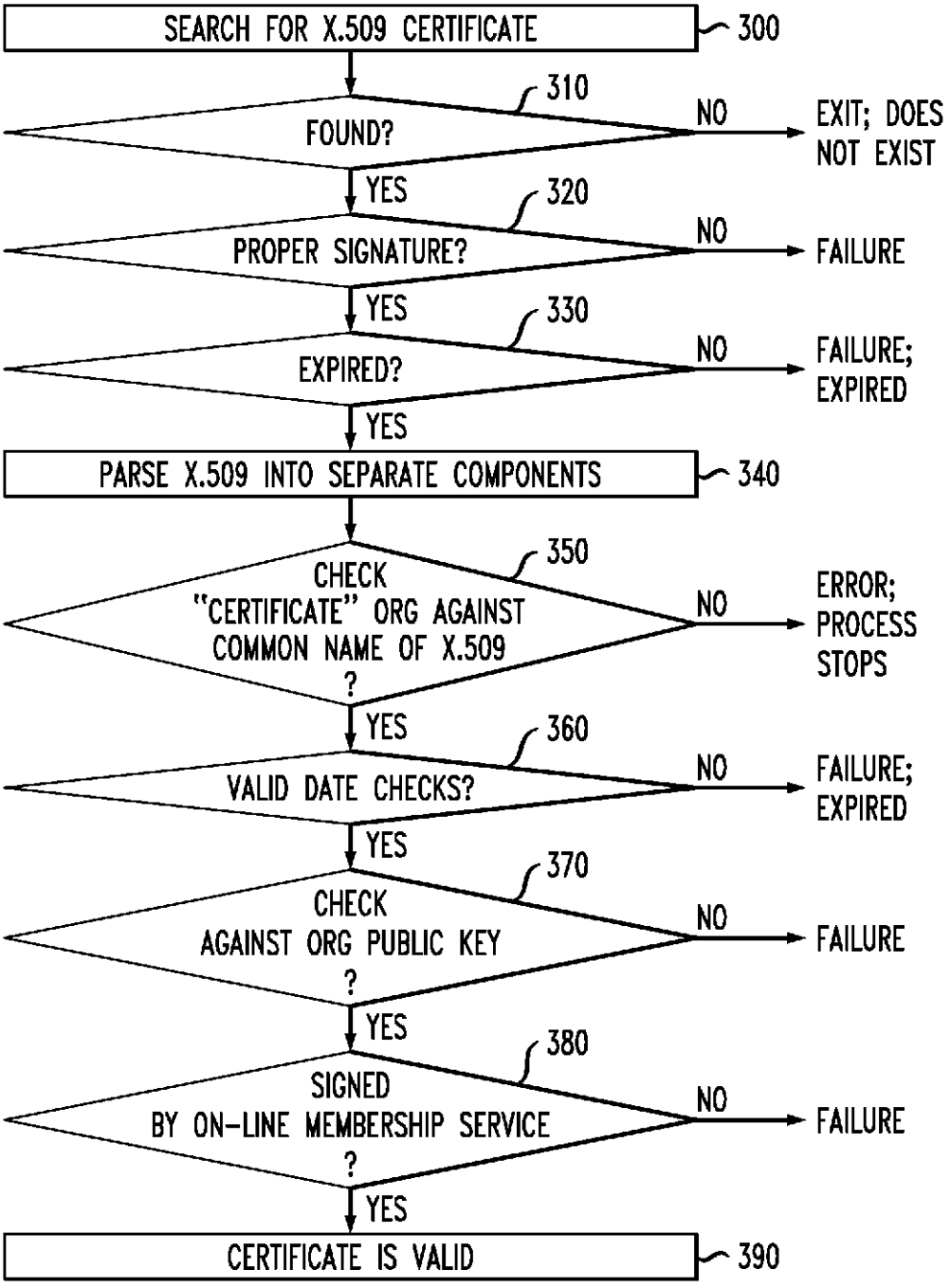

File Edit View History Bookmarks Tools Help
http://www.verify-membership.com/thomas-BBB.vm.cert.asc.php
Most Visited
Getting Started
WNYC - New York Pub...
Latest Headlines
Flagler County COU...
The Certificate:
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
<organization>Better Business Bureau of Westchester, NY</organization>
<group>Members in Good Standing</group>
<member>James Thomas</member>
<website>www.verify-membership.com</website>
<information>
Initiated: 7-2002
No Active complaints
</information>
<expires>2009-3-30</expires>
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.7 (GNU/Linux)
iD8DBQFI//+k1+Ides8qR8QRArFFAJ9dZQFnql8/GkI3sjsFPVD/1MHXdACgmDBF
4ZlXeUEeA8B1YdYzmZH7R7w=
=RCsx
-----END PGP SIGNATURE-----
Your security phase is: A check the certificate is real
Valid host: www.verify-membership.com
Certificate processing:
Certificate expiration year=2009, month=3, day=30
The certificate has expired. THE CERTIFICATE IS VOID.
D
Done

FIG. 12


SEARCH FOR X.509 CERTIFICATE
300
310
FOUND?
NO
EXIT; DOES NOT EXIST
YES
320
PROPER SIGNATURE?
NO
FAILURE
YES
330
EXPIRED?
NO
FAILURE; EXPIRED
YES
PARSE X.509 INTO SEPARATE COMPONENTS
340
350
CHECK "CERTIFICATE" ORG AGAINST COMMON NAME OF X.509 ?
NO
ERROR; PROCESS STOPS
YES
360
VALID DATE CHECKS?
NO
FAILURE; EXPIRED
YES
370
CHECK AGAINST ORG PUBLIC KEY ?
NO
FAILURE
YES
380
SIGNED BY ON-LINE MEMBERSHIP SERVICE ?
NO
FAILURE
YES
CERTIFICATE IS VALID
390