Website Identification Element 12
Organization Identification Element 14
Member Identification Element 16
Certification Information 18 <field> <field> <field>

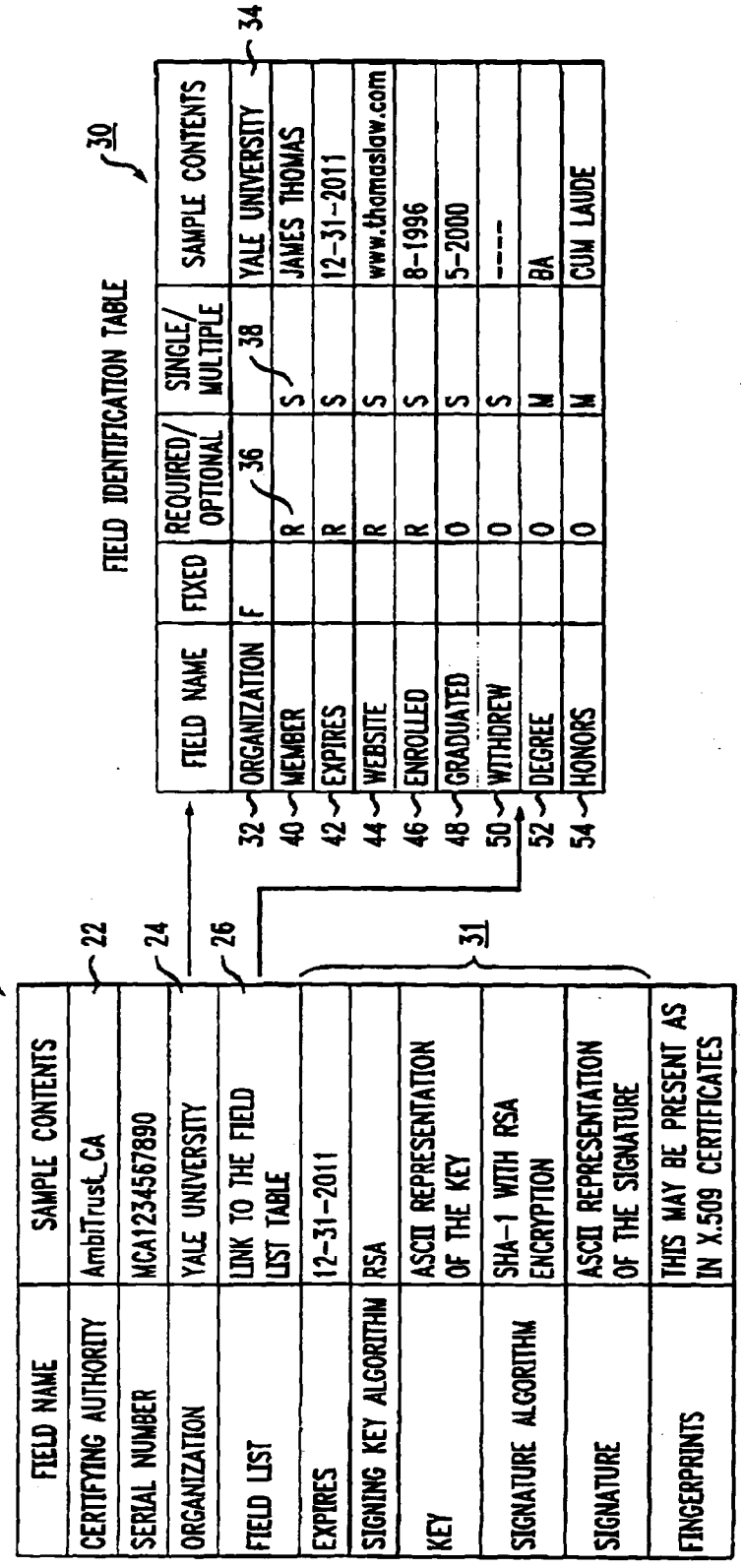
Membership Certificate (MC) 10

FIG. 1

```
<website>www.james_taylor.com</website>                    12
<expires>12-31-2012</expires>
<organization>Yale University</organization>
<OC>00:00:A3:DA:42:7E:A4:B1:AE:DA</OC>                     } 14
<member>James Taylor</member>                              ~ 16
<degree>Bachelor of Arts</degree>
<matriculated1>9-2000</matriculated1>
<graduated>6-2004</graduated>
<honors>Undergraduate Leadership Medal</honors>
<honors>Cum Laude</honors>
<honors>Lacrosse Letter 2003, 2004</honors>                } 18
<major>English</major>
<major>Visual Arts</major>
<degree2>Master of Fine Arts</degree2>
<matriculated2>9-2000</matriculated2>
<graduated2>6-2004</graduated2>
<major2>Sculpture</major2>
<minor2>Web Design</minor2>
<comment>You may contact the registrar at 203-234-5678 for any additional information about the student. Our offices are open 9 AM to 4 PM Eastern time</comment>
```

FIG. 2

FIG. 3


ORGANIZATION CERTIFICATE (OC)
20
FIELD NAME
SAMPLE CONTENTS
CERTIFYING AUTHORITY
AmbiTrust_CA
22
SERIAL NUMBER
MCA1234567890
24
ORGANIZATION
YALE UNIVERSITY
26
FIELD LIST
LINK TO THE FIELD LIST TABLE
EXPIRES
12-31-2011
SIGNING KEY ALGORITHM
RSA
KEY
ASCII REPRESENTATION OF THE KEY
SIGNATURE ALGORITHM
SHA-1 WITH RSA ENCRYPTION
SIGNATURE
ASCII REPRESENTATION OF THE SIGNATURE
FINGERPRINTS
THIS MAY BE PRESENT AS IN X.509 CERTIFICATES
31
FIELD IDENTIFICATION TABLE
30
FIELD NAME
FIXED
REQUIRED/ OPTIONAL
36
SINGLE/ MULTIPLE
38
SAMPLE CONTENTS
34
32 ORGANIZATION F R S YALE UNIVERSITY
40 MEMBER R S JAMES THOMAS
42 EXPIRES R S 12-31-2011
44 WEBSITE R S www.thomaslaw.com
46 ENROLLED R S 8-1996
48 GRADUATED O S 5-2000
50 WITHDREW O S ----
52 DEGREE O M BA
54 HONORS O M CUM LAUDE

CA field 22

<OC_version>1</OC_version>
<OC_serial_number>00:00:A3:DA:42:7E:A4:B1:AE:DA</OC_serial_number>
<issuer_number>00:00</issuer_number>
<issuer_parent>00:00</issuer_parent>
<issuer>Verify Membership Inc.</issuer>
<issuer_URL>verify-membership.com</issuer_URL>
<issuer_phone_number>1-845-555-1212<issuer_phone_number>
<issuer_email>OC_information@verify-membership.com</issuer_email>
<issuer_signature_algorithm>PGP</issuer_signature_algorithm>
<certificate_verification_level>1</certificate_verification_level>
<issuer_CRL_URL>www.verify-membership.com/CRL</issuer_CRL_URL>

FIG. 4

Organization ID field 24

<organization>Yale University</organization>
<Sub_organization>Yale College</Sub_organization>
<organization_common_name>Yale</organization_common_name>
<organization_street_address>123 Elm Street. New Haven, Ct</organization_street_address>
<organization_country>USA</organization_country>
<organization_telephone>1-203-555-1212</organization_telephone>
<organization_website>www.yale.edu</organization_website>
<organization_industry>Higher Education</organization_industry>
<organization_CRL_URL>www.yale.edu/registrar/CRL</organization_CRL_URL>

FIG. 5

50

Name	Required/Opt	Single/Mult	REQUIRES	PRODUCES
degree2	O	S	degree	matriculated2,graduated2
matriculated2	O	S	degree2	
graduated2	O	S	degree2	

FIG. 6

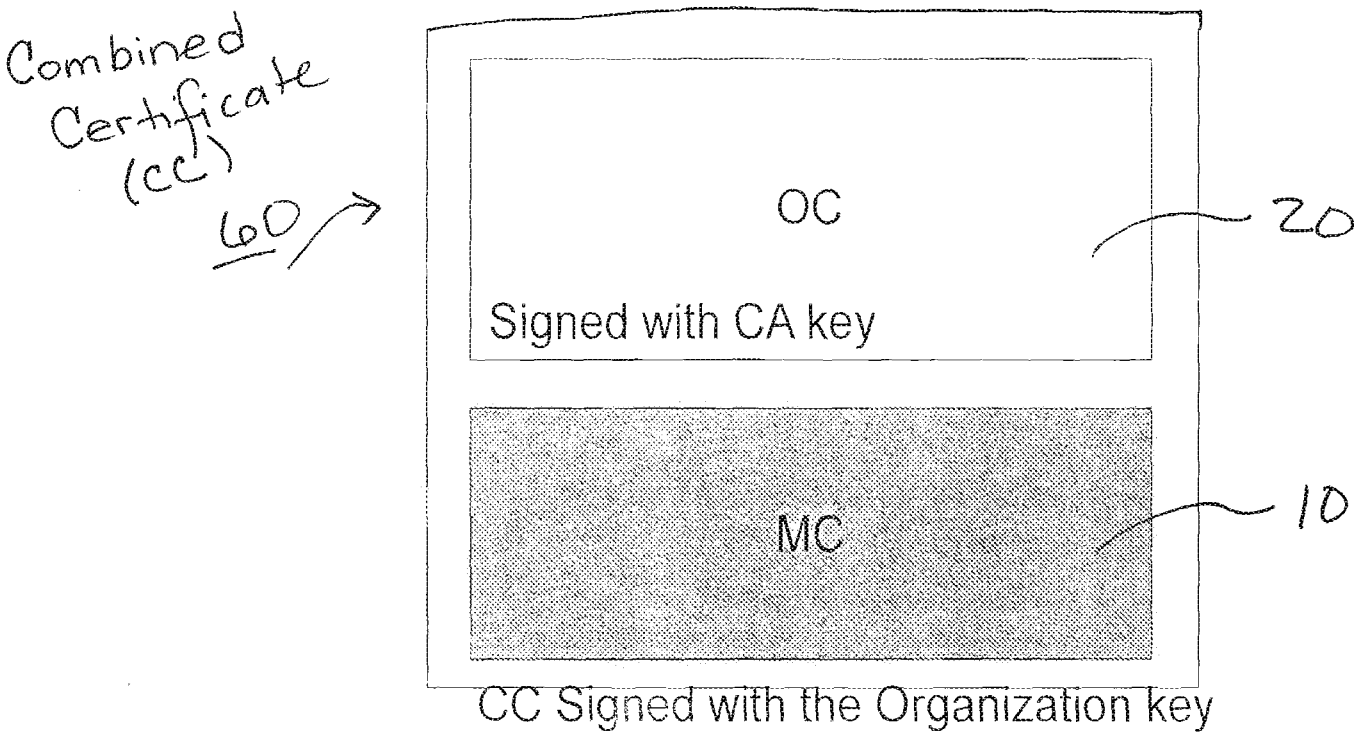
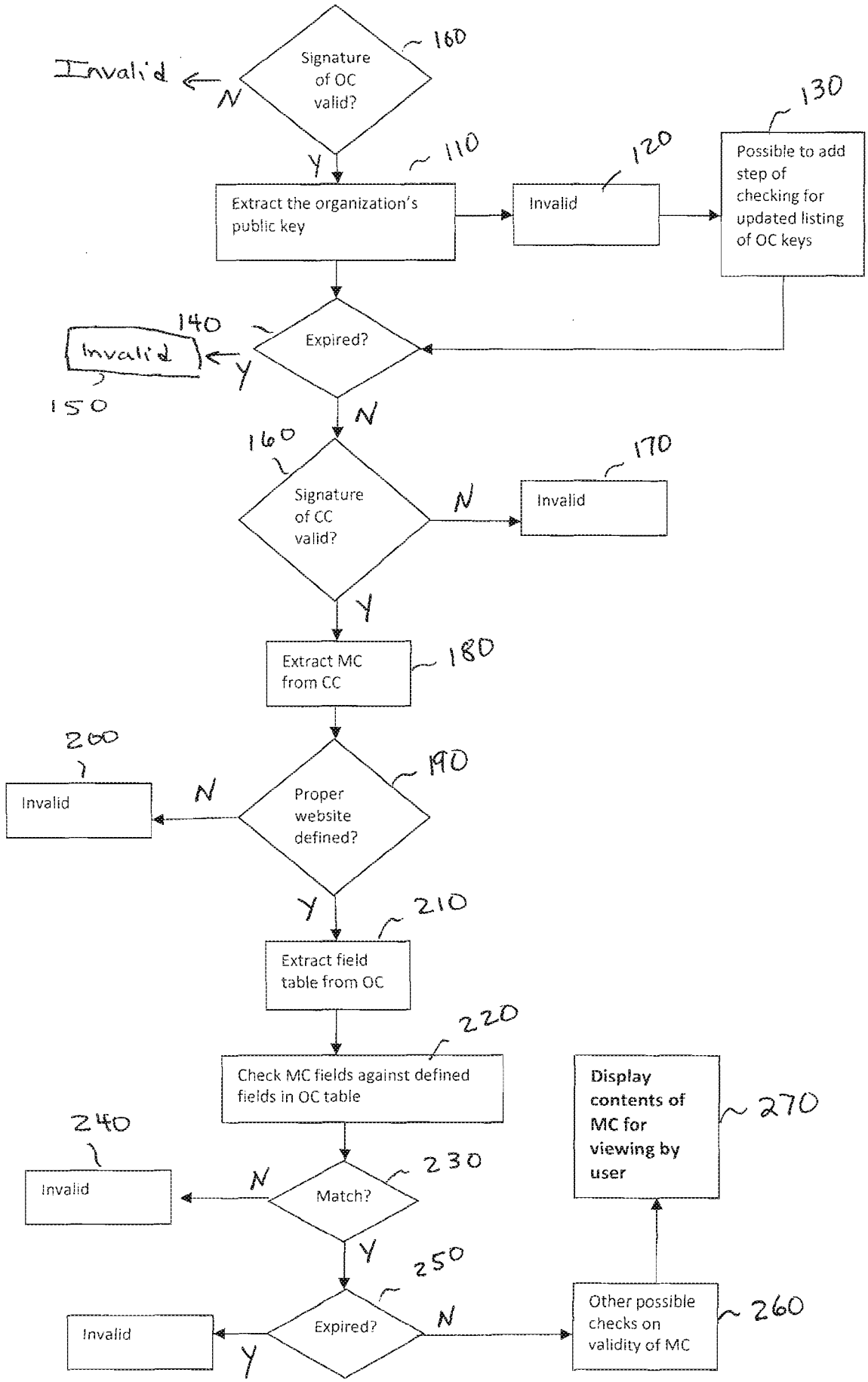


FIG. 7

FIG. 8


Signature of OC valid?
160
Invalid
N
Y
Extract the organization's public key
110
Invalid
120
Possible to add step of checking for updated listing of OC keys
130
Expired?
140
Invalid
150
Y
N
Signature of CC valid?
160
N
Invalid
170
Y
Extract MC from CC
180
Proper website defined?
190
N
Invalid
200
Y
Extract field table from OC
210
Check MC fields against defined fields in OC table
220
Match?
230
N
Invalid
240
Y
Expired?
250
Y
Invalid
N
Other possible checks on validity of MC
260
Display contents of MC for viewing by user
270