FIG.1

PKI SYSTEM

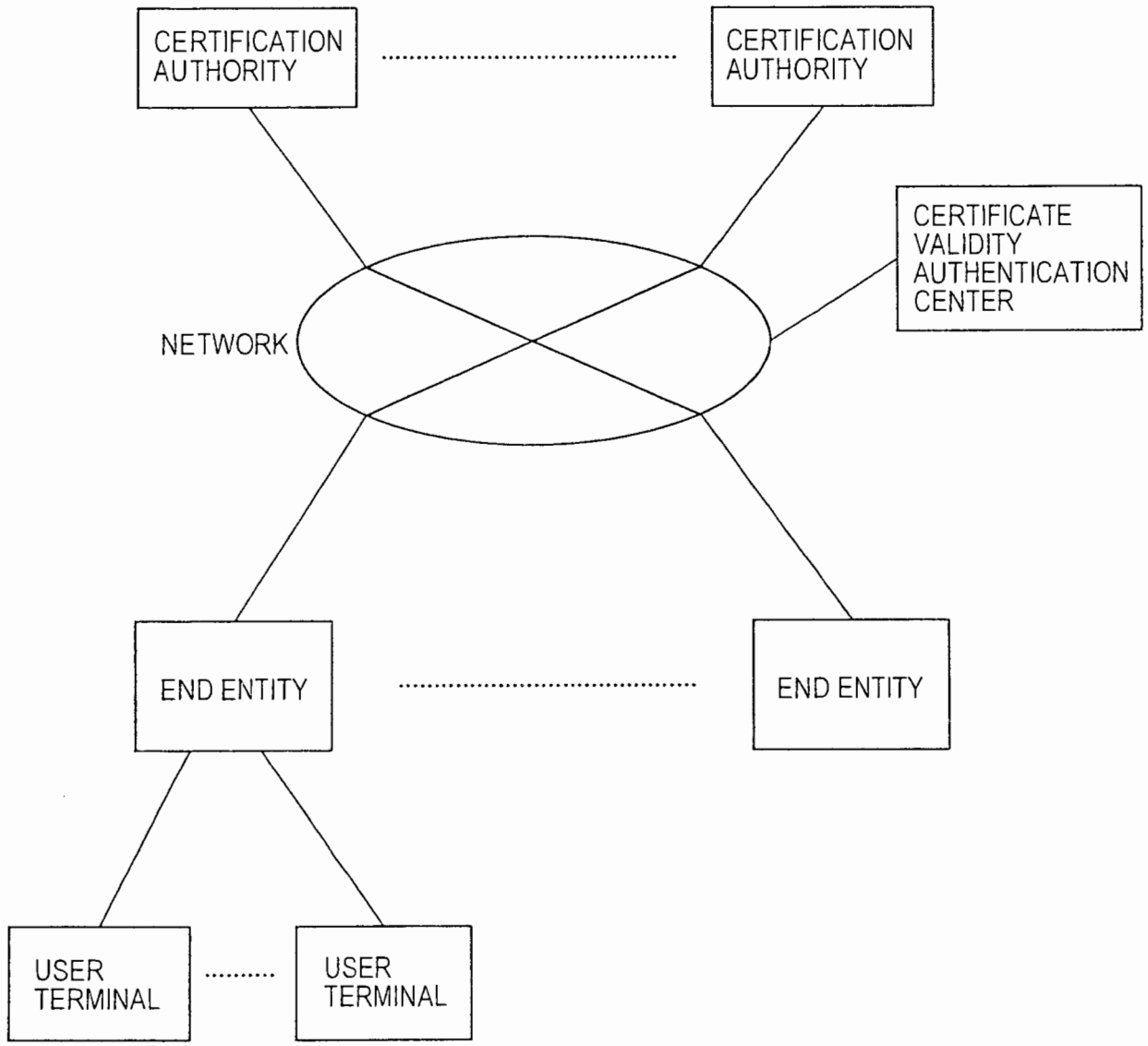
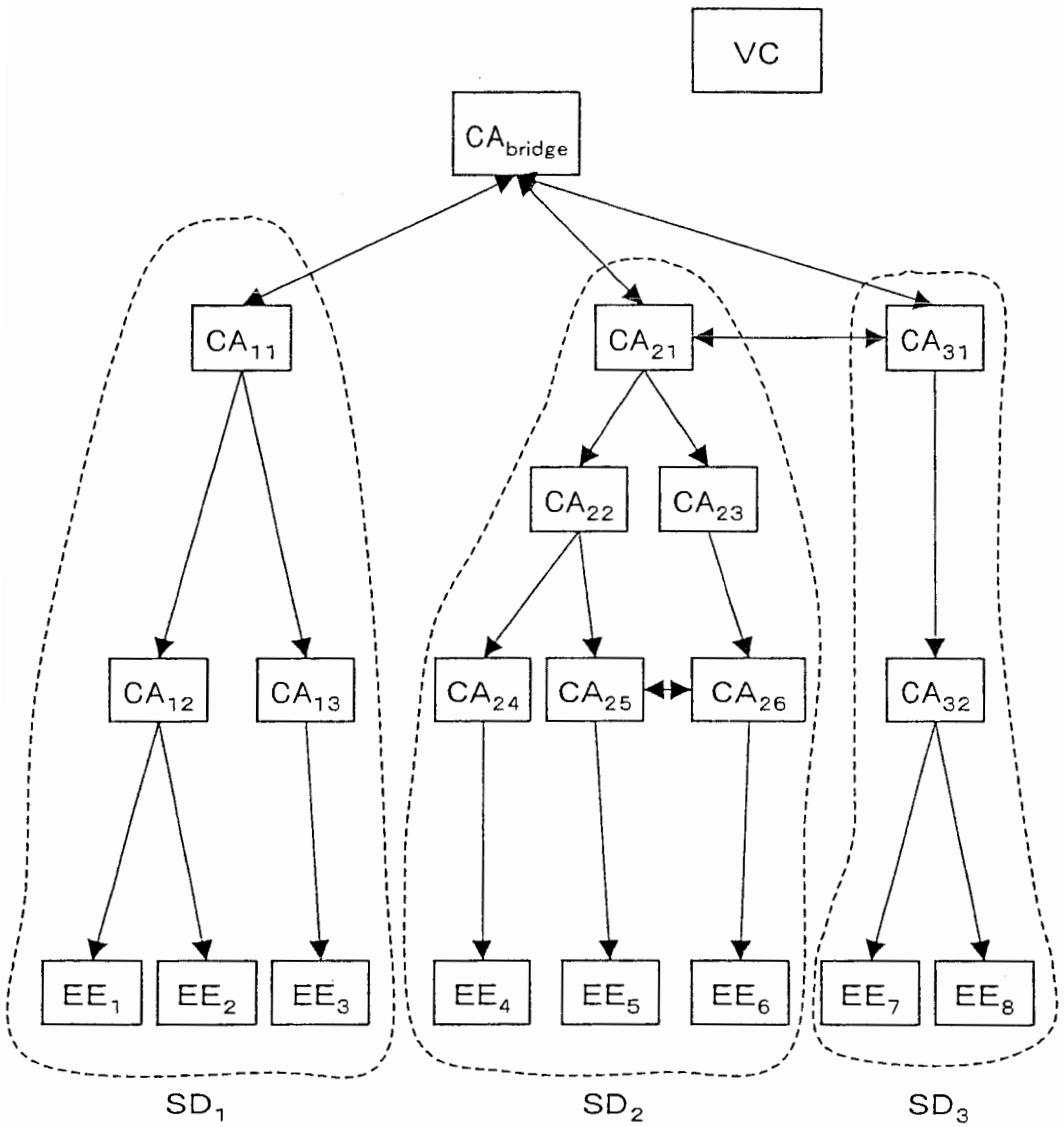


FIG.2



⟶ : FLOW OF PUBLIC KEY CERTIFICATE

CA : CERTIFICATION AUTHORITY

EE : END ENTITY

VC : CERTIFICATE VALIDITY AUTHENTICATION CENTER

SD : SECURITY DOMAIN

FIG.3

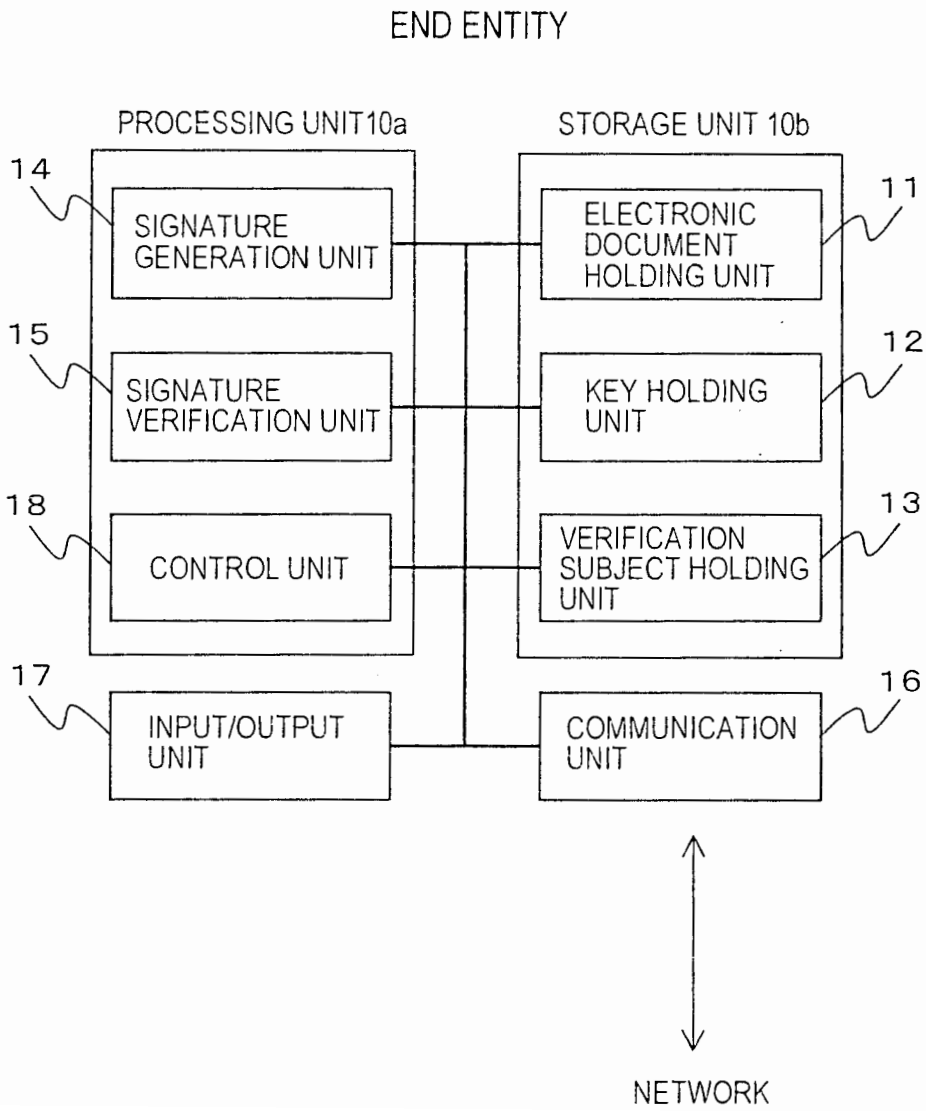

END ENTITY
PROCESSING UNIT10a
STORAGE UNIT 10b
14
SIGNATURE GENERATION UNIT
15
SIGNATURE VERIFICATION UNIT
18
CONTROL UNIT
17
INPUT/OUTPUT UNIT
11
ELECTRONIC DOCUMENT HOLDING UNIT
12
KEY HOLDING UNIT
13
VERIFICATION SUBJECT HOLDING UNIT
16
COMMUNICATION UNIT
NETWORK

FIG.4

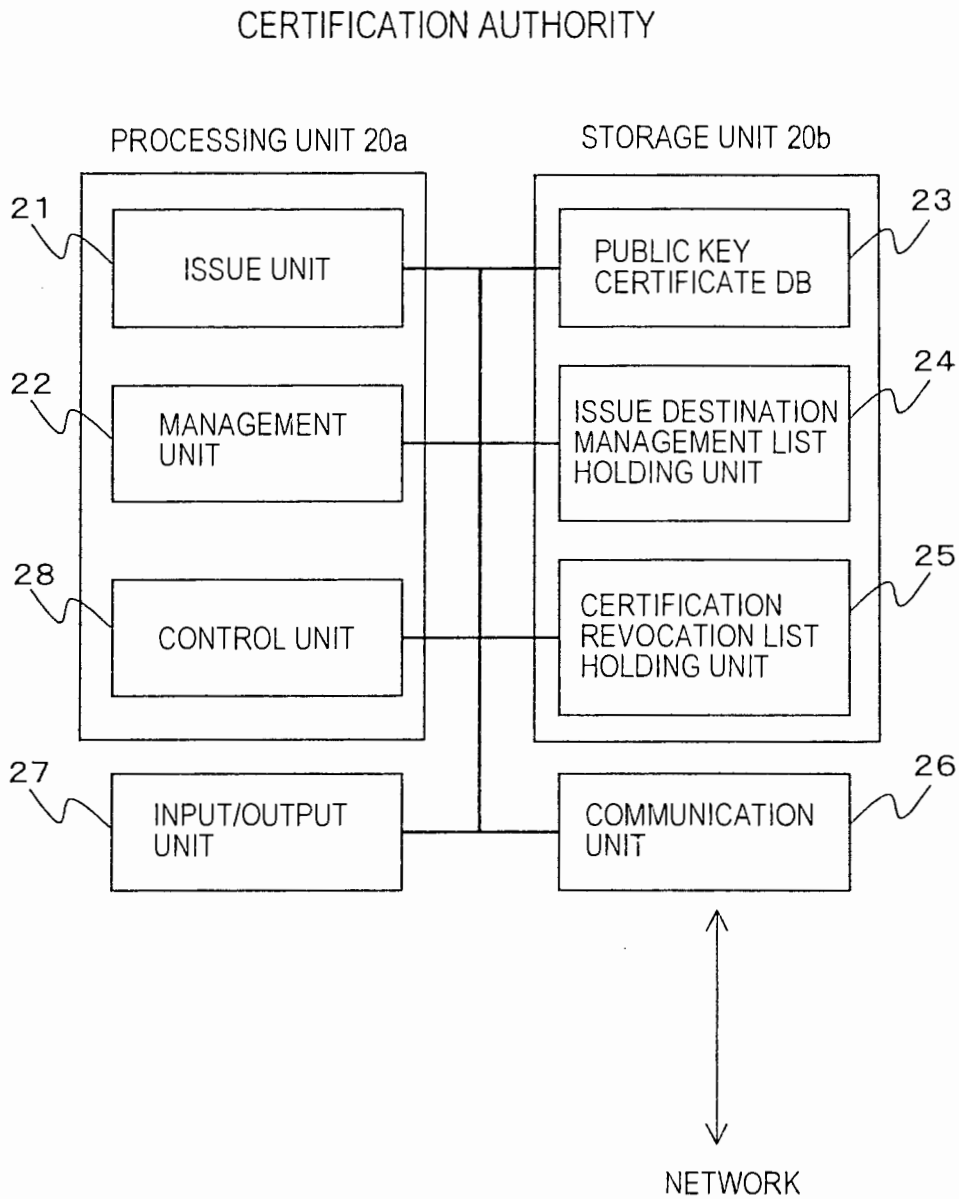

CERTIFICATION AUTHORITY
PROCESSING UNIT 20a
STORAGE UNIT 20b
21
ISSUE UNIT
22
MANAGEMENT UNIT
28
CONTROL UNIT
27
INPUT/OUTPUT UNIT
23
PUBLIC KEY CERTIFICATE DB
24
ISSUE DESTINATION MANAGEMENT LIST HOLDING UNIT
25
CERTIFICATION REVOCATION LIST HOLDING UNIT
26
COMMUNICATION UNIT
NETWORK

FIG.5

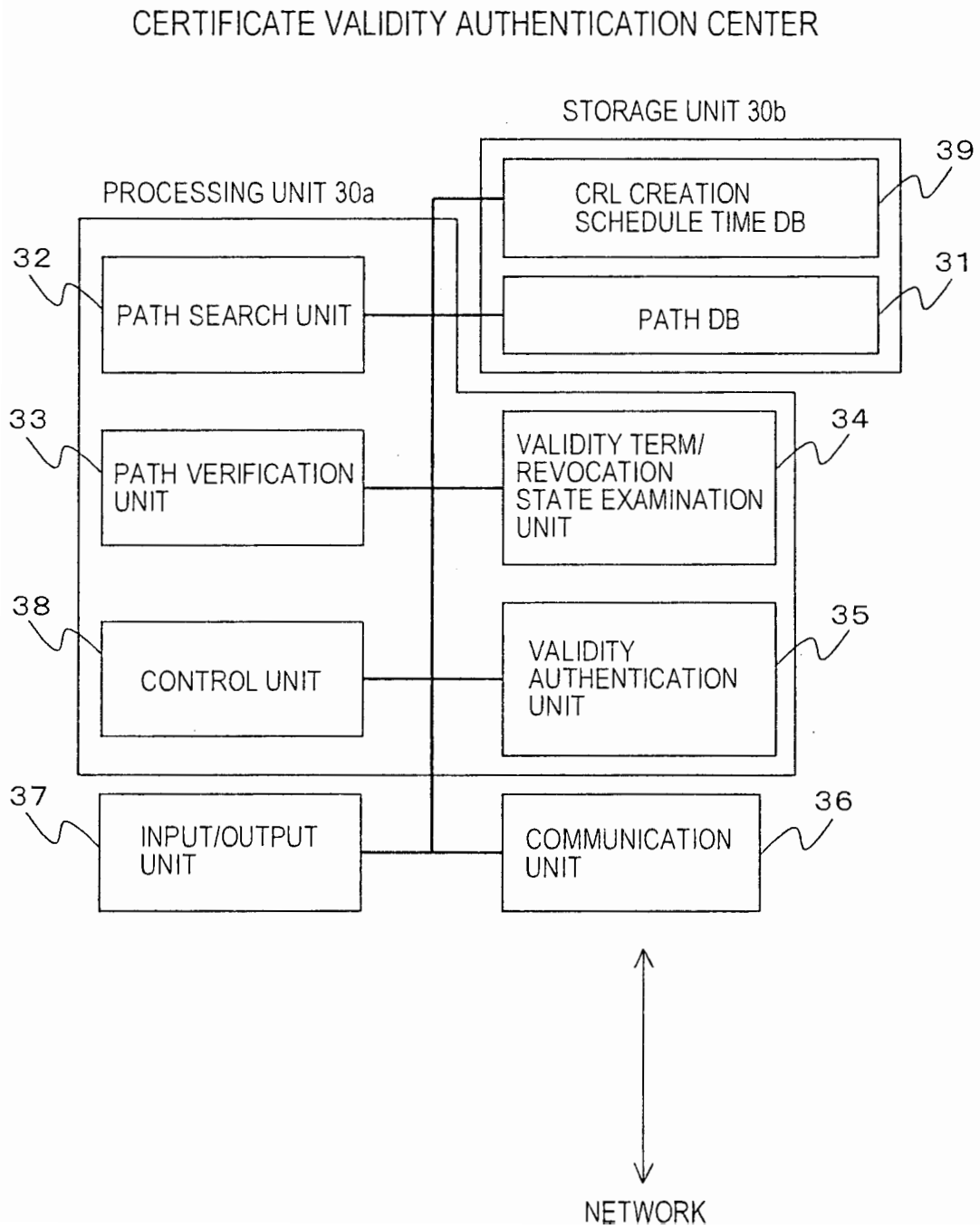

CERTIFICATE VALIDITY AUTHENTICATION CENTER
STORAGE UNIT 30b
39
CRL CREATION SCHEDULE TIME DB
PROCESSING UNIT 30a
32
PATH SEARCH UNIT
31
PATH DB
33
PATH VERIFICATION UNIT
34
VALIDITY TERM/ REVOCATION STATE EXAMINATION UNIT
38
CONTROL UNIT
35
VALIDITY AUTHENTICATION UNIT
37
INPUT/OUTPUT UNIT
36
COMMUNICATION UNIT
NETWORK

FIG.6

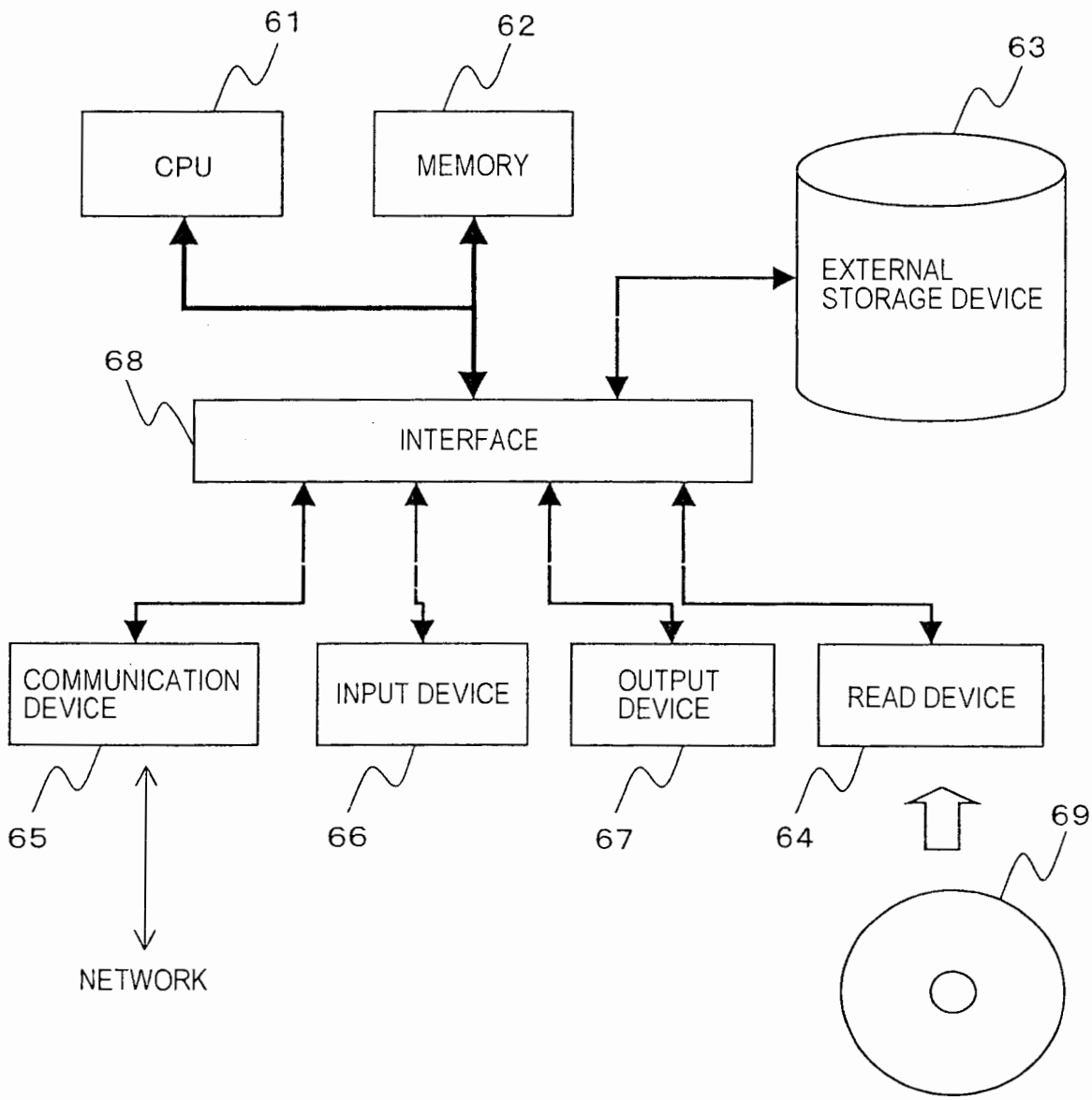

61
62
63
CPU
MEMORY
EXTERNAL STORAGE DEVICE
68
INTERFACE
COMMUNICATION DEVICE
INPUT DEVICE
OUTPUT DEVICE
READ DEVICE
65
66
67
64
69
NETWORK

FIG.7

OPERATION OF SEARCHING FOR, VERIFYING AND MANAGING PATHS

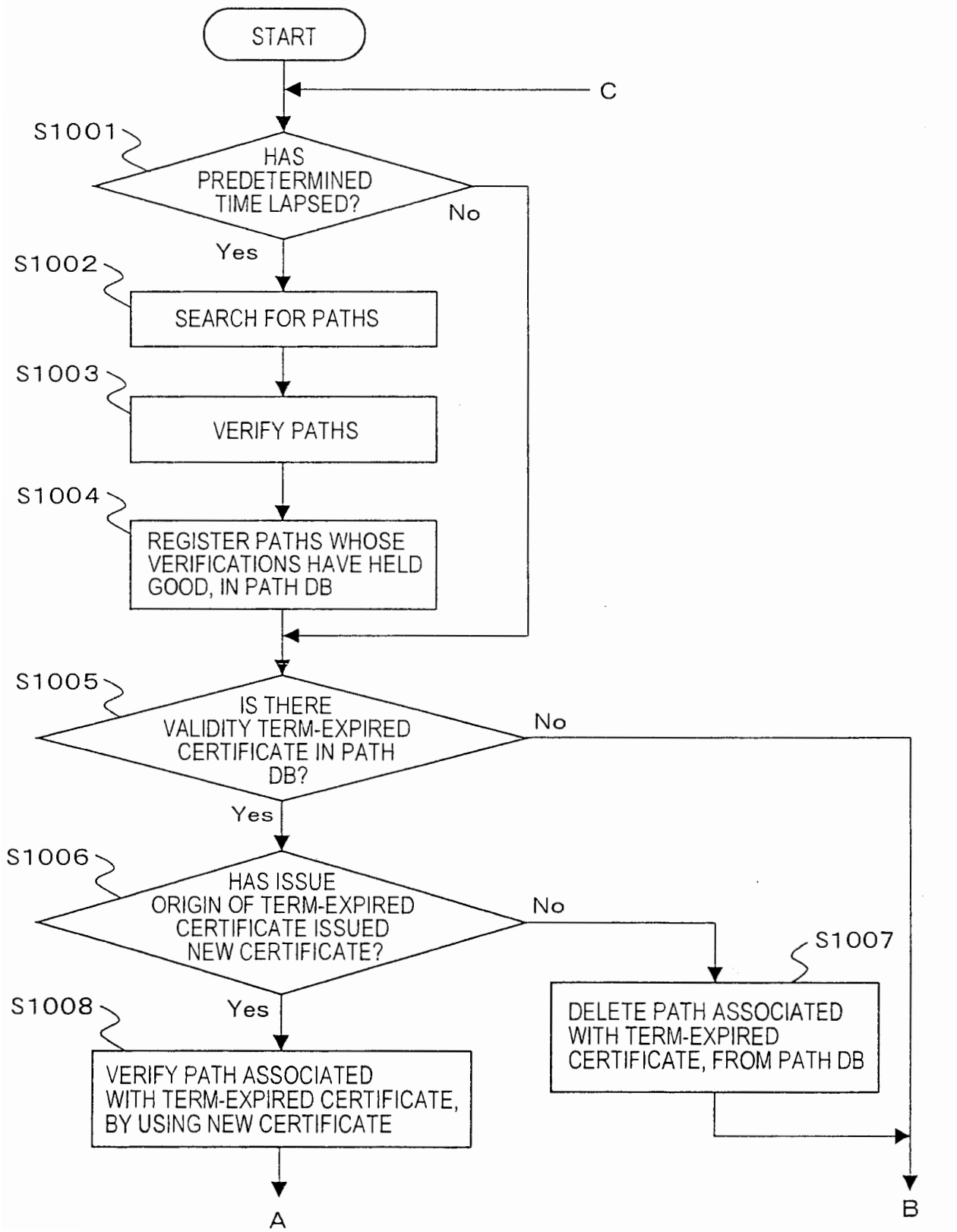


FIG.8

OPERATION OF SEARCHING FOR, VERIFYING AND MANAGING PATHS

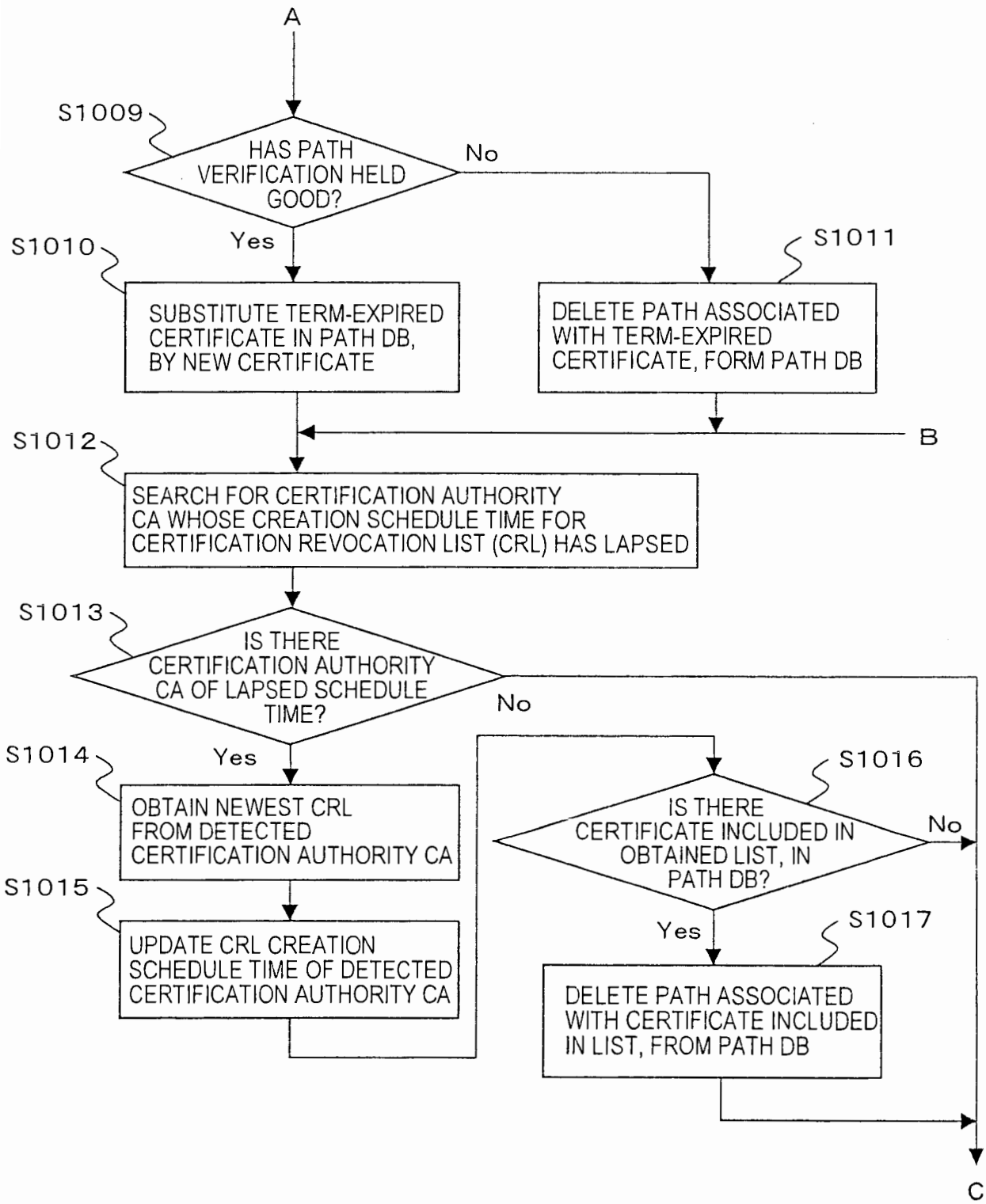


FIG.9

PATH SEARCH RESULT (IN CASE OF FIG. 2)

TERMINAL ADMITTING CERTIFICATION AUTHORITY	PATH
CA_{12}	CA_{bride}-CA_{11}-CA_{12}
CA_{13}	CA_{bride}-CA_{11}-CA_{13}
CA_{24}	CA_{bride}-CA_{21}-CA_{22}-CA_{24}
	CA_{bride}-CA_{31}-CA_{21}-CA_{22}-CA_{24}
CA_{25}	CA_{bride}-CA_{21}-CA_{22}-CA_{25}
	CA_{bride}-CA_{21}-CA_{23}-CA_{26}-CA_{25}
	CA_{bride}-CA_{31}-CA_{21}-CA_{22}-CA_{25}
	CA_{bride}-CA_{31}-CA_{21}-CA_{23}-CA_{26}-CA_{25}
CA_{26}	CA_{bride}-CA_{21}-CA_{23}-CA_{26}
	CA_{bride}-CA_{21}-CA_{22}-CA_{25}-CA_{26}
	CA_{bride}-CA_{31}-CA_{21}-CA_{23}-CA_{26}
	CA_{bride}-CA_{31}-CA_{21}-CA_{22}-CA_{25}-CA_{26}
CA_{32}	CA_{bride}-CA_{31}-CA_{32}
	CA_{bride}-CA_{21}-CA_{31}-CA_{32}

FIG.10

OPERATION OF AUTHENTICATING VALIDITY OF PUBLIC KEY CERTIFICATE

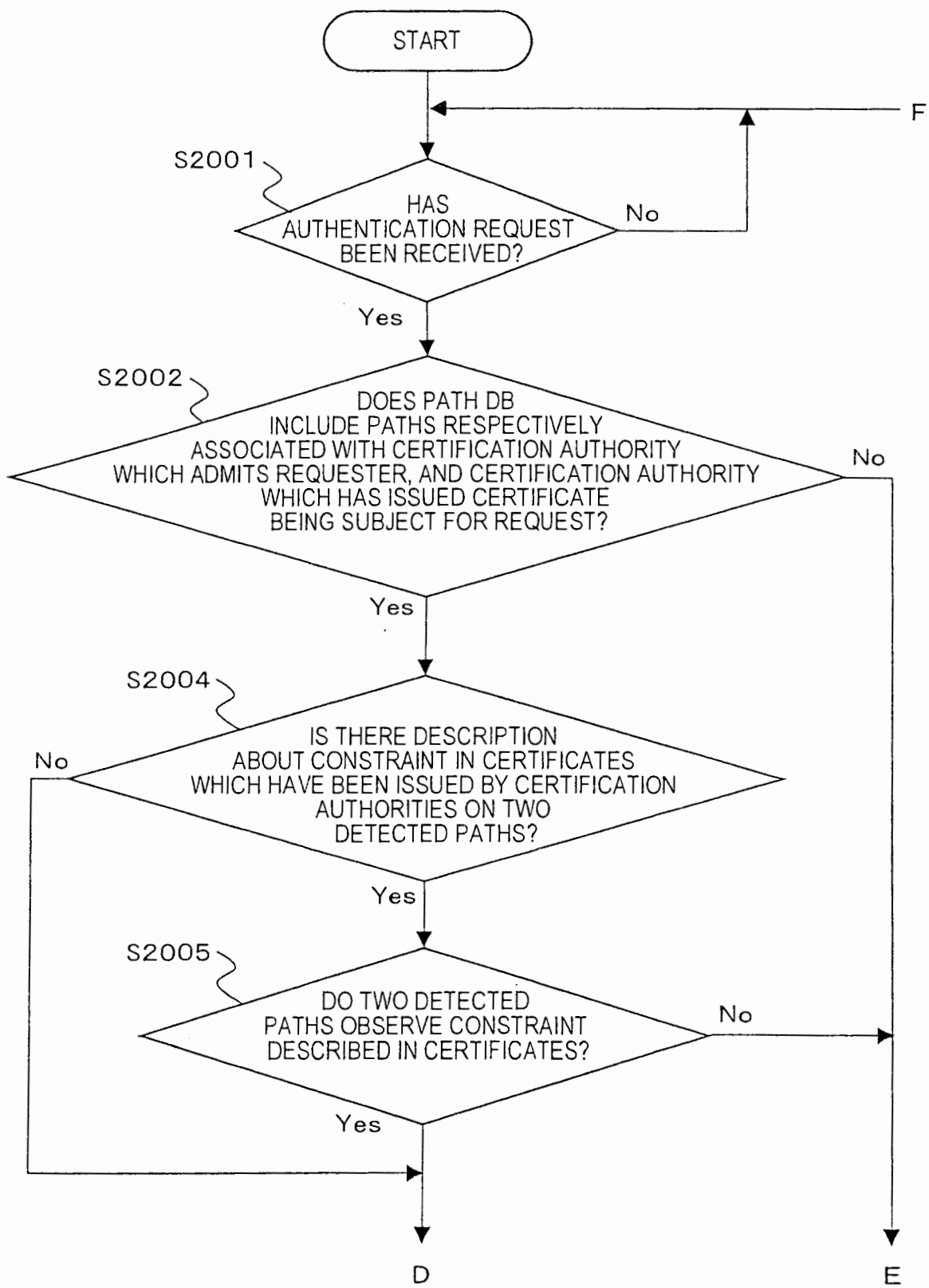


FIG.11

OPERATION OF AUTHENTICATING VALIDITY OF PUBLIC KEY CERTIFICATE

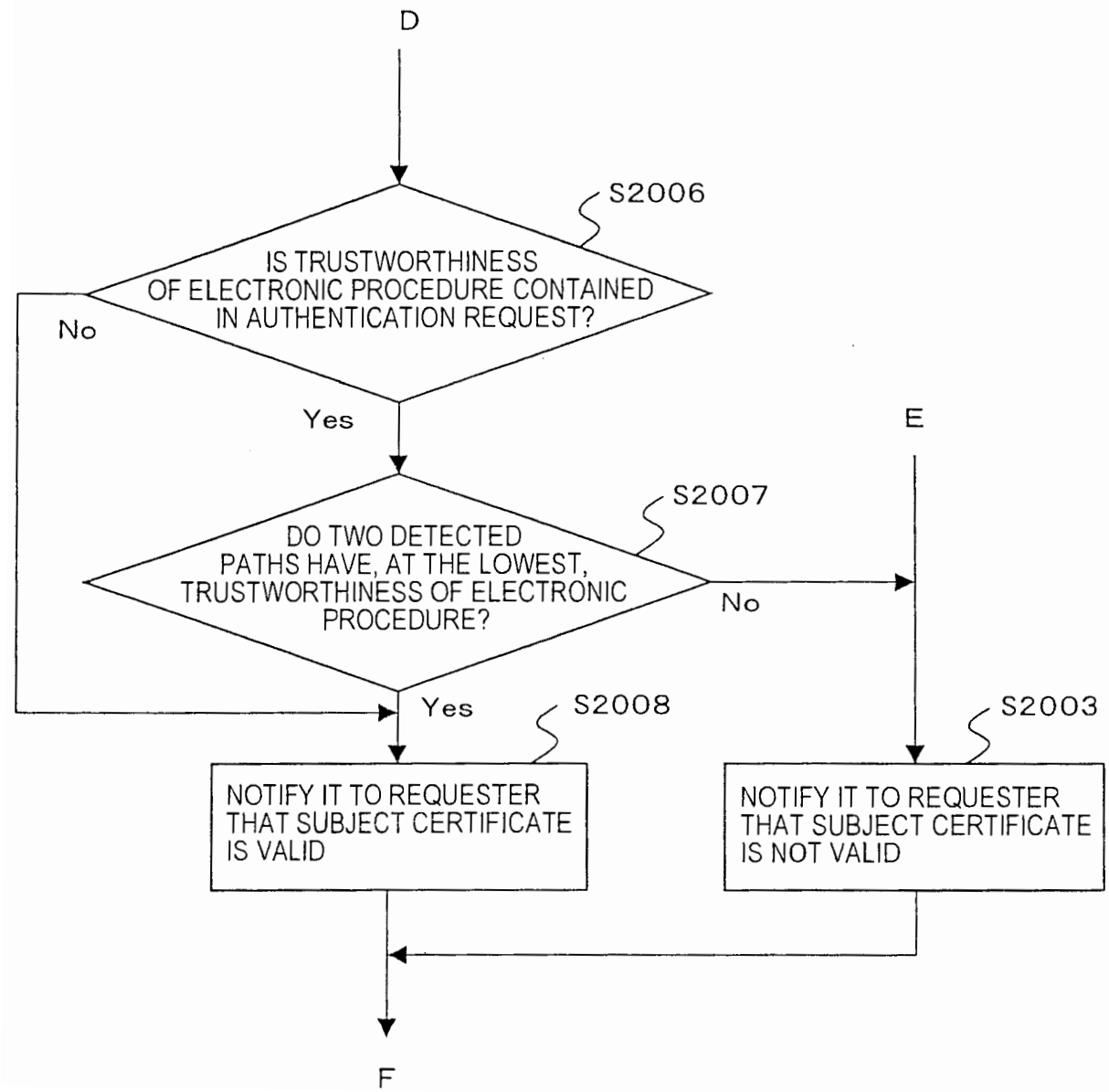
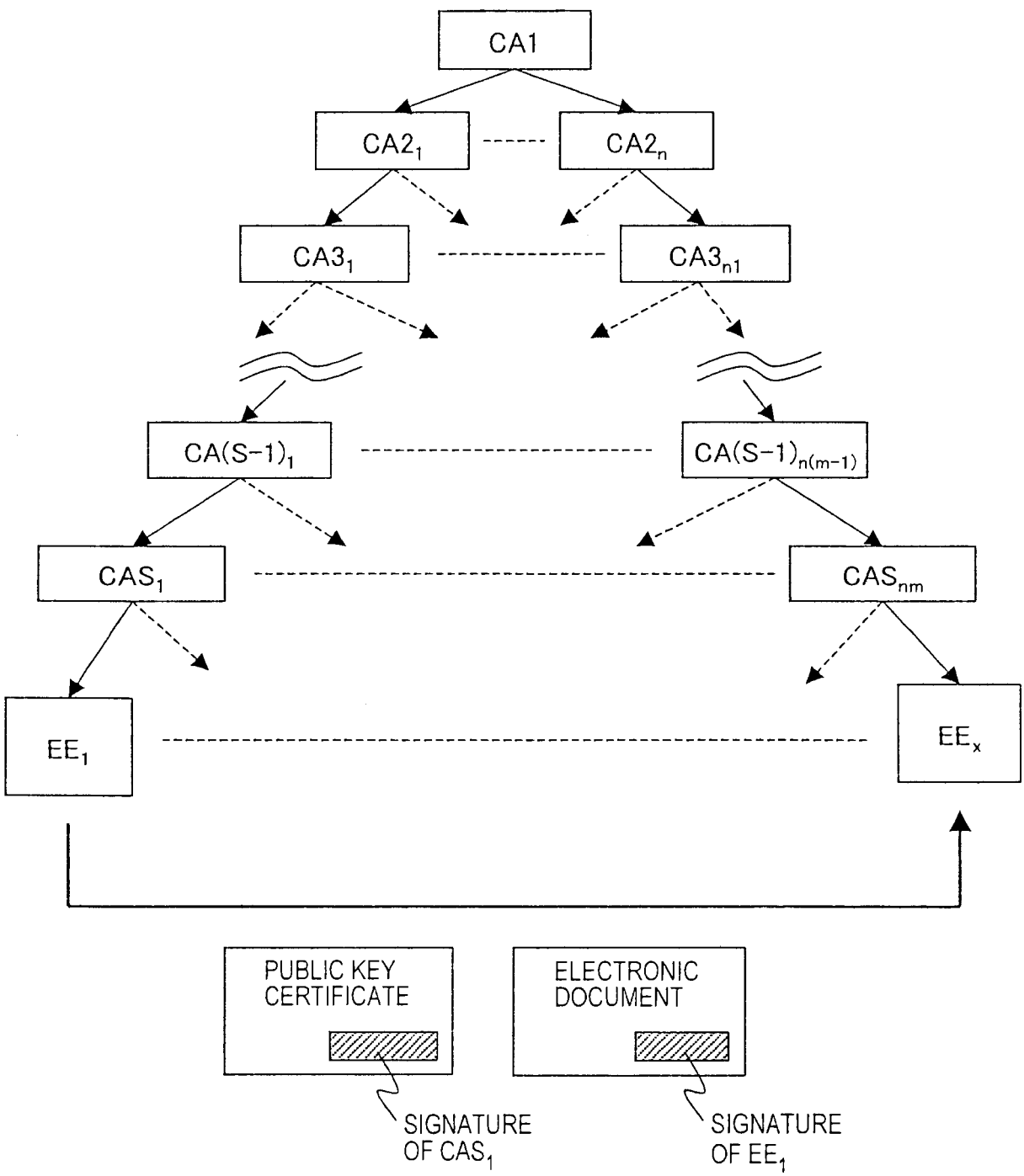


FIG.12



CA : CERTIFICATION AUTHORITY

EE : END ENTITY

⟶ : FLOW OF PUBLIC KEY CERTIFICATE