FIG. 1

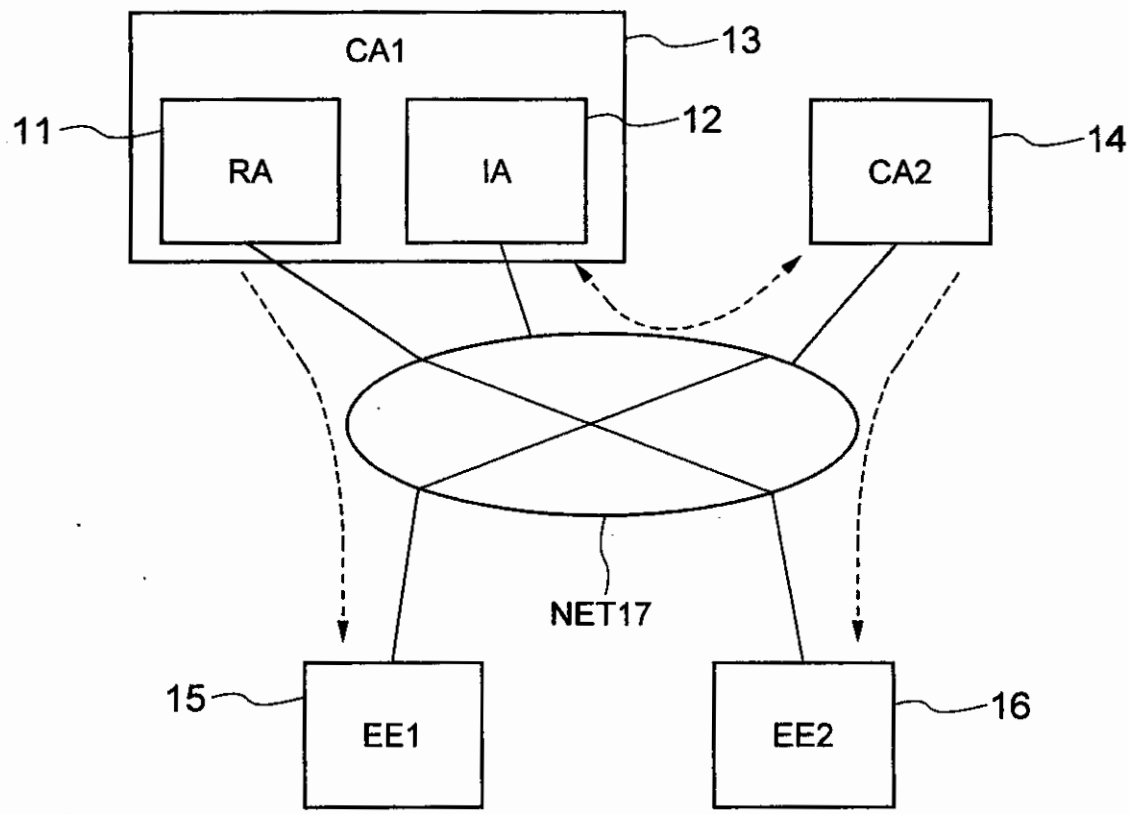


FIG. 2

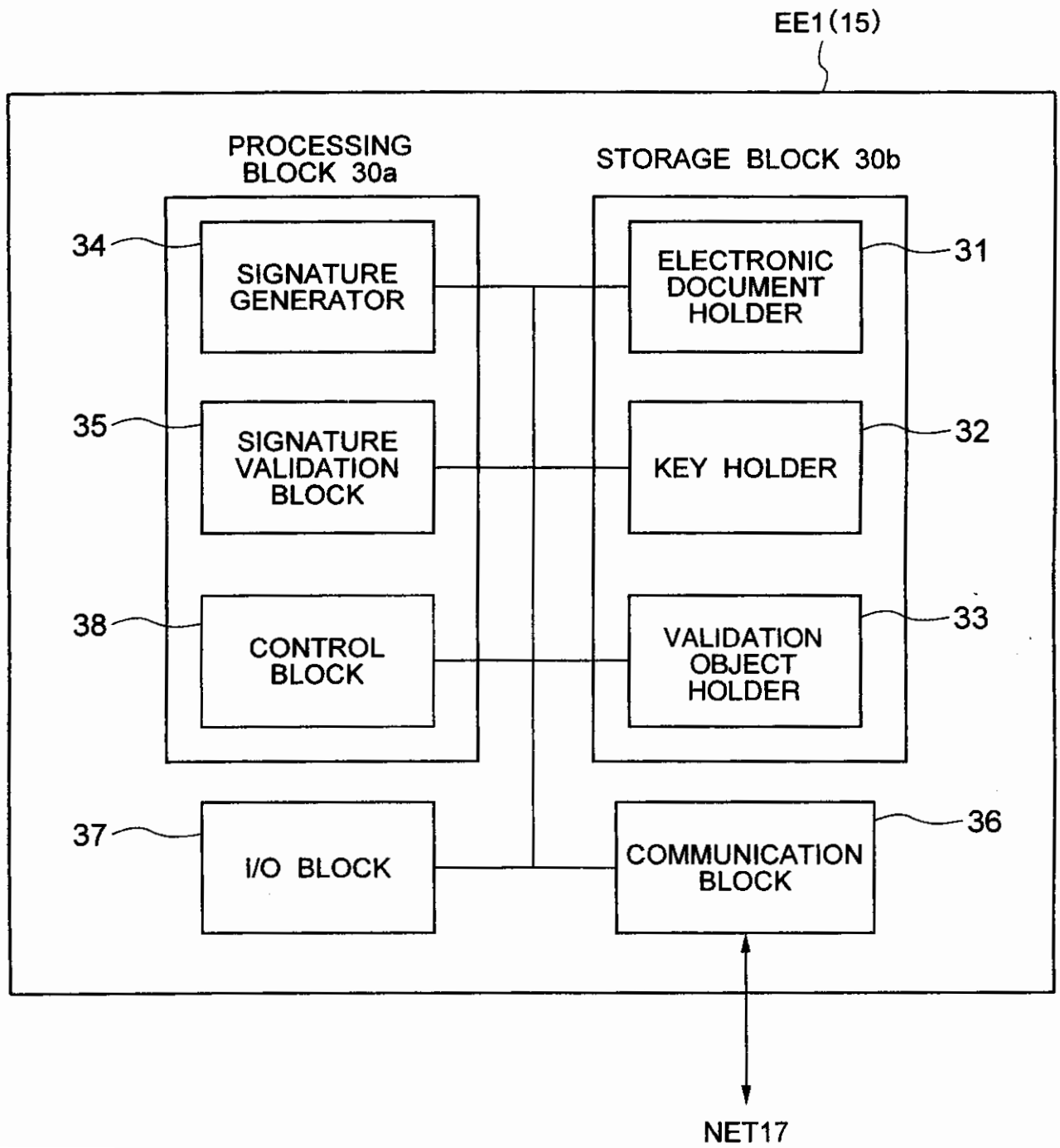

EE1(15)
PROCESSING BLOCK 30a
STORAGE BLOCK 30b
34
SIGNATURE GENERATOR
ELECTRONIC DOCUMENT HOLDER
31
35
SIGNATURE VALIDATION BLOCK
KEY HOLDER
32
38
CONTROL BLOCK
VALIDATION OBJECT HOLDER
33
37
I/O BLOCK
COMMUNICATION BLOCK
36
NET17

FIG. 3

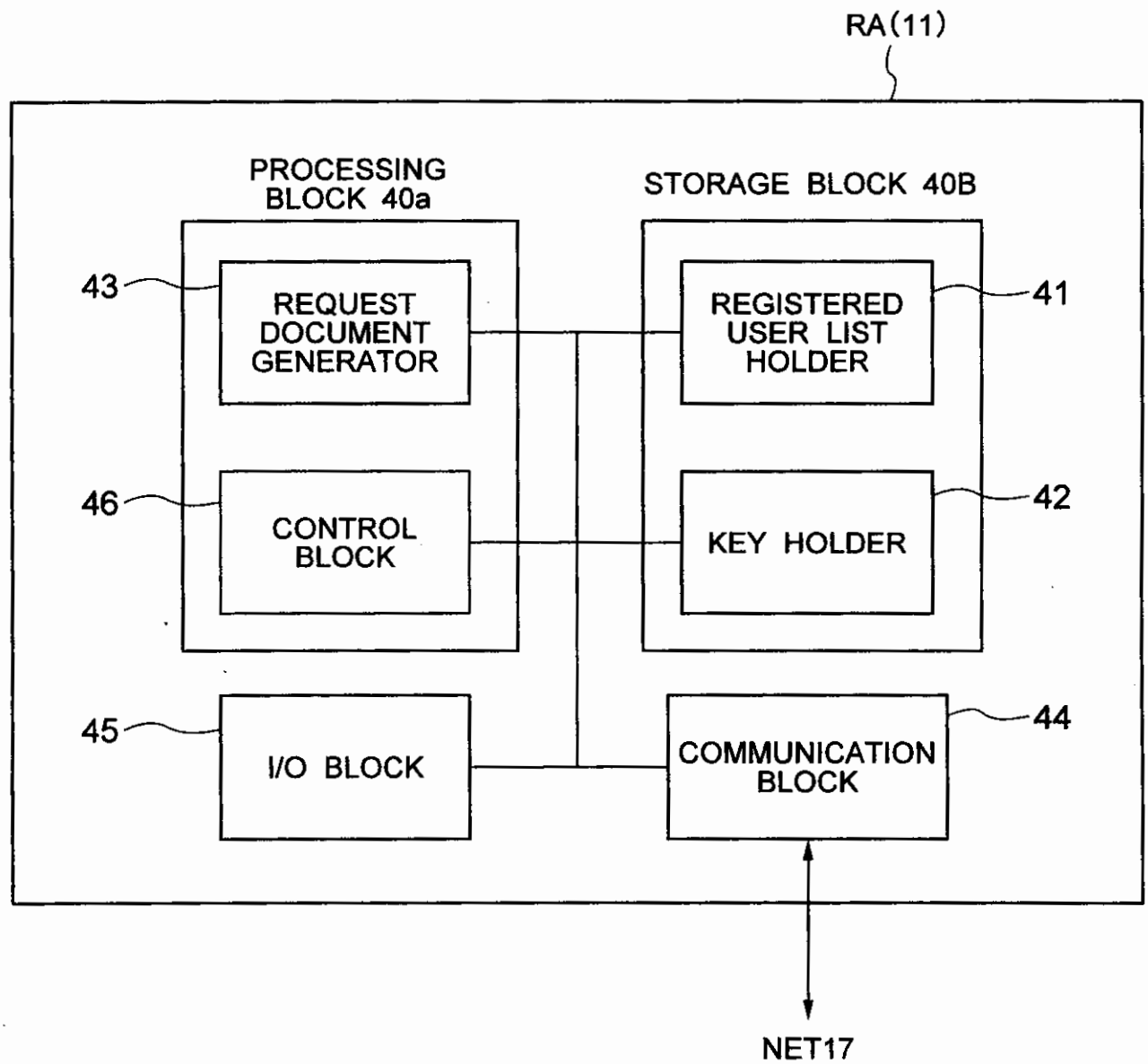

RA(11)
PROCESSING BLOCK 40a
STORAGE BLOCK 40B
43
REQUEST DOCUMENT GENERATOR
REGISTERED USER LIST HOLDER
41
46
CONTROL BLOCK
KEY HOLDER
42
45
I/O BLOCK
COMMUNICATION BLOCK
44
NET17

FIG. 4

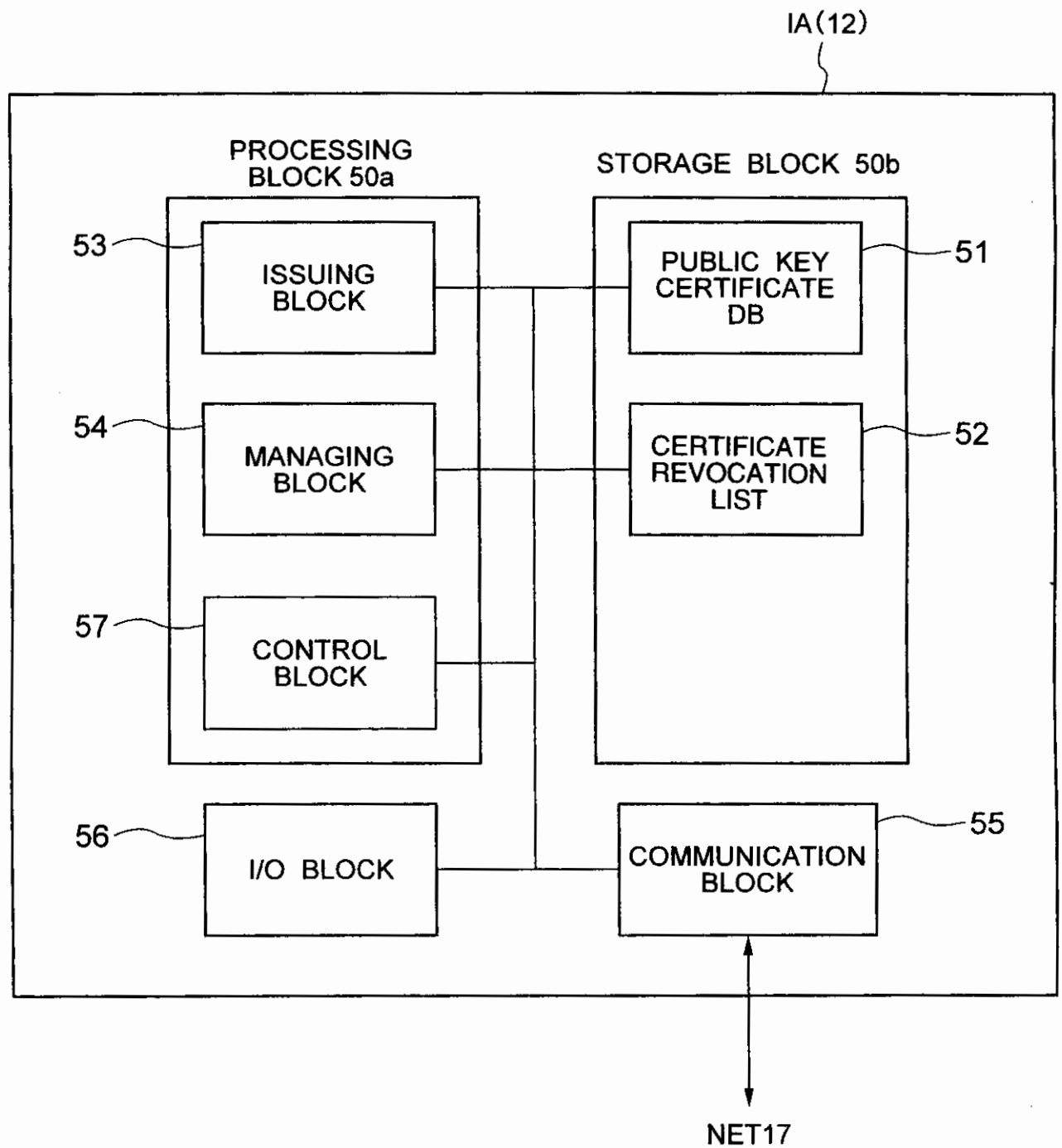

IA(12)
PROCESSING BLOCK 50a
STORAGE BLOCK 50b
53
ISSUING BLOCK
PUBLIC KEY CERTIFICATE DB
51
54
MANAGING BLOCK
CERTIFICATE REVOCATION LIST
52
57
CONTROL BLOCK
56
I/O BLOCK
COMMUNICATION BLOCK
55
NET17

FIG. 5

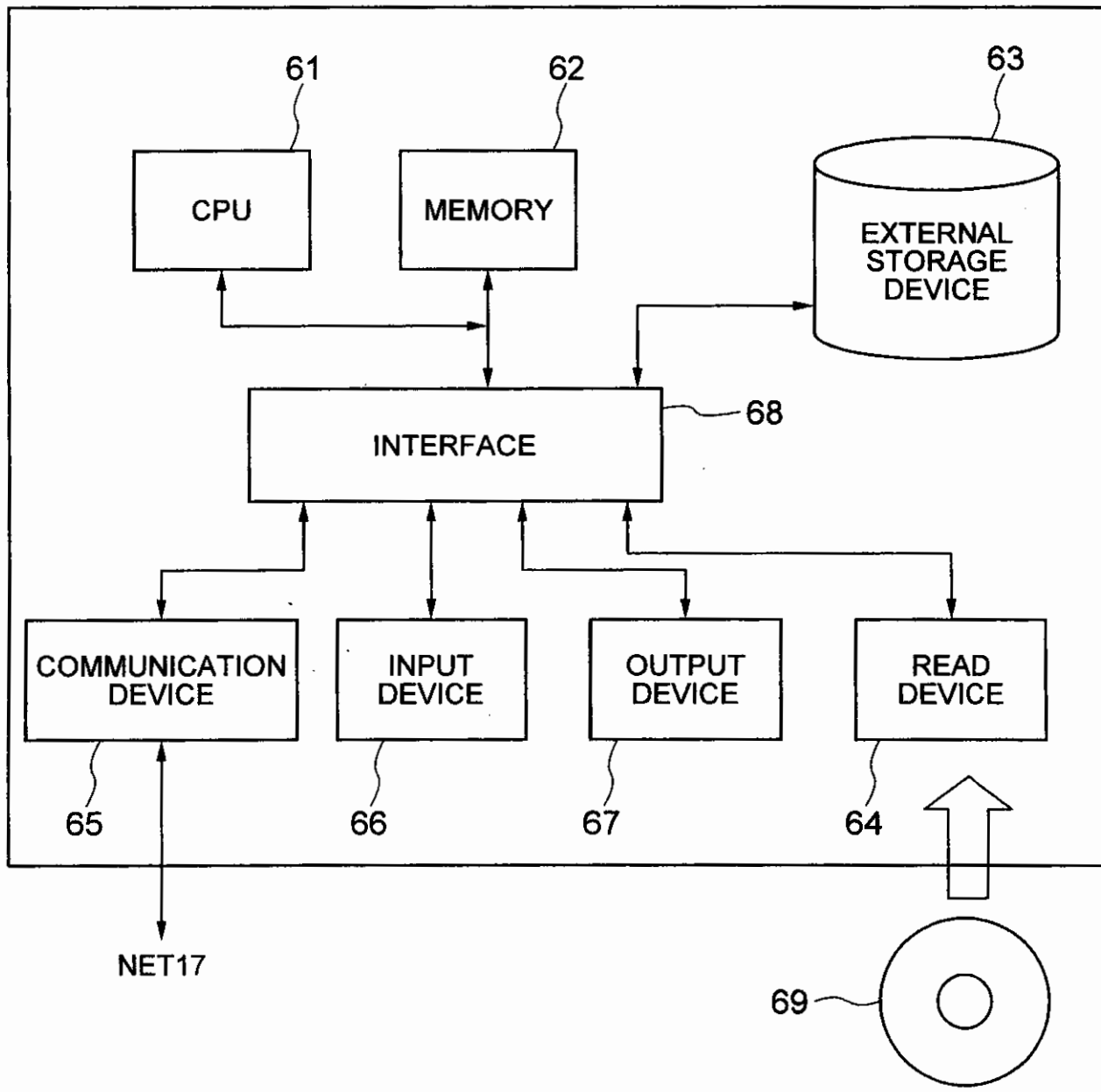

61
62
63
CPU
MEMORY
EXTERNAL STORAGE DEVICE
INTERFACE
68
COMMUNICATION DEVICE
INPUT DEVICE
OUTPUT DEVICE
READ DEVICE
65
66
67
64
NET17
69

FIG. 6

PUBLIC KEY CERTIFICATE ISSUING PROCEDURE

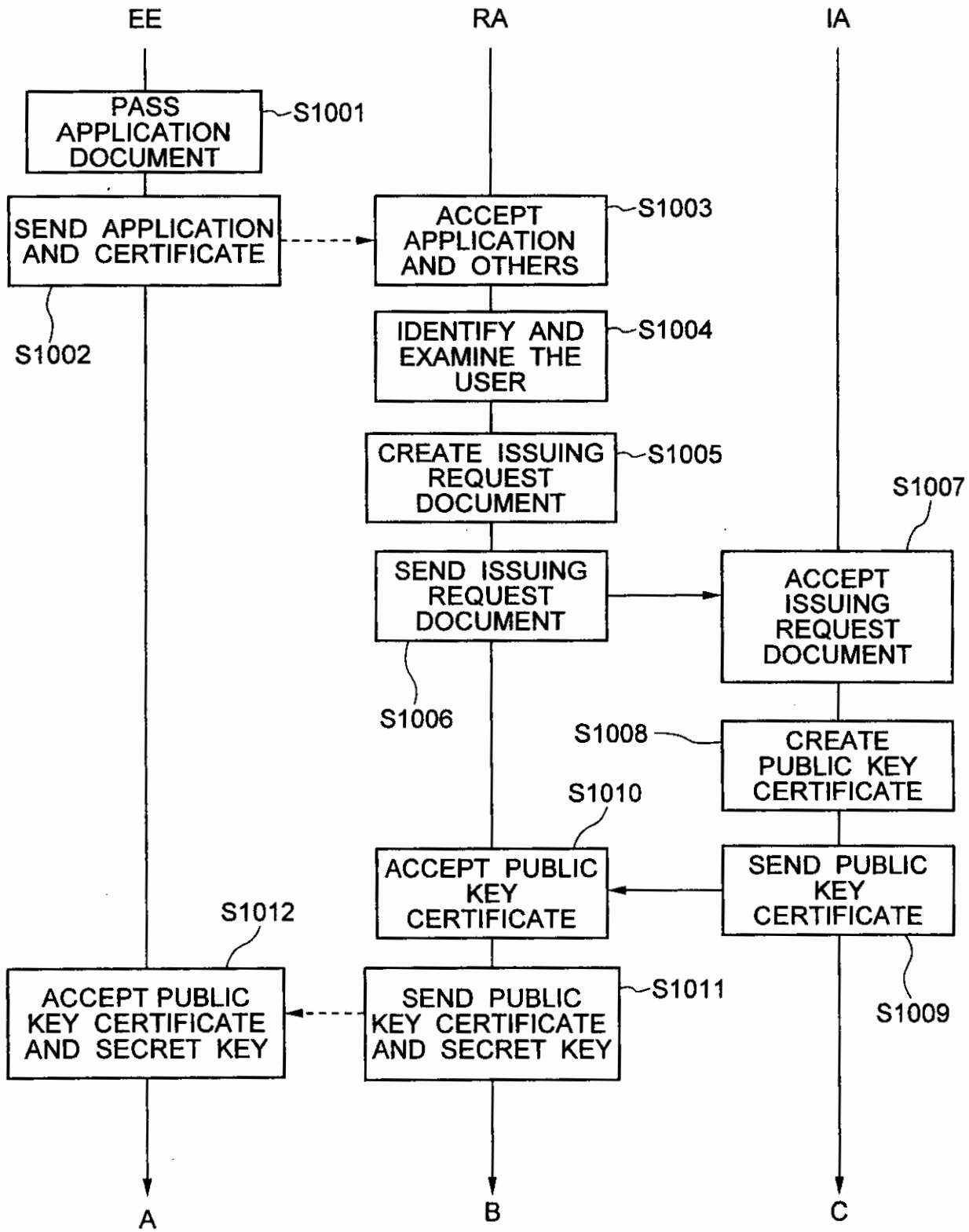


FIG. 7

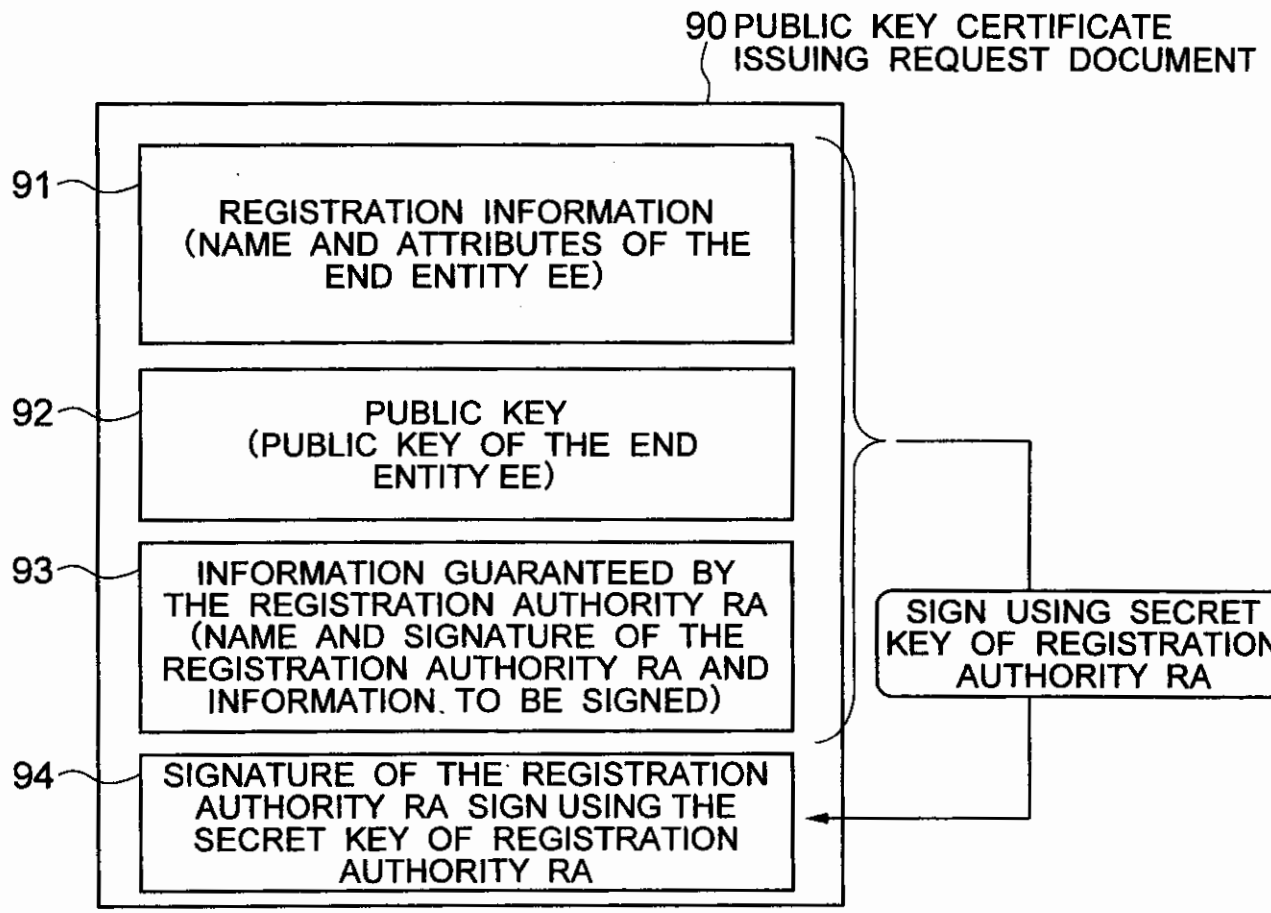

90 PUBLIC KEY CERTIFICATE ISSUING REQUEST DOCUMENT
91
REGISTRATION INFORMATION (NAME AND ATTRIBUTES OF THE END ENTITY EE)
92
PUBLIC KEY (PUBLIC KEY OF THE END ENTITY EE)
93
INFORMATION GUARANTEED BY THE REGISTRATION AUTHORITY RA (NAME AND SIGNATURE OF THE REGISTRATION AUTHORITY RA AND INFORMATION TO BE SIGNED)
94
SIGNATURE OF THE REGISTRATION AUTHORITY RA SIGN USING THE SECRET KEY OF REGISTRATION AUTHORITY RA
SIGN USING SECRET KEY OF REGISTRATION AUTHORITY RA

FIG. 8

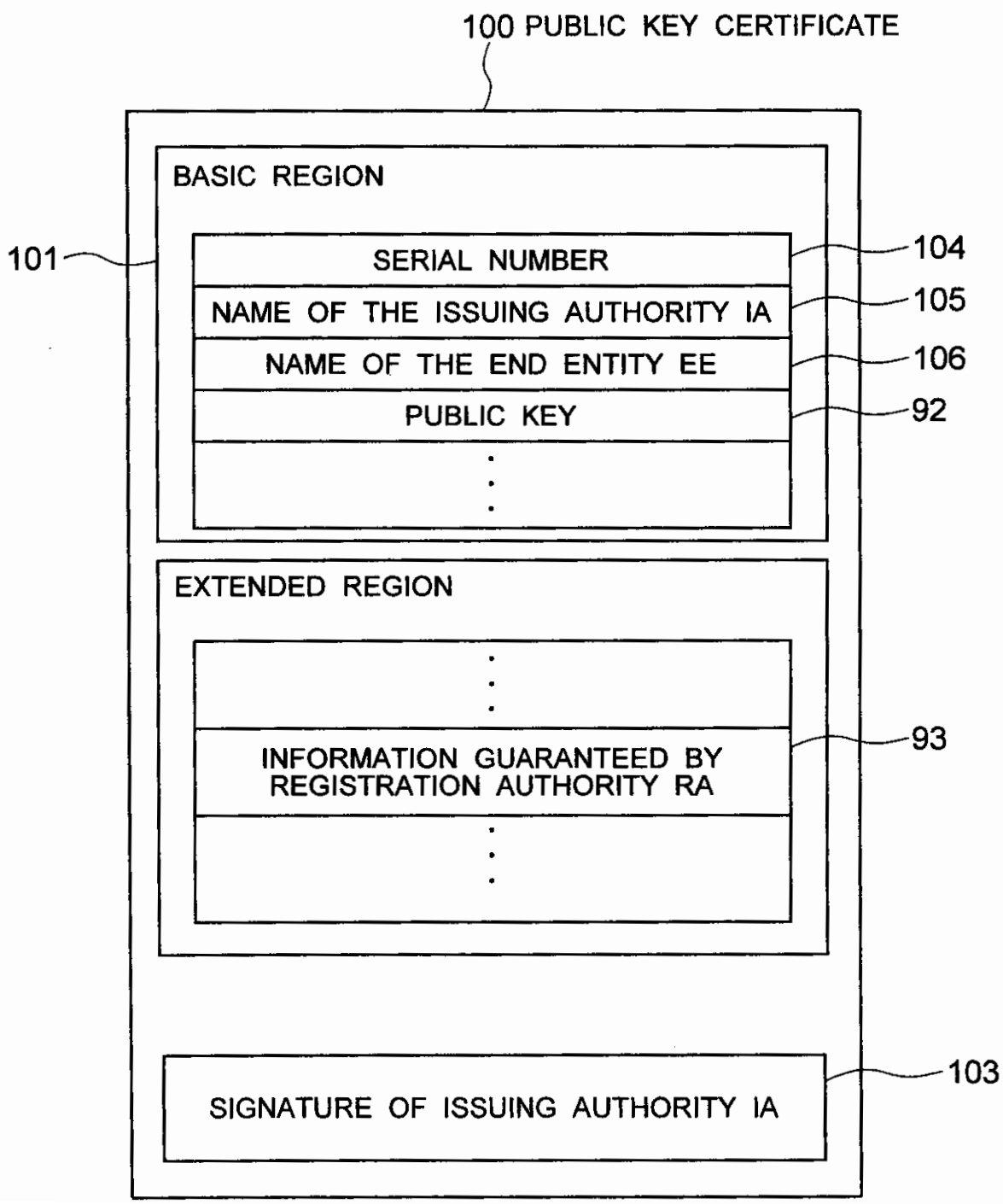

100 PUBLIC KEY CERTIFICATE
BASIC REGION
101
SERIAL NUMBER
NAME OF THE ISSUING AUTHORITY IA
NAME OF THE END ENTITY EE
PUBLIC KEY
104
105
106
92
EXTENDED REGION
INFORMATION GUARANTEED BY REGISTRATION AUTHORITY RA
93
SIGNATURE OF ISSUING AUTHORITY IA
103

FIG. 9

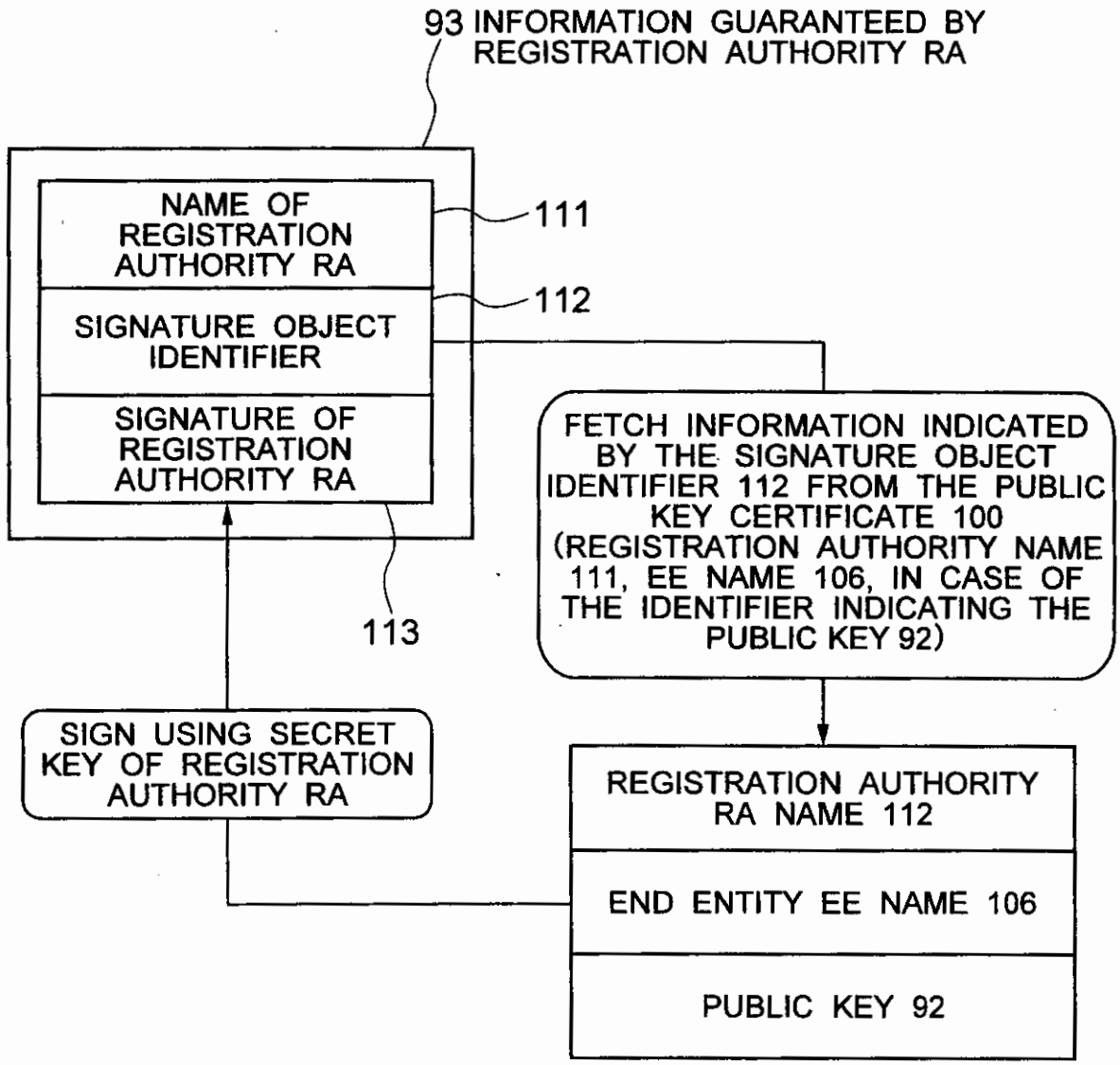

93 INFORMATION GUARANTEED BY REGISTRATION AUTHORITY RA
NAME OF REGISTRATION AUTHORITY RA
111
SIGNATURE OBJECT IDENTIFIER
112
SIGNATURE OF REGISTRATION AUTHORITY RA
113
FETCH INFORMATION INDICATED BY THE SIGNATURE OBJECT IDENTIFIER 112 FROM THE PUBLIC KEY CERTIFICATE 100 (REGISTRATION AUTHORITY NAME 111, EE NAME 106, IN CASE OF THE IDENTIFIER INDICATING THE PUBLIC KEY 92)
SIGN USING SECRET KEY OF REGISTRATION AUTHORITY RA
REGISTRATION AUTHORITY RA NAME 112
END ENTITY EE NAME 106
PUBLIC KEY 92

FIG. 10

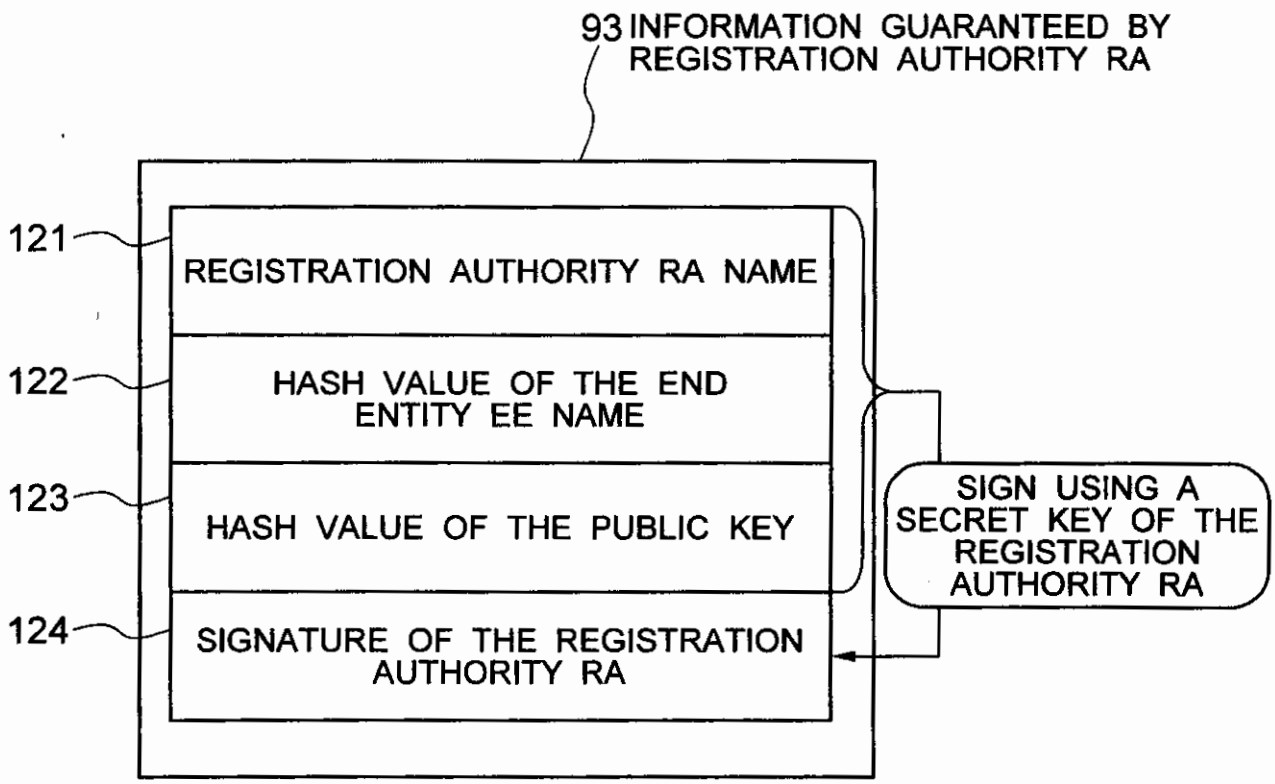

93 INFORMATION GUARANTEED BY REGISTRATION AUTHORITY RA
121
REGISTRATION AUTHORITY RA NAME
122
HASH VALUE OF THE END ENTITY EE NAME
123
HASH VALUE OF THE PUBLIC KEY
124
SIGNATURE OF THE REGISTRATION AUTHORITY RA
SIGN USING A SECRET KEY OF THE REGISTRATION AUTHORITY RA

FIG. 11

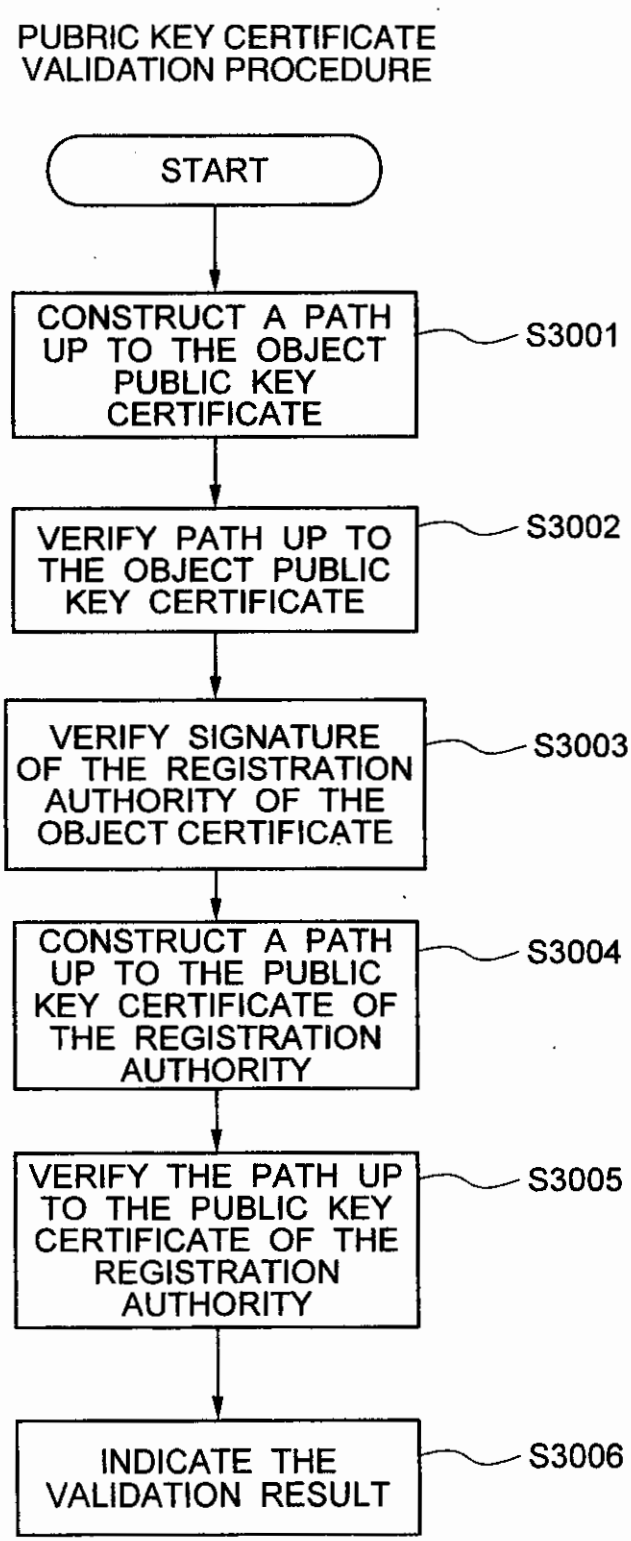

PUBRIC KEY CERTIFICATE VALIDATION PROCEDURE
START
CONSTRUCT A PATH UP TO THE OBJECT PUBLIC KEY CERTIFICATE
S3001
VERIFY PATH UP TO THE OBJECT PUBLIC KEY CERTIFICATE
S3002
VERIFY SIGNATURE OF THE REGISTRATION AUTHORITY OF THE OBJECT CERTIFICATE
S3003
CONSTRUCT A PATH UP TO THE PUBLIC KEY CERTIFICATE OF THE REGISTRATION AUTHORITY
S3004
VERIFY THE PATH UP TO THE PUBLIC KEY CERTIFICATE OF THE REGISTRATION AUTHORITY
S3005
INDICATE THE VALIDATION RESULT
S3006

FIG. 12

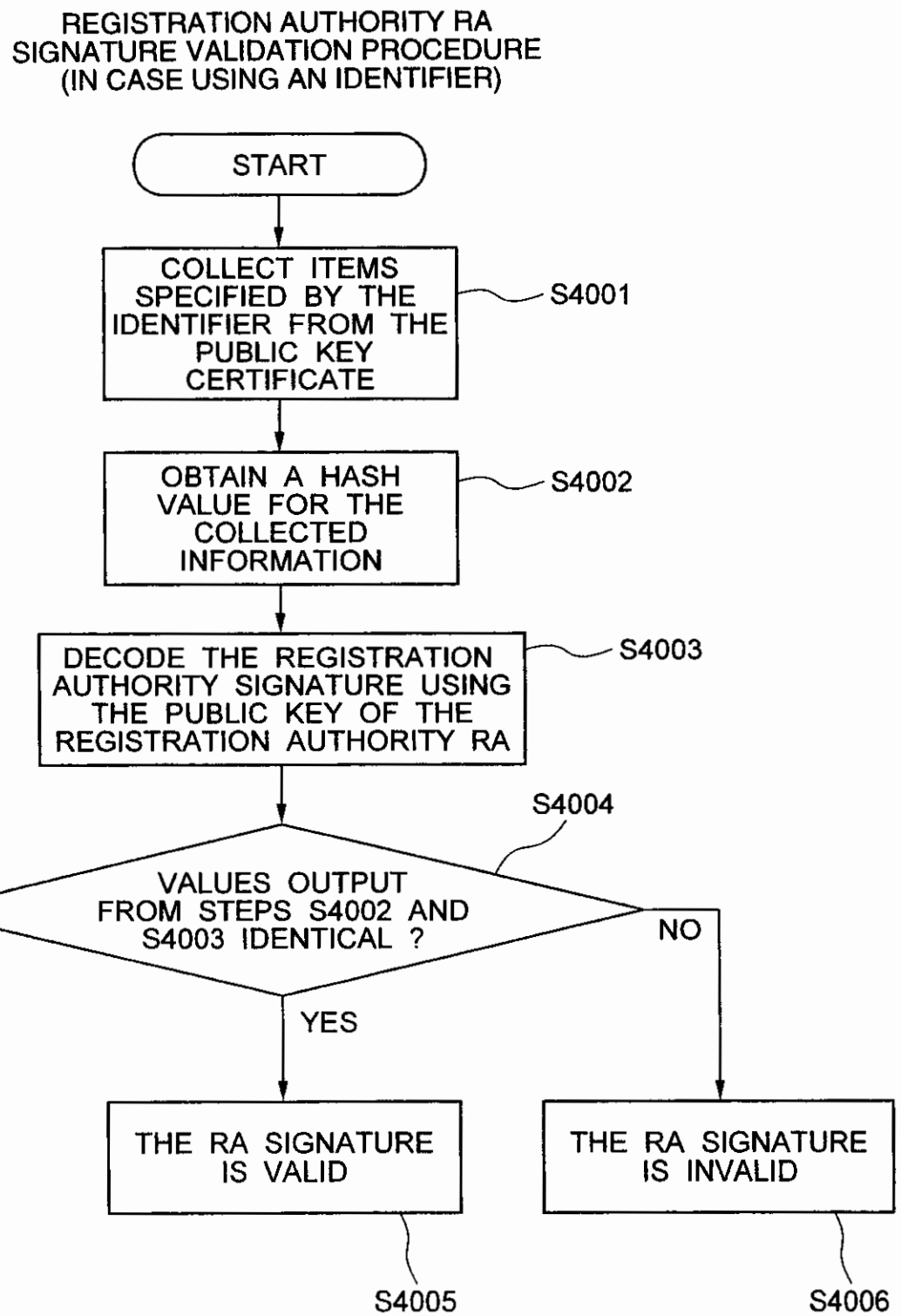

REGISTRATION AUTHORITY RA
SIGNATURE VALIDATION PROCEDURE
(IN CASE USING AN IDENTIFIER)
START
COLLECT ITEMS SPECIFIED BY THE IDENTIFIER FROM THE PUBLIC KEY CERTIFICATE
S4001
OBTAIN A HASH VALUE FOR THE COLLECTED INFORMATION
S4002
DECODE THE REGISTRATION AUTHORITY SIGNATURE USING THE PUBLIC KEY OF THE REGISTRATION AUTHORITY RA
S4003
S4004
VALUES OUTPUT FROM STEPS S4002 AND S4003 IDENTICAL ?
NO
YES
THE RA SIGNATURE IS VALID
THE RA SIGNATURE IS INVALID
S4005
S4006

FIG. 13

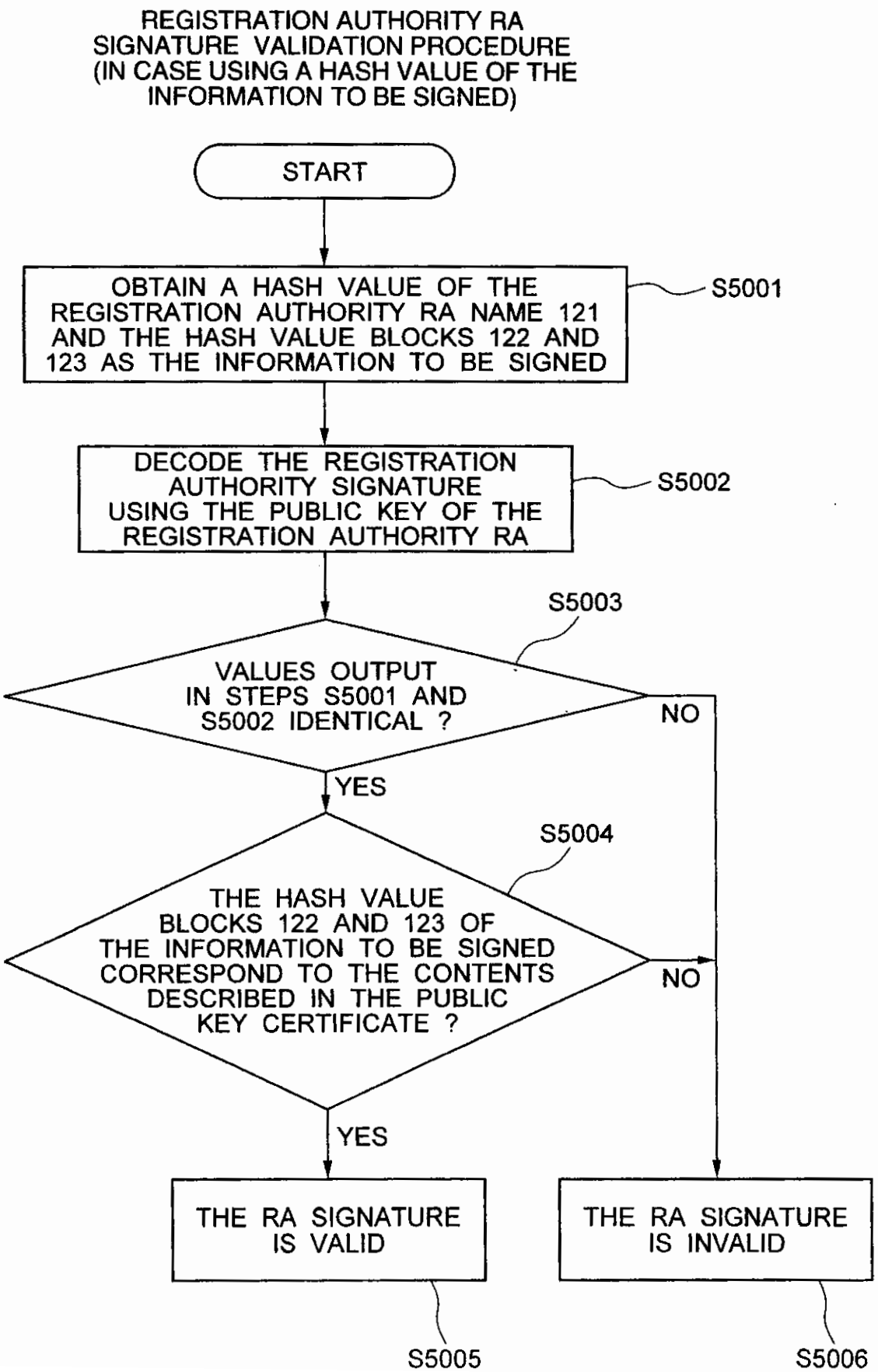

REGISTRATION AUTHORITY RA SIGNATURE VALIDATION PROCEDURE (IN CASE USING A HASH VALUE OF THE INFORMATION TO BE SIGNED)
START
OBTAIN A HASH VALUE OF THE REGISTRATION AUTHORITY RA NAME 121 AND THE HASH VALUE BLOCKS 122 AND 123 AS THE INFORMATION TO BE SIGNED
S5001
DECODE THE REGISTRATION AUTHORITY SIGNATURE USING THE PUBLIC KEY OF THE REGISTRATION AUTHORITY RA
S5002
S5003
VALUES OUTPUT IN STEPS S5001 AND S5002 IDENTICAL ?
NO
YES
S5004
THE HASH VALUE BLOCKS 122 AND 123 OF THE INFORMATION TO BE SIGNED CORRESPOND TO THE CONTENTS DESCRIBED IN THE PUBLIC KEY CERTIFICATE ?
NO
YES
THE RA SIGNATURE IS VALID
THE RA SIGNATURE IS INVALID
S5005
S5006

FIG. 14

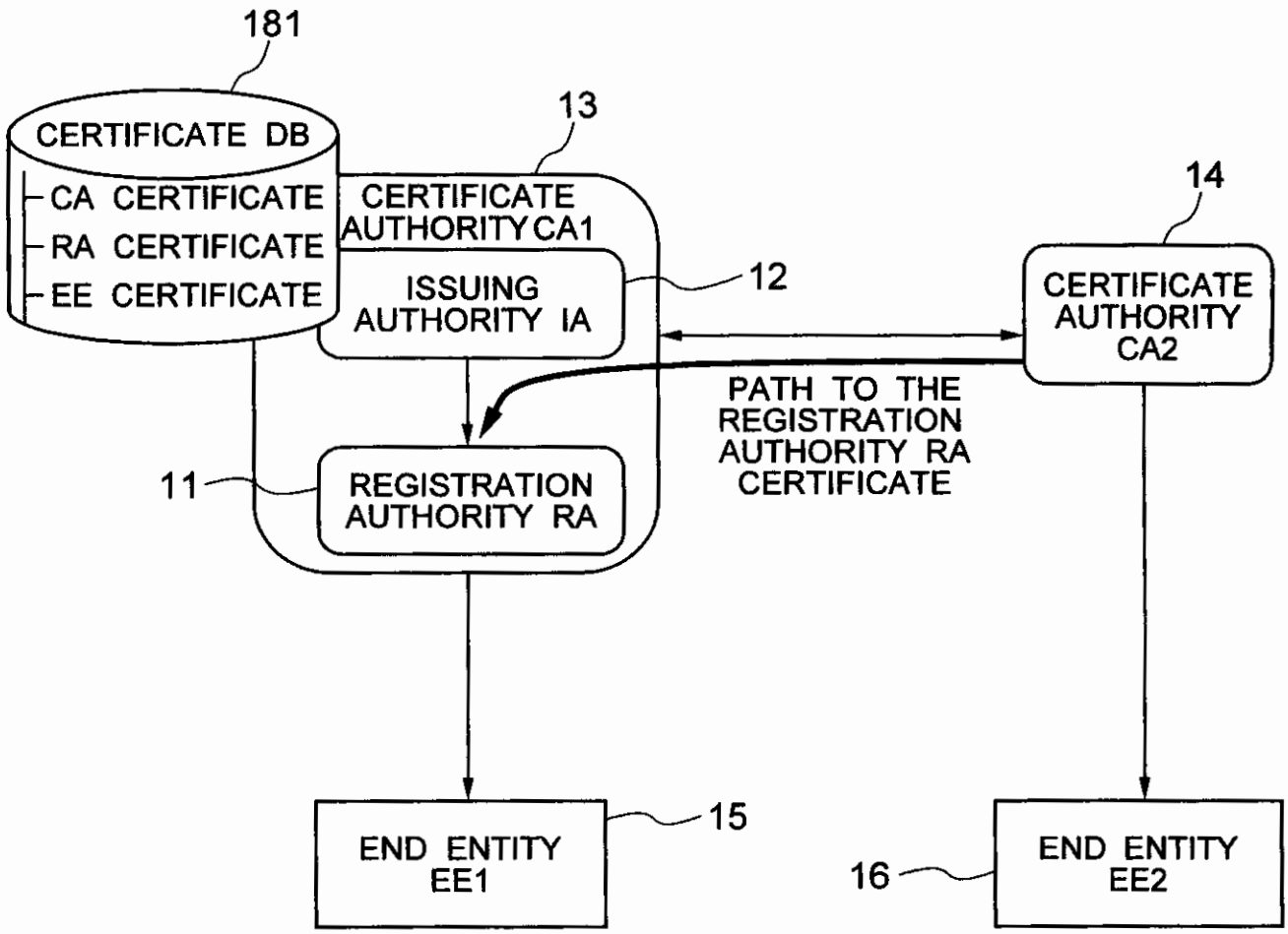
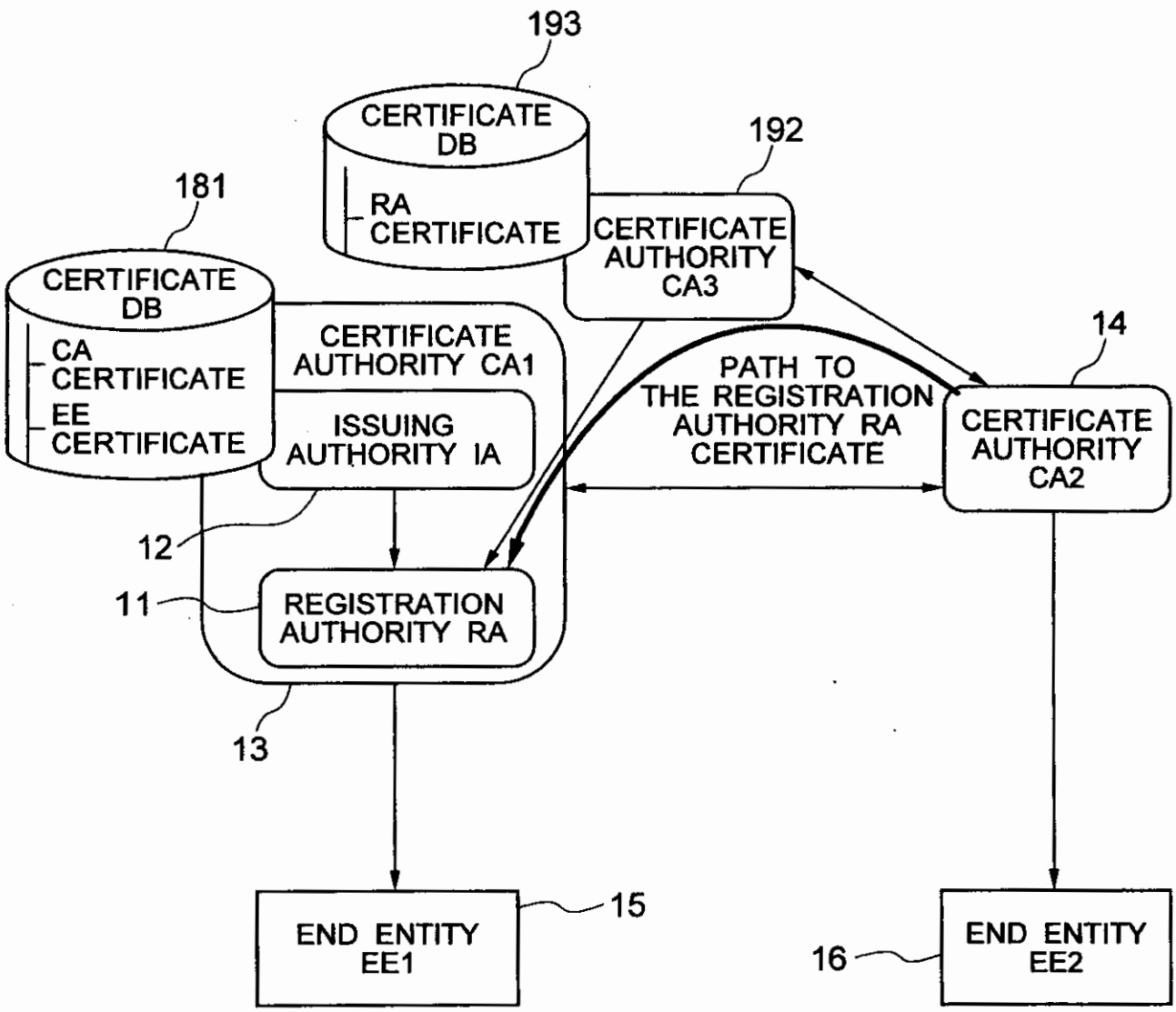

181
CERTIFICATE DB
CA CERTIFICATE
RA CERTIFICATE
EE CERTIFICATE
13
CERTIFICATE AUTHORITY CA1
ISSUING AUTHORITY IA
12
14
CERTIFICATE AUTHORITY CA2
PATH TO THE REGISTRATION AUTHORITY RA CERTIFICATE
11
REGISTRATION AUTHORITY RA
END ENTITY EE1
15
16
END ENTITY EE2

FIG. 15


193
CERTIFICATE DB
RA CERTIFICATE
192
CERTIFICATE AUTHORITY CA3
181
CERTIFICATE DB
CA CERTIFICATE
EE CERTIFICATE
CERTIFICATE AUTHORITY CA1
ISSUING AUTHORITY IA
PATH TO THE REGISTRATION AUTHORITY RA CERTIFICATE
14
CERTIFICATE AUTHORITY CA2
12
11
REGISTRATION AUTHORITY RA
13
END ENTITY EE1
15
16
END ENTITY EE2