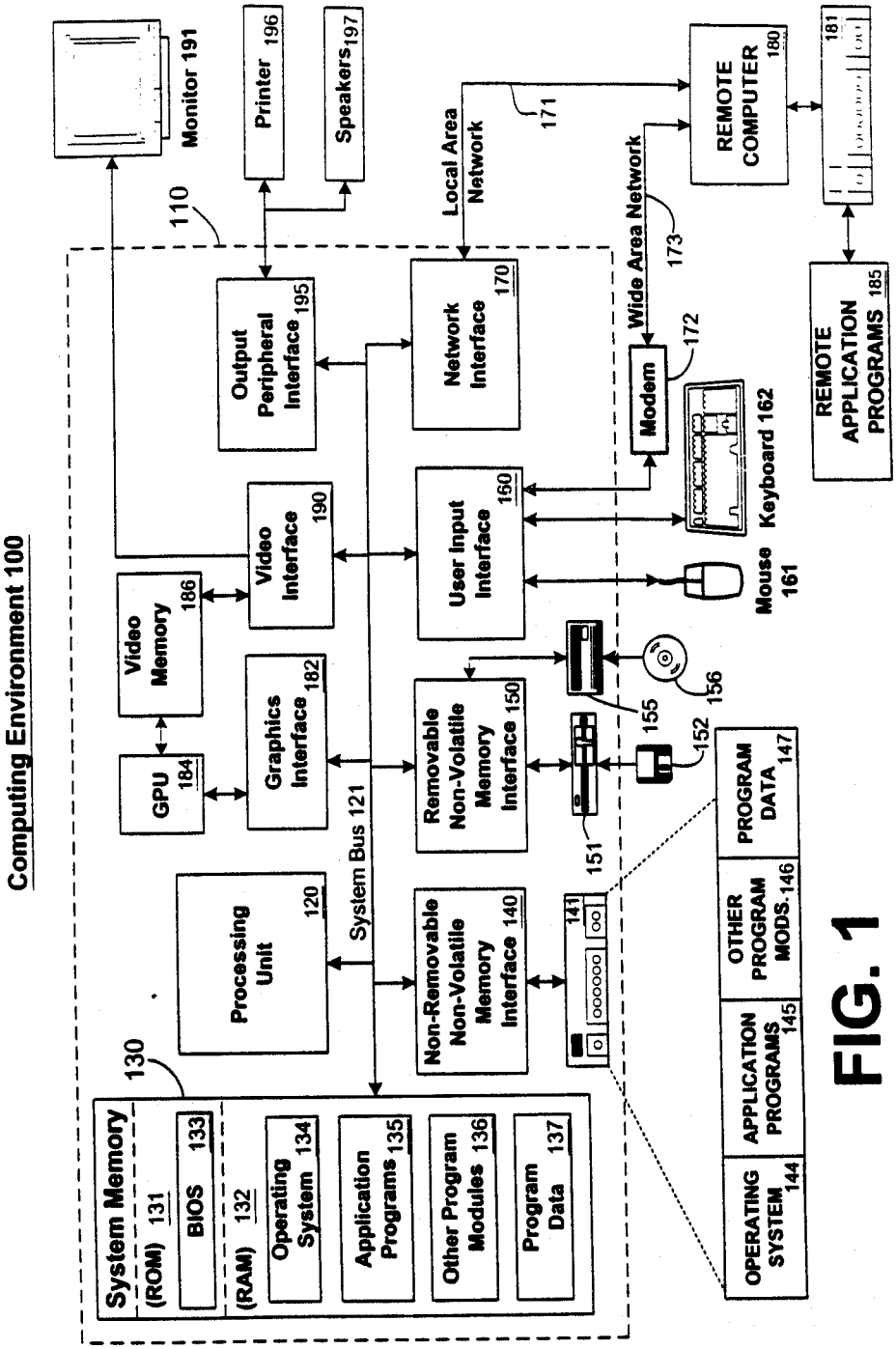

Computing Environment 100
110
Monitor 191
Printer 196
Speakers 197
Local Area Network
171
REMOTE COMPUTER 180
181
Wide Area Network
173
Output Peripheral Interface 195
Network Interface 170
REMOTE APPLICATION PROGRAMS 185
Modem 172
Video Memory 186
Video Interface 190
User Input Interface 160
Keyboard 162
Mouse 161
GPU 184
Graphics Interface 182
Removable Non-Volatile Memory Interface 150
155
156
152
151
System Bus 121
Processing Unit 120
Non-Removable Non-Volatile Memory Interface 140
141
PROGRAM DATA 147
OTHER PROGRAM MODS. 146
APPLICATION PROGRAMS 145
OPERATING SYSTEM 144
130
System Memory
(ROM) 131
BIOS 133
(RAM) 132
Operating System 134
Application Programs 135
Other Program Modules 136
Program Data 137

FIG. 1

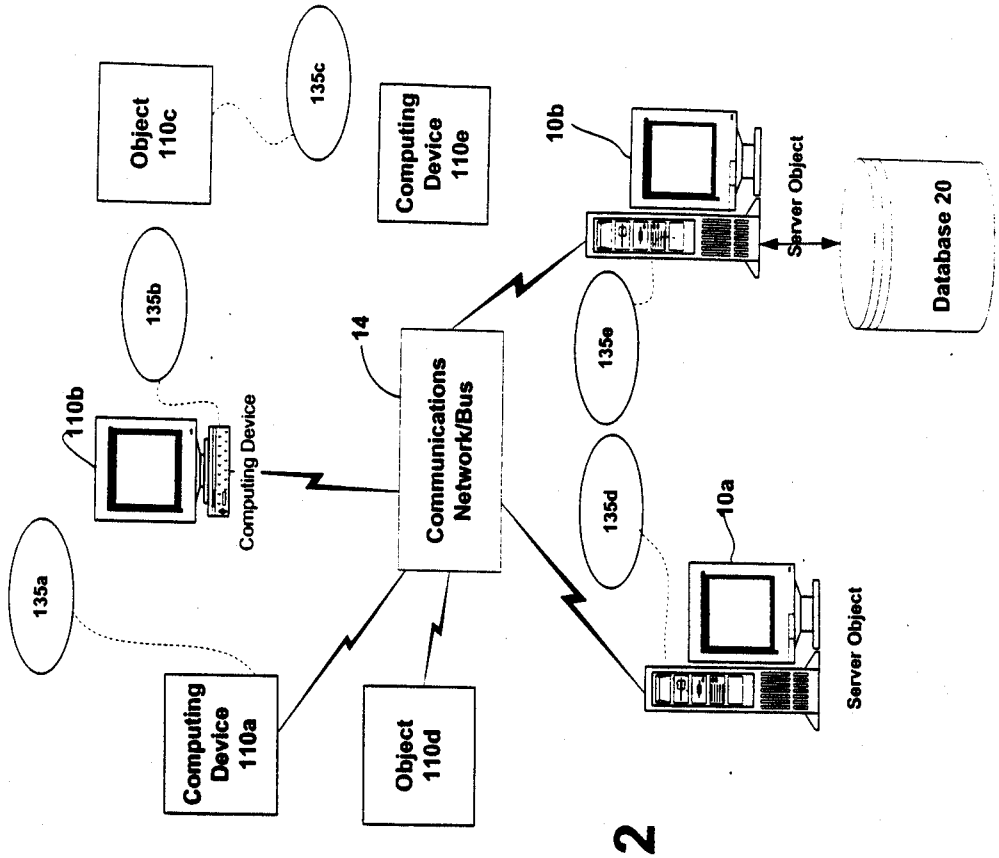

Object 110c
135c
Computing Device 110e
10b
Server Object
Database 20
135b
14
Communications Network/Bus
135e
110b
Computing Device
135a
135d
10a
Computing Device 110a
Object 110d
Server Object

FIG. 2

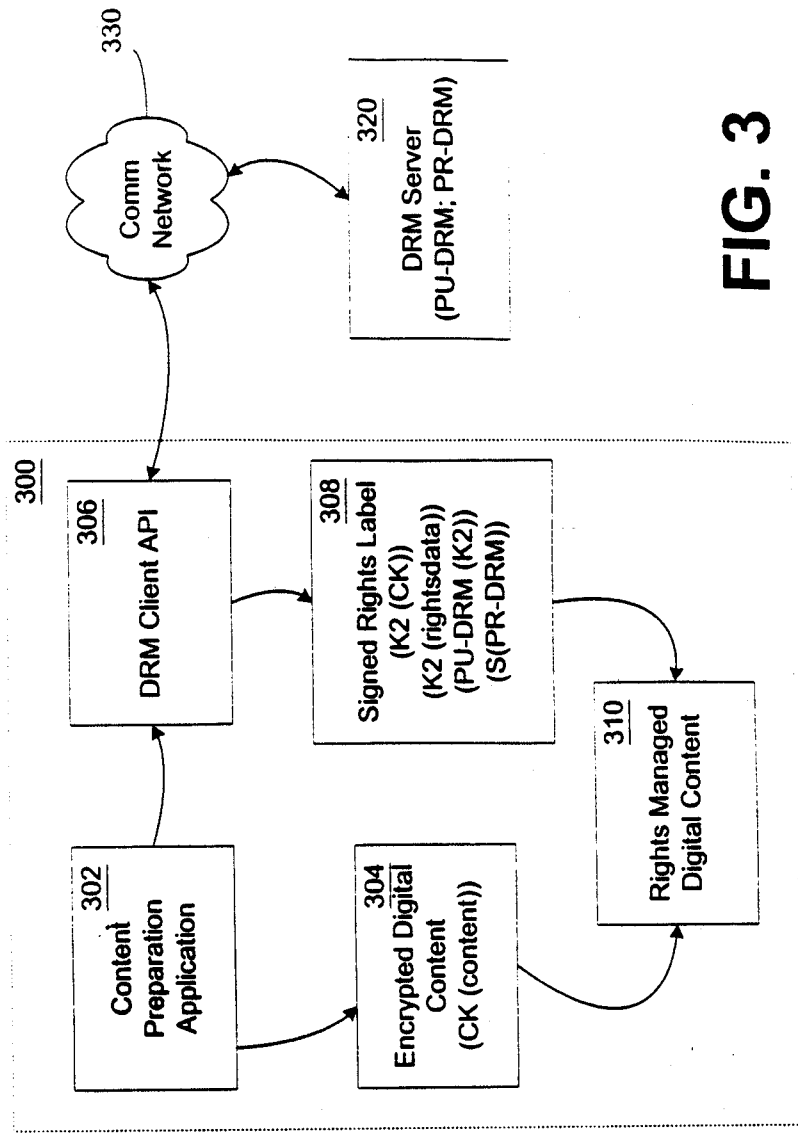

330
Comm Network
320
DRM Server
(PU-DRM; PR-DRM)
300
306
DRM Client API
308
Signed Rights Label
(K2 (CK))
(K2 (rightsdata))
(PU-DRM (K2))
(S(PR-DRM))
302
Content Preparation Application
304
Encrypted Digital Content
(CK (content))
310
Rights Managed Digital Content

FIG. 3

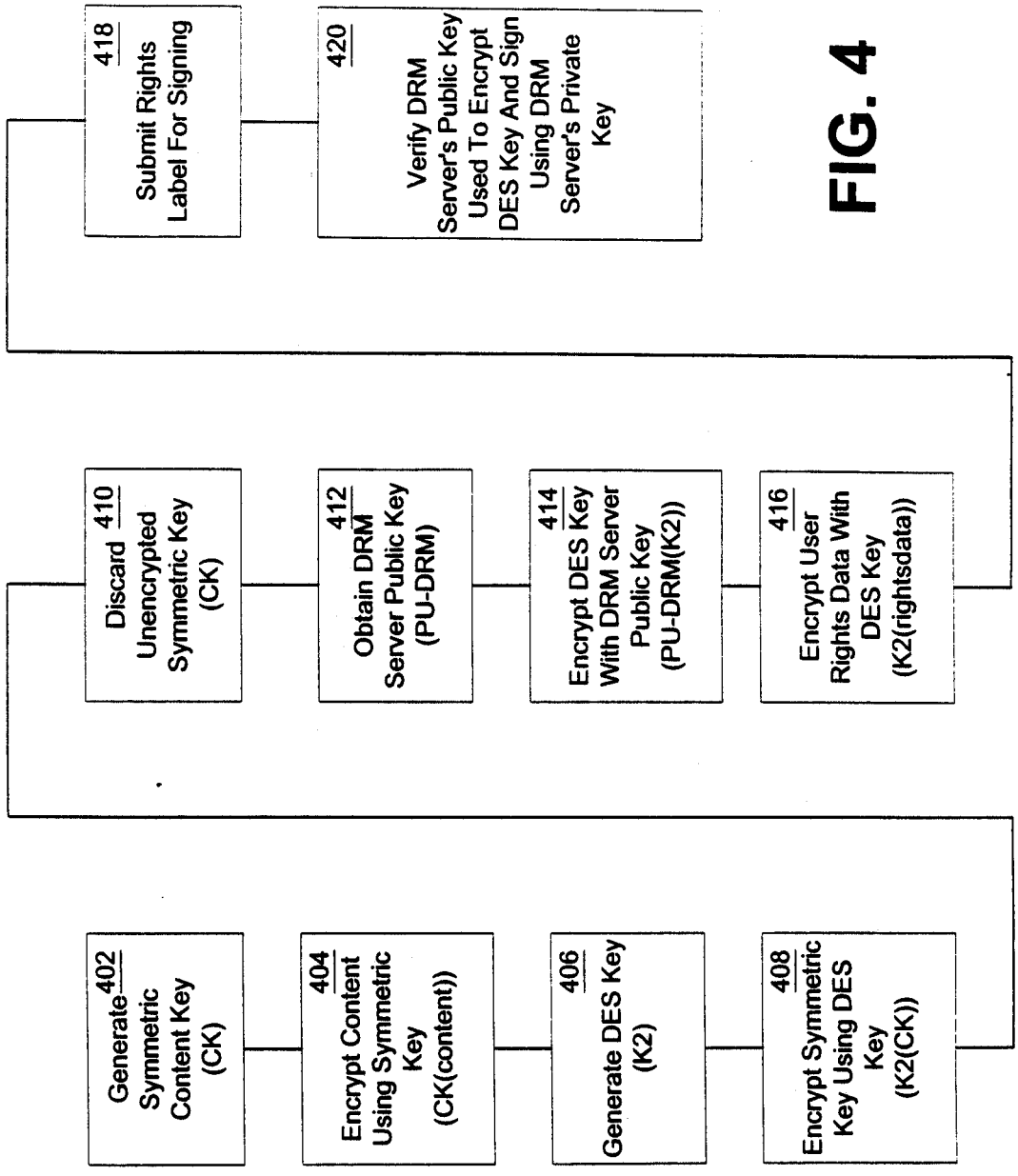

Generate 402 Symmetric Content Key (CK)
404 Encrypt Content Using Symmetric Key (CK(content))
406 Generate DES Key (K2)
408 Encrypt Symmetric Key Using DES Key (K2(CK))
Discard 410 Unencrypted Symmetric Key (CK)
412 Obtain DRM Server Public Key (PU-DRM)
414 Encrypt DES Key With DRM Server Public Key (PU-DRM(K2))
416 Encrypt User Rights Data With DES Key (K2(rightsdata))
418 Submit Rights Label For Signing
420 Verify DRM Server's Public Key Used To Encrypt DES Key And Sign Using DRM Server's Private Key

FIG. 4

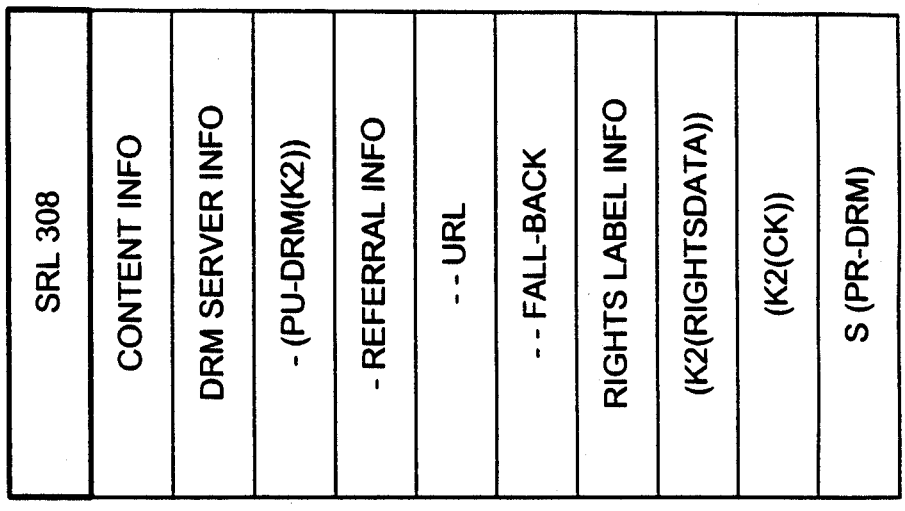

SRL 308
CONTENT INFO
DRM SERVER INFO
- (PU-DRM(K2))
- REFERRAL INFO
- - URL
- - FALL-BACK
RIGHTS LABEL INFO
(K2(RIGHTSDATA))
(K2(CK))
S (PR-DRM)

FIG. 4A

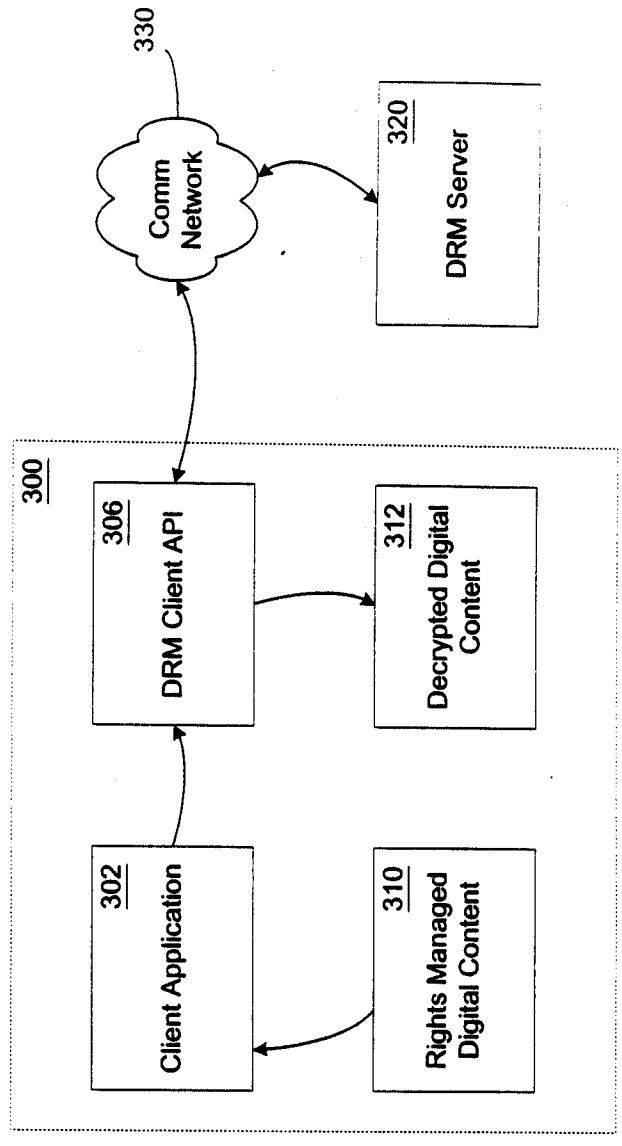

330
Comm Network
320
DRM Server
300
306
DRM Client API
312
Decrypted Digital Content
302
Client Application
310
Rights Managed Digital Content

FIG. 5

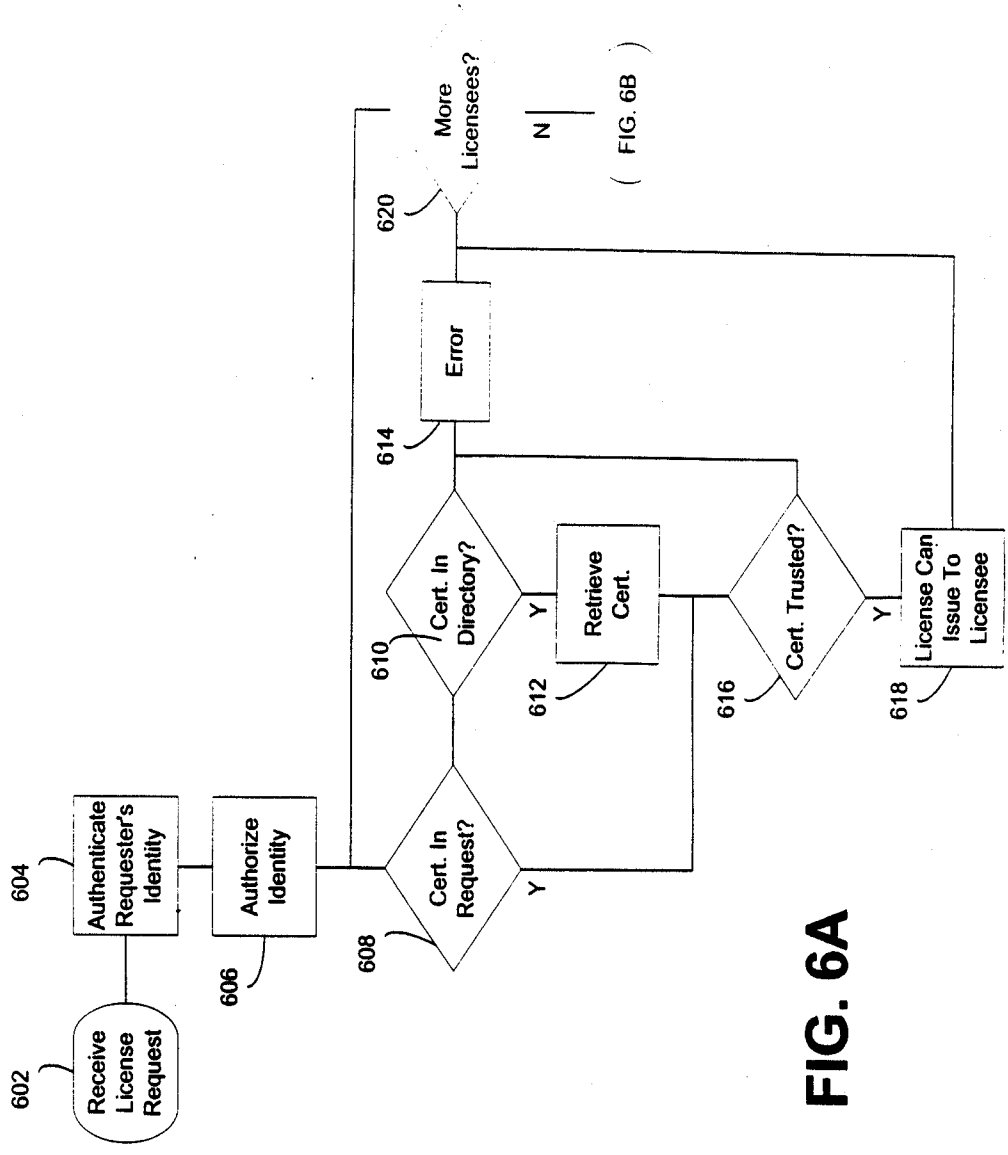

Receive License Request
602
Authenticate Requester's Identity
604
Authorize Identity
606
Cert. In Request?
608
Y
Cert. In Directory?
610
Y
Retrieve Cert.
612
Cert. Trusted?
616
Y
License Can Issue To Licensee
618
Error
614
More Licensees?
620
N
(FIG. 6B)

FIG. 6A

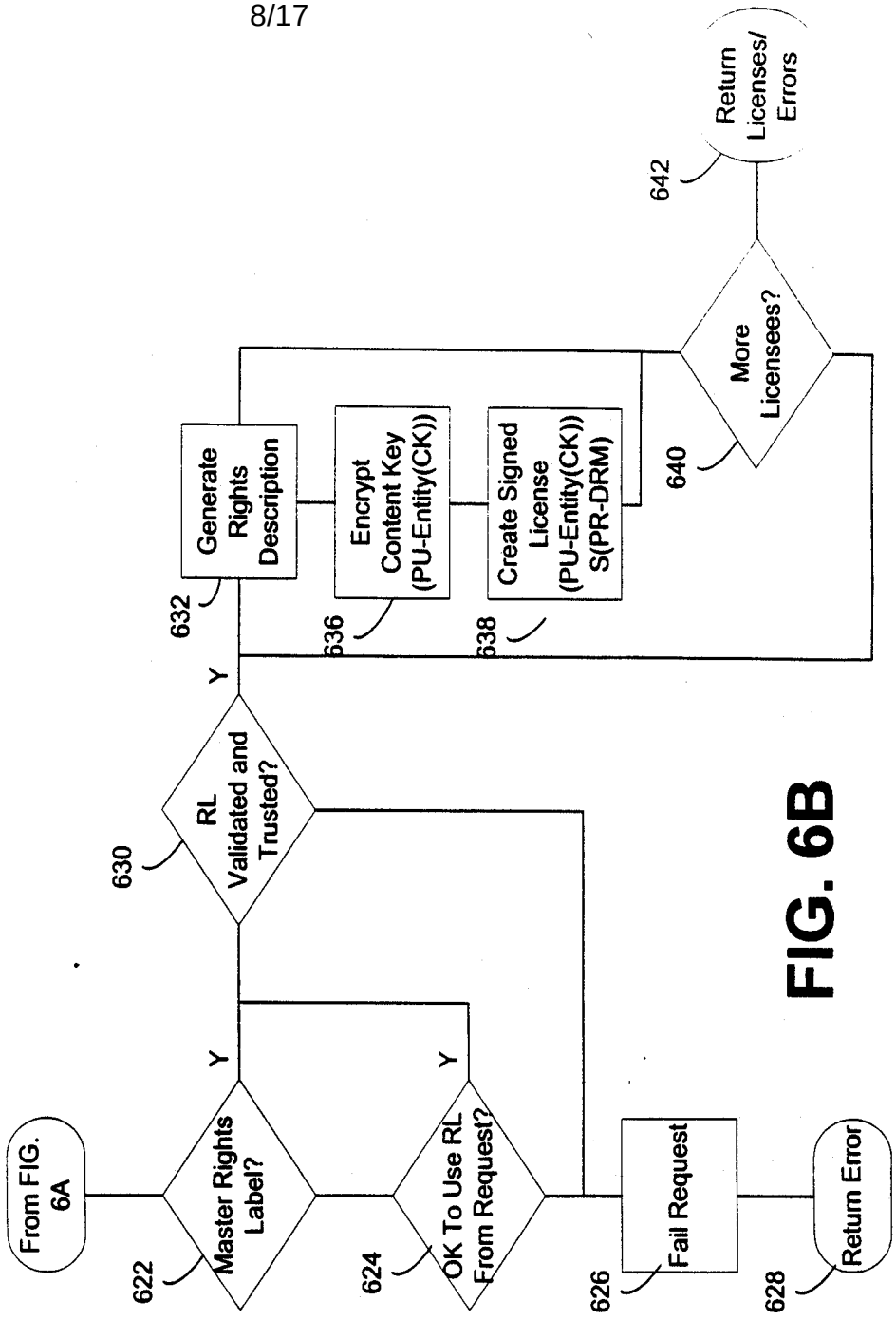

From FIG. 6A
Master Rights Label?
622
Y
OK To Use RL From Request?
624
Y
RL Validated and Trusted?
630
Y
Fail Request
626
Return Error
628
Generate Rights Description
632
Encrypt Content Key (PU-Entity(CK))
636
Create Signed License (PU-Entity(CK)) S(PR-DRM)
638
More Licensees?
640
Return Licenses/ Errors
642

FIG. 6B

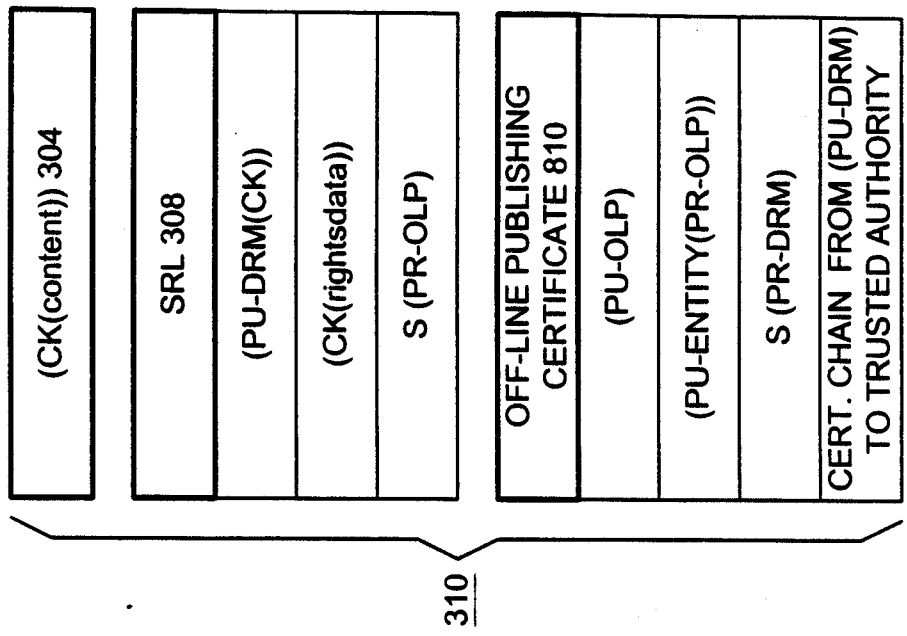

(CK(content)) 304
SRL 308
(PU-DRM(CK))
(CK(rightsdata))
S (PR-OLP)
OFF-LINE PUBLISHING CERTIFICATE 810
(PU-OLP)
(PU-ENTITY(PR-OLP))
S (PR-DRM)
CERT. CHAIN FROM (PU-DRM) TO TRUSTED AUTHORITY
310

FIG. 7

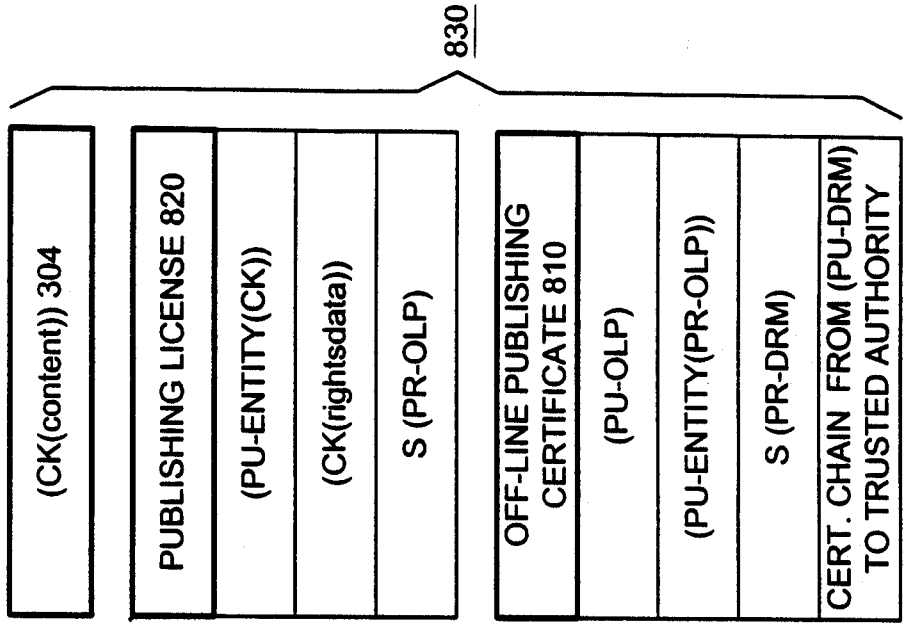

830
(CK(content)) 304
PUBLISHING LICENSE 820
(PU-ENTITY(CK))
(CK(rightsdata))
S (PR-OLP)
OFF-LINE PUBLISHING CERTIFICATE 810
(PU-OLP)
(PU-ENTITY(PR-OLP))
S (PR-DRM)
CERT. CHAIN FROM (PU-DRM) TO TRUSTED AUTHORITY

FIG. 8

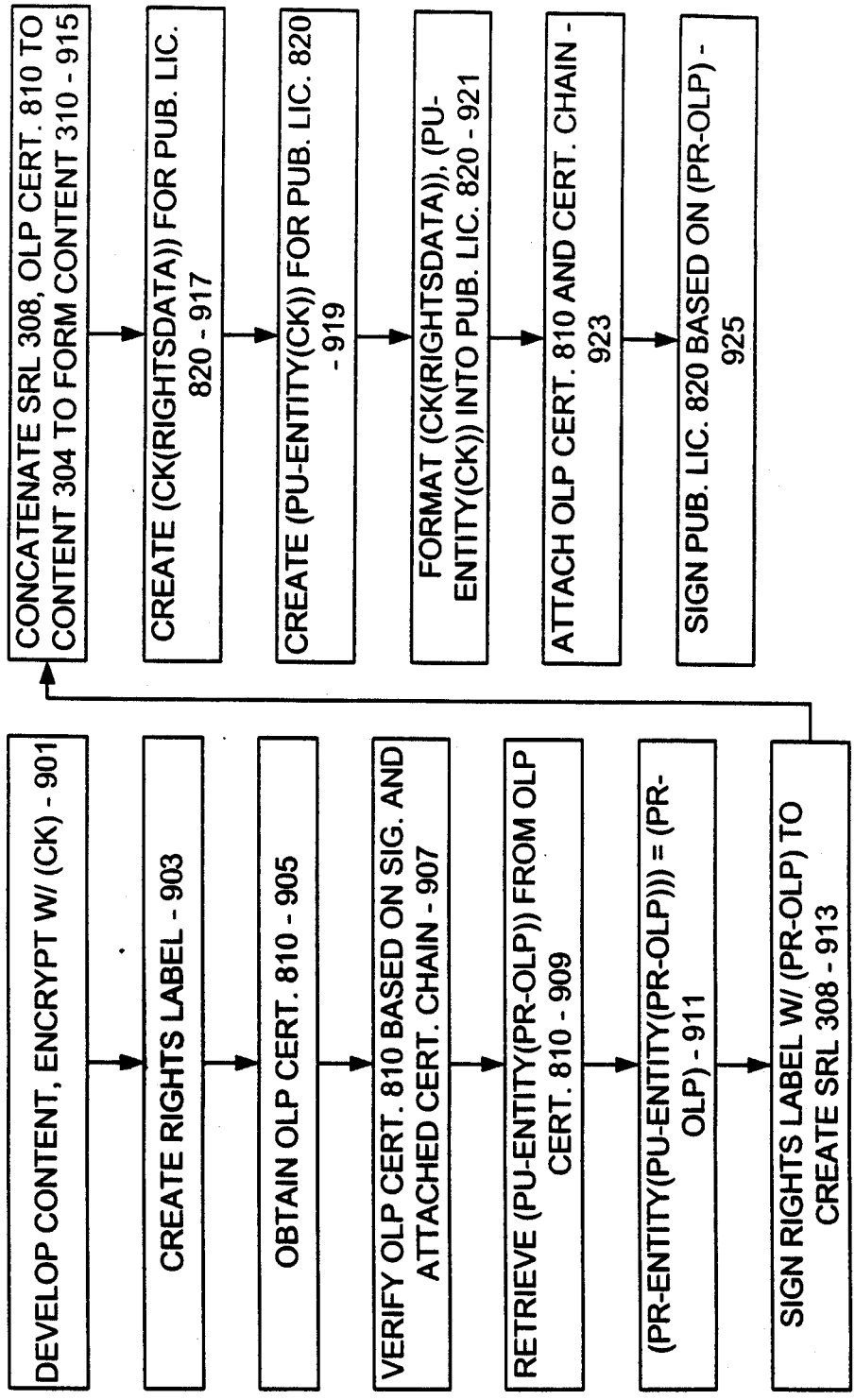

DEVELOP CONTENT, ENCRYPT W/ (CK) - 901
CREATE RIGHTS LABEL - 903
OBTAIN OLP CERT. 810 - 905
VERIFY OLP CERT. 810 BASED ON SIG. AND ATTACHED CERT. CHAIN - 907
RETRIEVE (PU-ENTITY(PR-OLP)) FROM OLP CERT. 810 - 909
(PR-ENTITY(PU-ENTITY(PR-OLP))) = (PR-OLP) - 911
SIGN RIGHTS LABEL W/ (PR-OLP) TO CREATE SRL 308 - 913
CONCATENATE SRL 308, OLP CERT. 810 TO CONTENT 304 TO FORM CONTENT 310 - 915
CREATE (CK(RIGHTSDATA)) FOR PUB. LIC. 820 - 917
CREATE (PU-ENTITY(CK)) FOR PUB. LIC. 820 - 919
FORMAT (CK(RIGHTSDATA)), (PU-ENTITY(CK)) INTO PUB. LIC. 820 - 921
ATTACH OLP CERT. 810 AND CERT. CHAIN - 923
SIGN PUB. LIC. 820 BASED ON (PR-OLP) - 925

Fig. 9

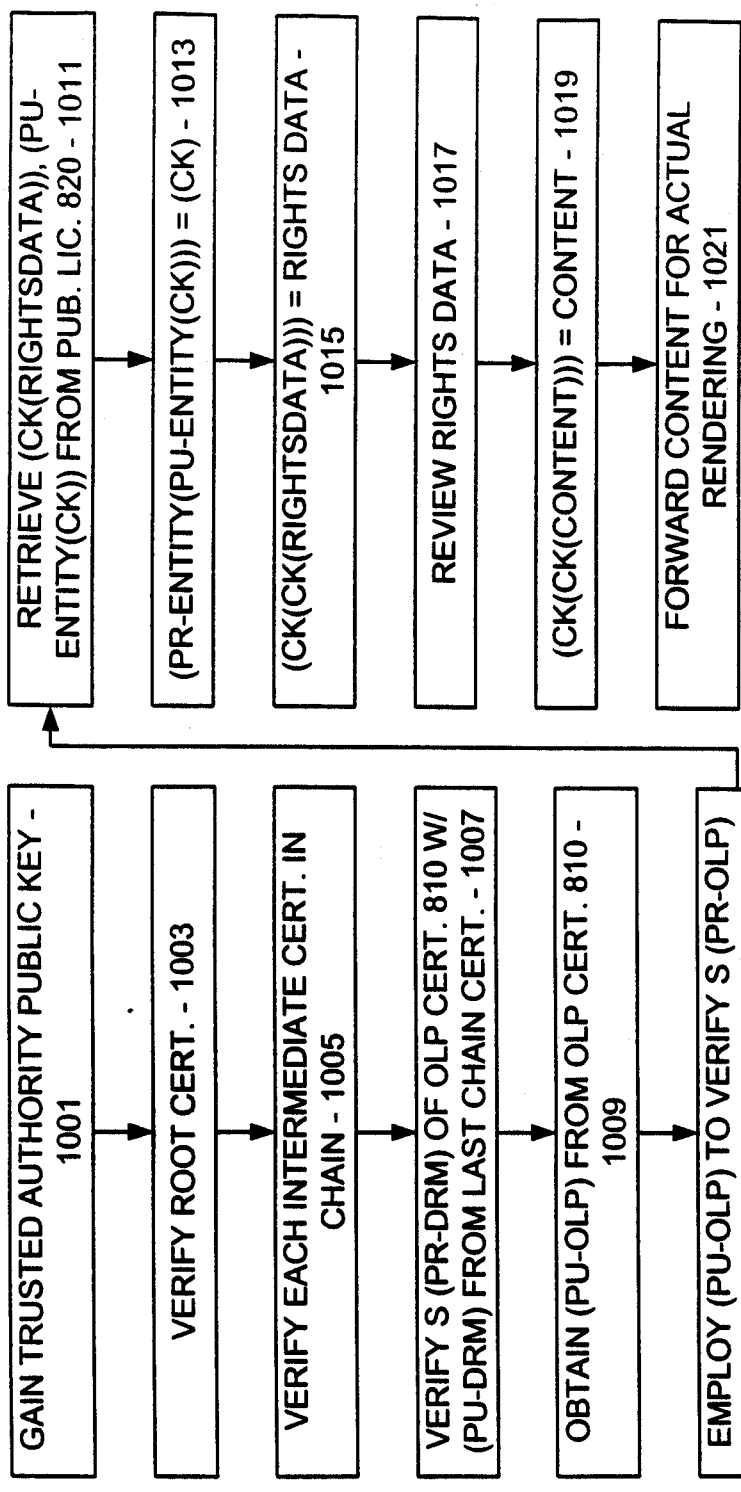

GAIN TRUSTED AUTHORITY PUBLIC KEY - 1001
VERIFY ROOT CERT. - 1003
VERIFY EACH INTERMEDIATE CERT. IN CHAIN - 1005
VERIFY S (PR-DRM) OF OLP CERT. 810 W/ (PU-DRM) FROM LAST CHAIN CERT. - 1007
OBTAIN (PU-OLP) FROM OLP CERT. 810 - 1009
EMPLOY (PU-OLP) TO VERIFY S (PR-OLP) OF PUB. LIC. 820 - 1010
RETRIEVE (CK(RIGHTSDATA)), (PU-ENTITY(CK)) FROM PUB. LIC. 820 - 1011
(PR-ENTITY(PU-ENTITY(CK))) = (CK) - 1013
(CK(CK(RIGHTSDATA))) = RIGHTS DATA - 1015
REVIEW RIGHTS DATA - 1017
(CK(CK(CONTENT))) = CONTENT - 1019
FORWARD CONTENT FOR ACTUAL RENDERING - 1021

Fig. 10

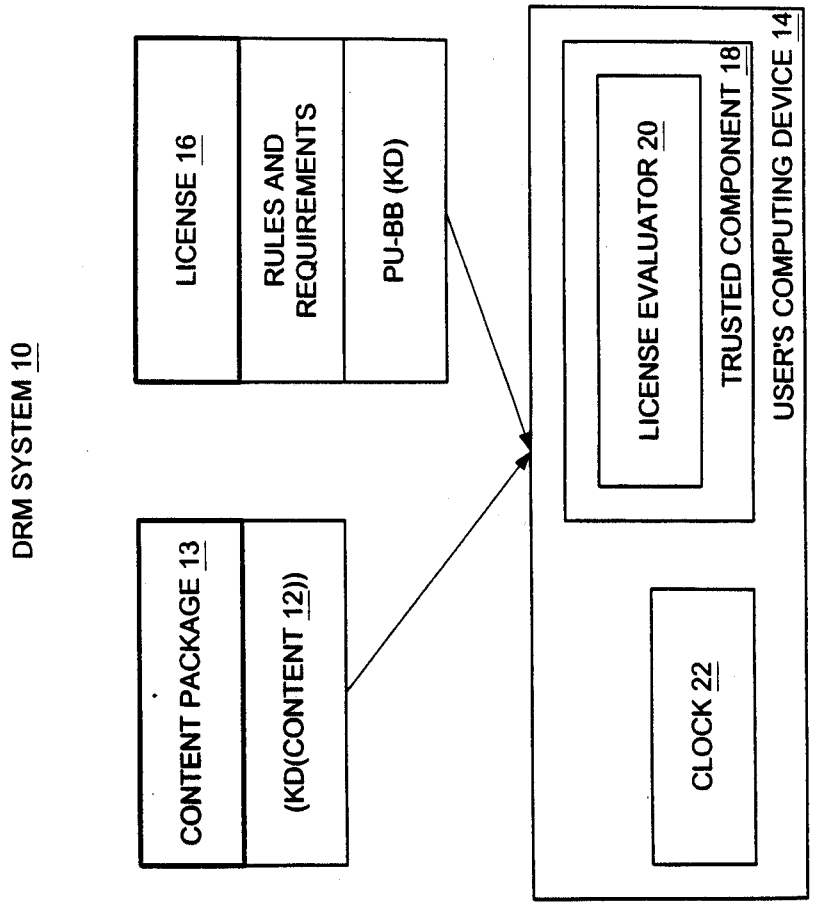

DRM SYSTEM 10
CONTENT PACKAGE 13
(KD(CONTENT 12))
LICENSE 16
RULES AND REQUIREMENTS
PU-BB (KD)
USER'S COMPUTING DEVICE 14
TRUSTED COMPONENT 18
LICENSE EVALUATOR 20
CLOCK 22

Fig. 11

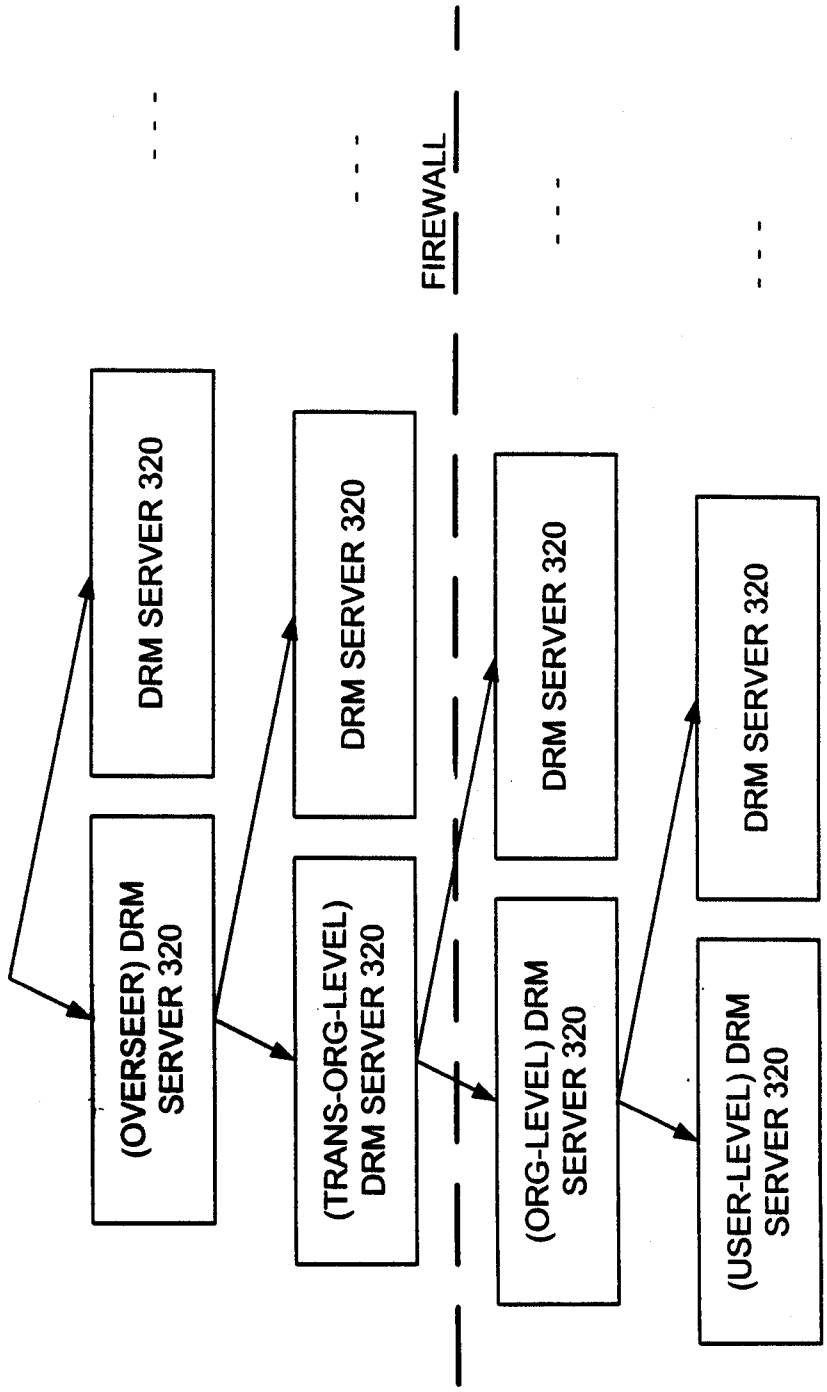

FIREWALL
(OVERSEER) DRM SERVER 320
DRM SERVER 320
(TRANS-ORG-LEVEL) DRM SERVER 320
DRM SERVER 320
(ORG-LEVEL) DRM SERVER 320
DRM SERVER 320
(USER-LEVEL) DRM SERVER 320

Fig. 12

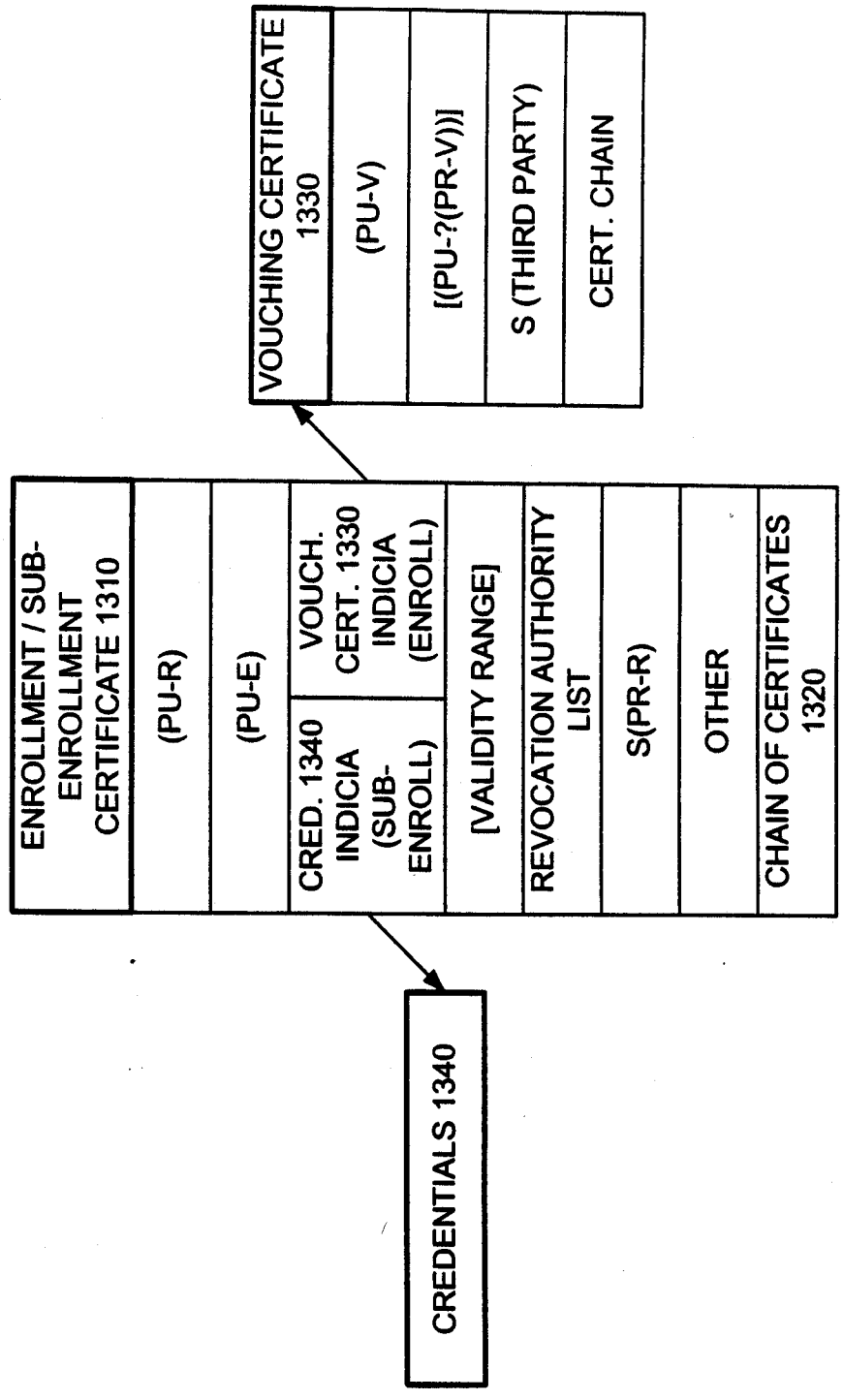

ENROLLMENT / SUB-ENROLLMENT CERTIFICATE 1310
(PU-R)
(PU-E)
CRED. 1340 INDICIA (SUB-ENROLL)
VOUCH. CERT. 1330 INDICIA (ENROLL)
[VALIDITY RANGE]
REVOCATION AUTHORITY LIST
S(PR-R)
OTHER
CHAIN OF CERTIFICATES 1320
CREDENTIALS 1340
VOUCHING CERTIFICATE 1330
(PU-V)
[(PU-?(PR-V))]
S (THIRD PARTY)
CERT. CHAIN

FIG. 13

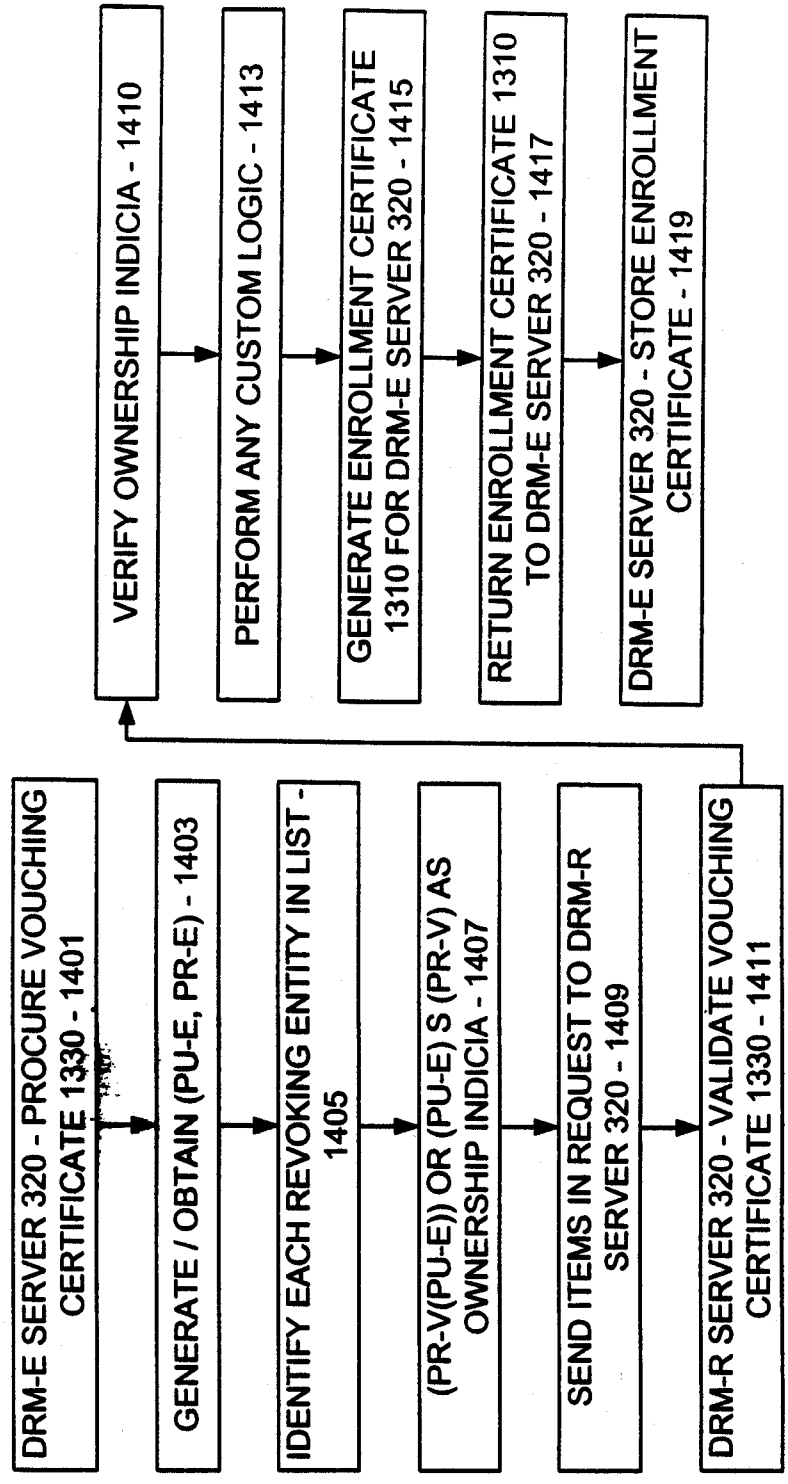

DRM-E SERVER 320 - PROCURE VOUCHING CERTIFICATE 1330 - 1401
GENERATE / OBTAIN (PU-E, PR-E) - 1403
IDENTIFY EACH REVOKING ENTITY IN LIST - 1405
(PR-V(PU-E)) OR (PU-E) S (PR-V) AS OWNERSHIP INDICIA - 1407
SEND ITEMS IN REQUEST TO DRM-R SERVER 320 - 1409
DRM-R SERVER 320 - VALIDATE VOUCHING CERTIFICATE 1330 - 1411
VERIFY OWNERSHIP INDICIA - 1410
PERFORM ANY CUSTOM LOGIC - 1413
GENERATE ENROLLMENT CERTIFICATE 1310 FOR DRM-E SERVER 320 - 1415
RETURN ENROLLMENT CERTIFICATE 1310 TO DRM-E SERVER 320 - 1417
DRM-E SERVER 320 - STORE ENROLLMENT CERTIFICATE - 1419

Fig. 14

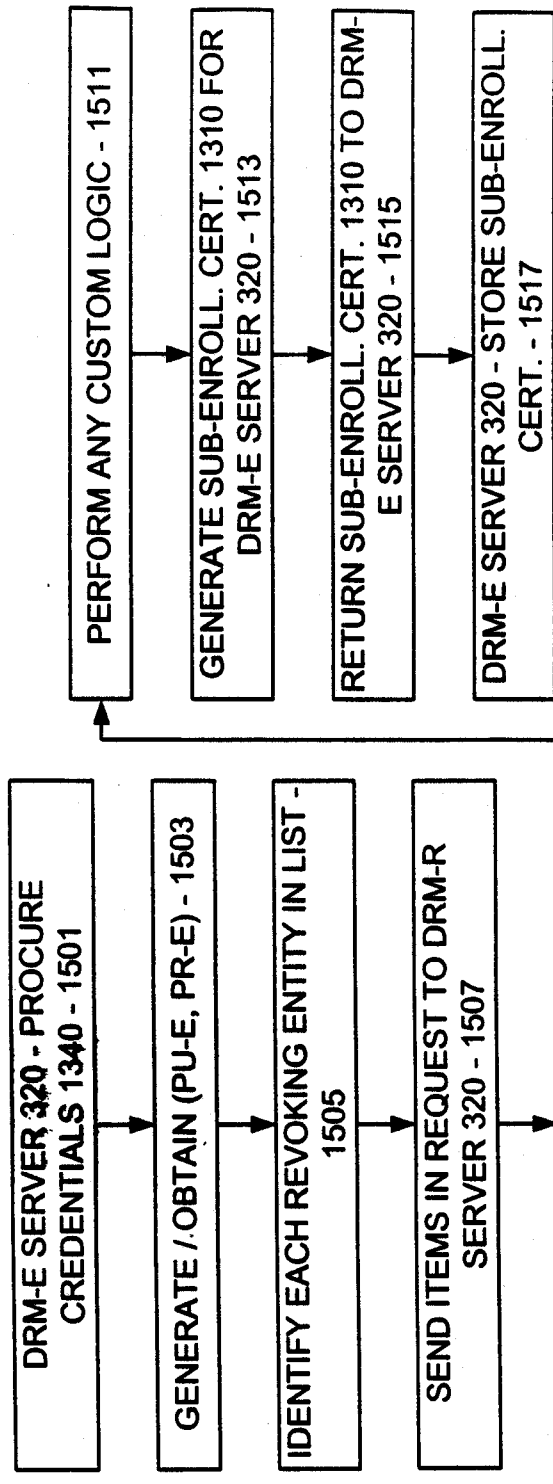

DRM-E SERVER 320 - PROCURE CREDENTIALS 1340 - 1501
GENERATE /.OBTAIN (PU-E, PR-E) - 1503
IDENTIFY EACH REVOKING ENTITY IN LIST - 1505
SEND ITEMS IN REQUEST TO DRM-R SERVER 320 - 1507
DRM-R SERVER 320 - VALIDATE CREDENTIALS 1340 - 1509
PERFORM ANY CUSTOM LOGIC - 1511
GENERATE SUB-ENROLL. CERT. 1310 FOR DRM-E SERVER 320 - 1513
RETURN SUB-ENROLL. CERT. 1310 TO DRM-E SERVER 320 - 1515
DRM-E SERVER 320 - STORE SUB-ENROLL. CERT. - 1517

Fig. 15