Fig. 1

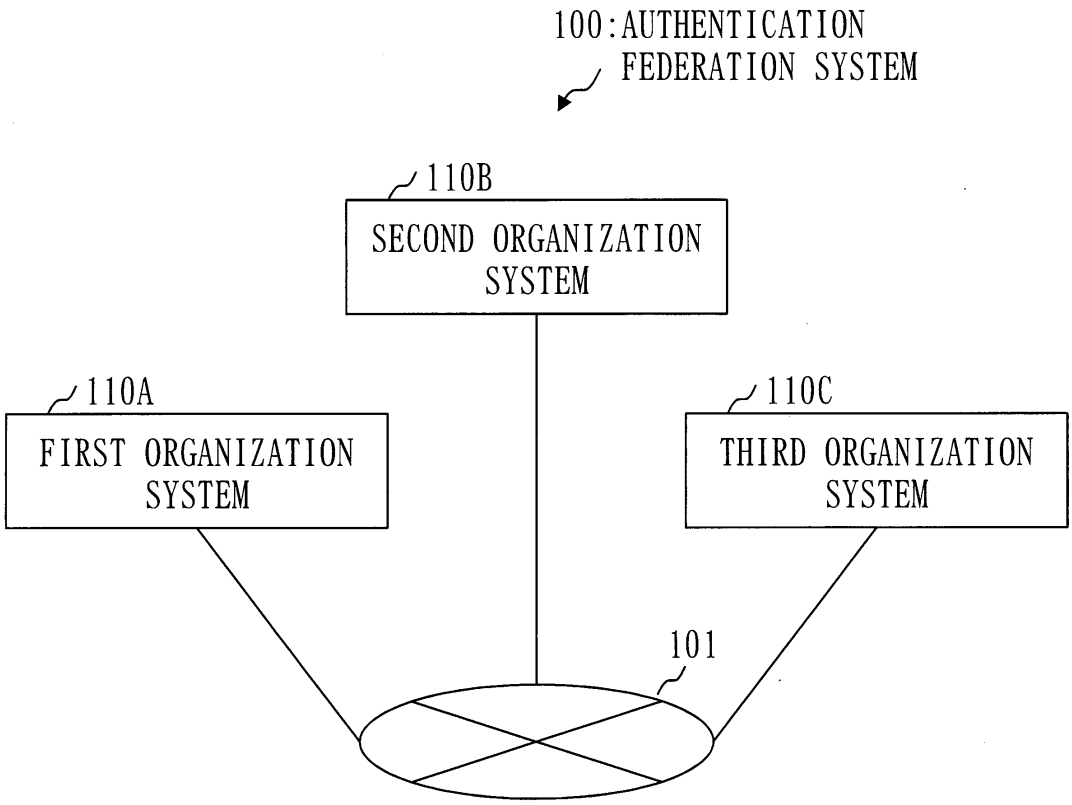

100:AUTHENTICATION FEDERATION SYSTEM
110B
SECOND ORGANIZATION SYSTEM
110A
FIRST ORGANIZATION SYSTEM
110C
THIRD ORGANIZATION SYSTEM
101

Fig. 2

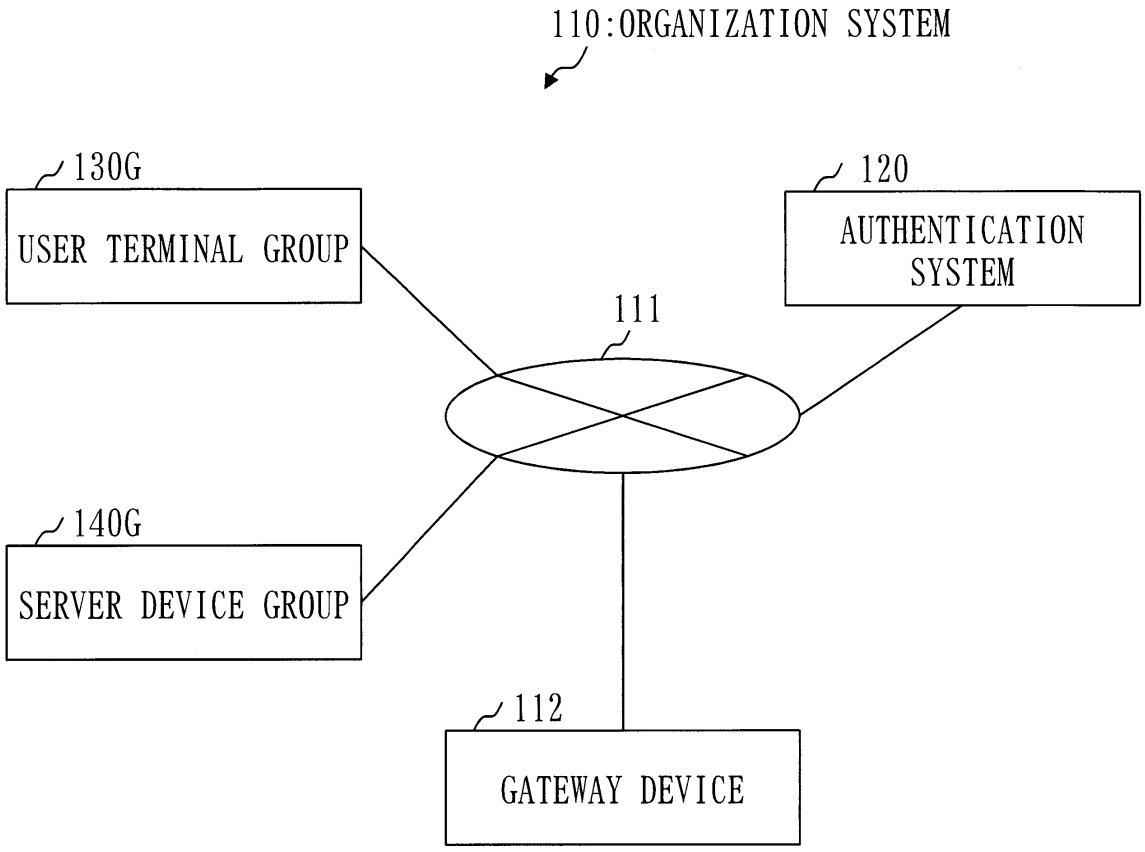

110:ORGANIZATION SYSTEM
130G
USER TERMINAL GROUP
120
AUTHENTICATION SYSTEM
111
140G
SERVER DEVICE GROUP
112
GATEWAY DEVICE

Fig. 3

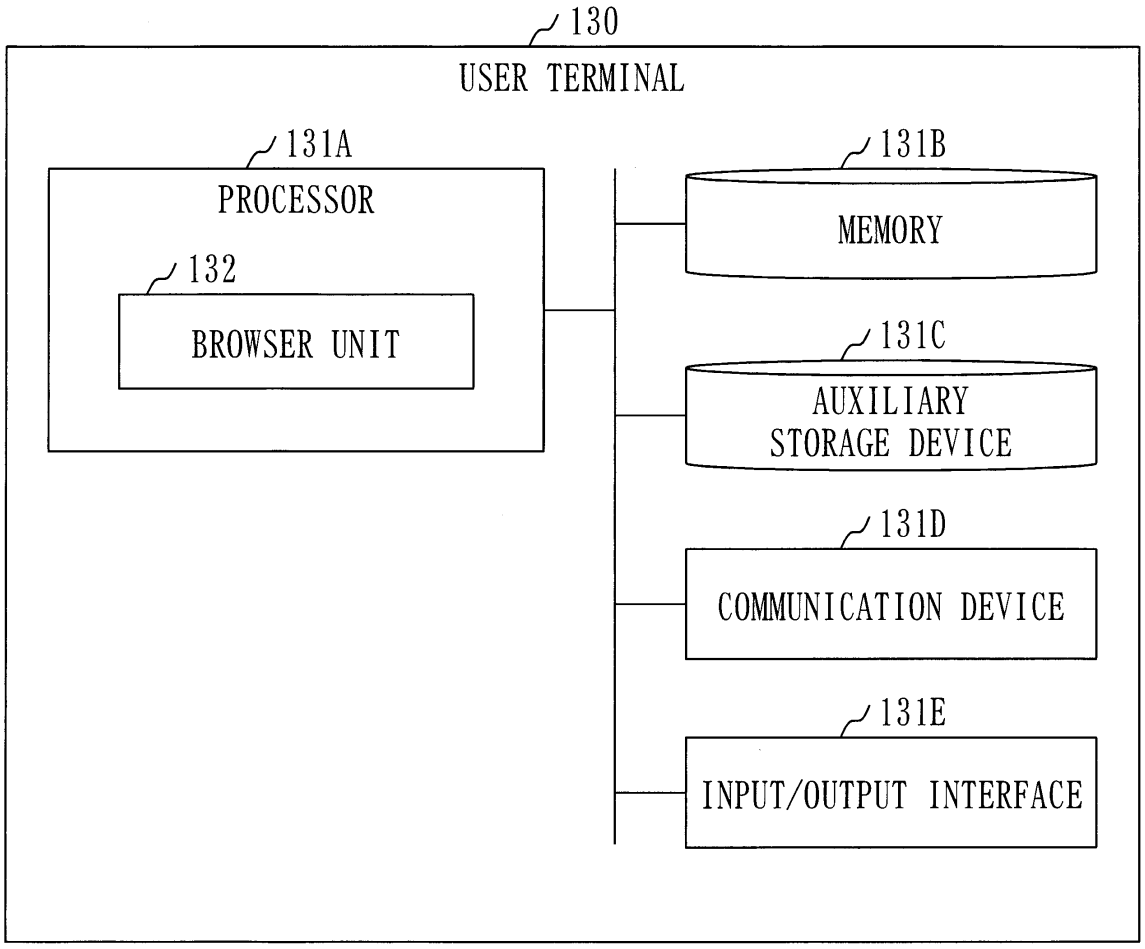

130
USER TERMINAL
131A
PROCESSOR
132
BROWSER UNIT
131B
MEMORY
131C
AUXILIARY
STORAGE DEVICE
131D
COMMUNICATION DEVICE
131E
INPUT/OUTPUT INTERFACE

Fig. 4

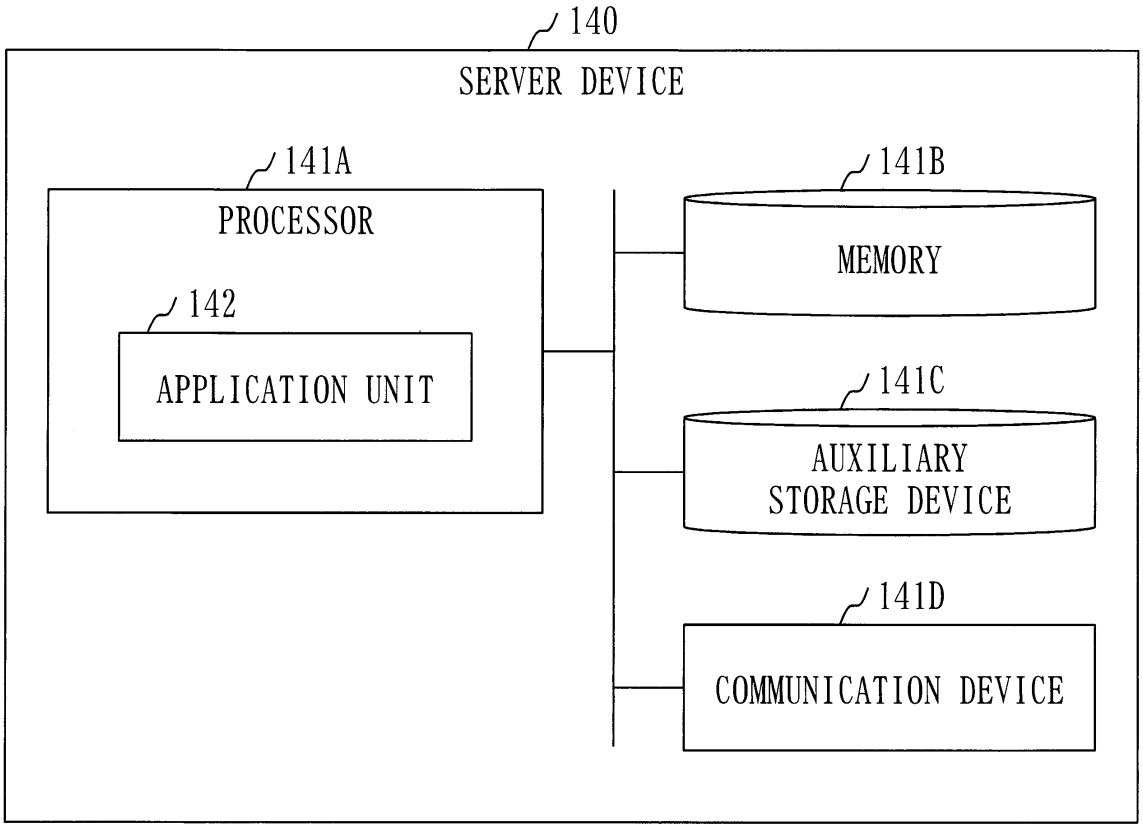

140
SERVER DEVICE
141A
PROCESSOR
142
APPLICATION UNIT
141B
MEMORY
141C
AUXILIARY
STORAGE DEVICE
141D
COMMUNICATION DEVICE

Fig. 5

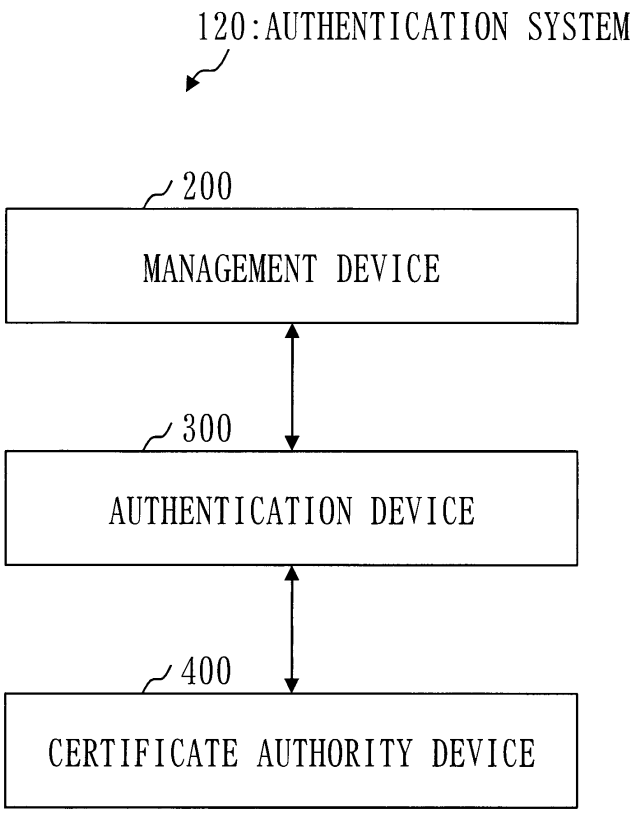

120:AUTHENTICATION SYSTEM
200
MANAGEMENT DEVICE
300
AUTHENTICATION DEVICE
400
CERTIFICATE AUTHORITY DEVICE

Fig. 6

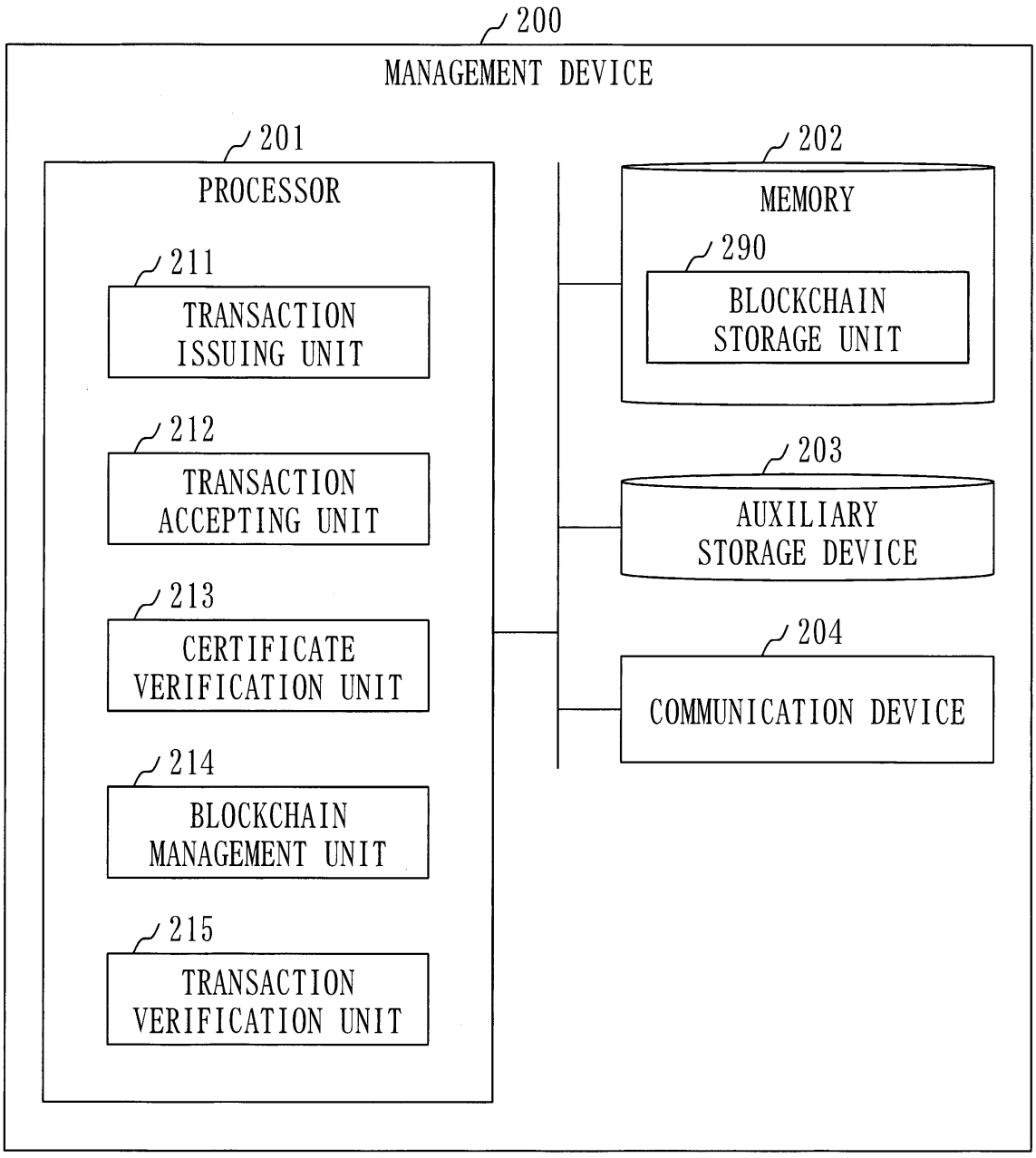

200
MANAGEMENT DEVICE
201
PROCESSOR
211
TRANSACTION ISSUING UNIT
212
TRANSACTION ACCEPTING UNIT
213
CERTIFICATE VERIFICATION UNIT
214
BLOCKCHAIN MANAGEMENT UNIT
215
TRANSACTION VERIFICATION UNIT
202
MEMORY
290
BLOCKCHAIN STORAGE UNIT
203
AUXILIARY STORAGE DEVICE
204
COMMUNICATION DEVICE

Fig. 7

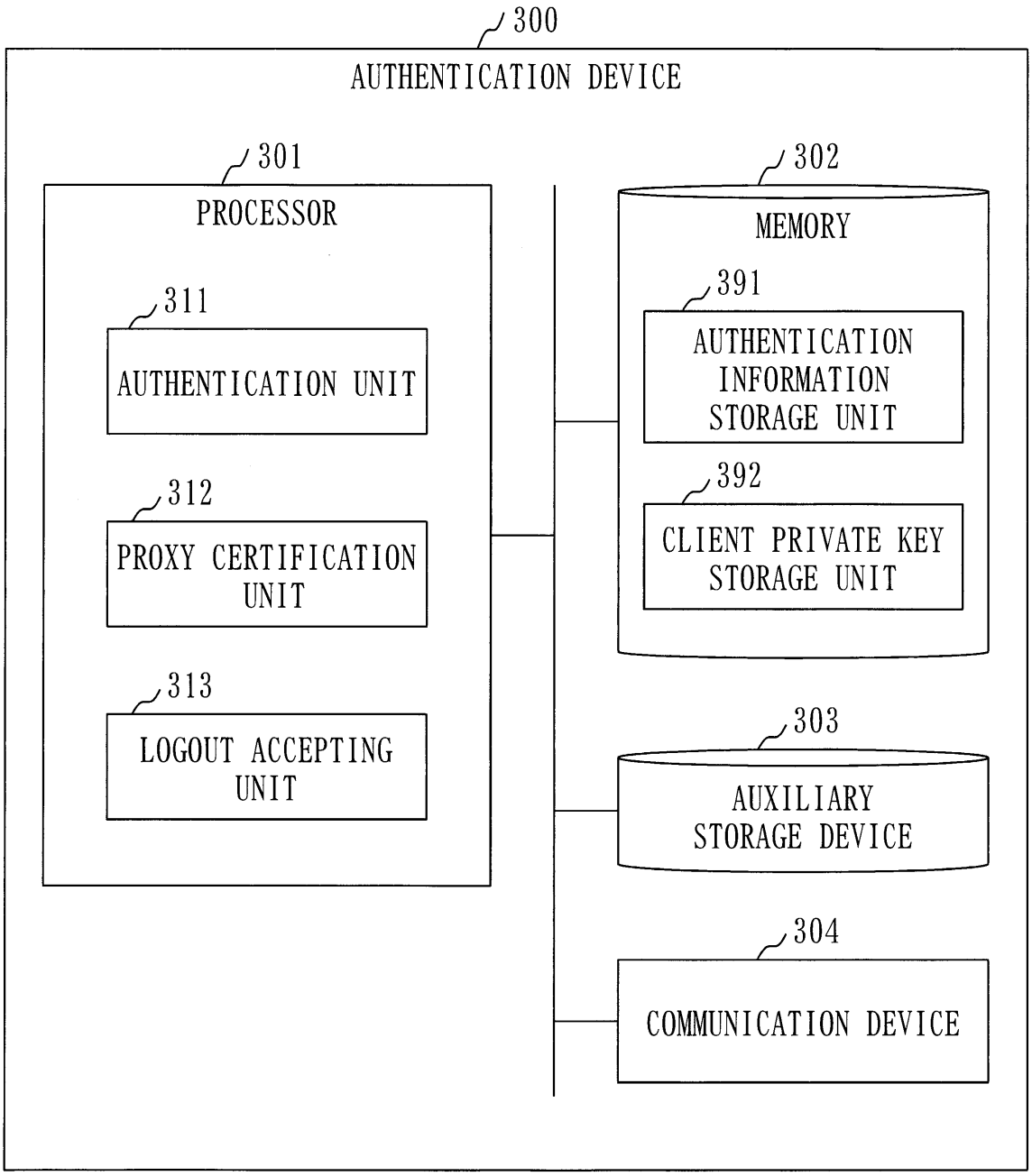

300
AUTHENTICATION DEVICE
301
PROCESSOR
311
AUTHENTICATION UNIT
312
PROXY CERTIFICATION UNIT
313
LOGOUT ACCEPTING UNIT
302
MEMORY
391
AUTHENTICATION INFORMATION STORAGE UNIT
392
CLIENT PRIVATE KEY STORAGE UNIT
303
AUXILIARY STORAGE DEVICE
304
COMMUNICATION DEVICE

Fig. 8

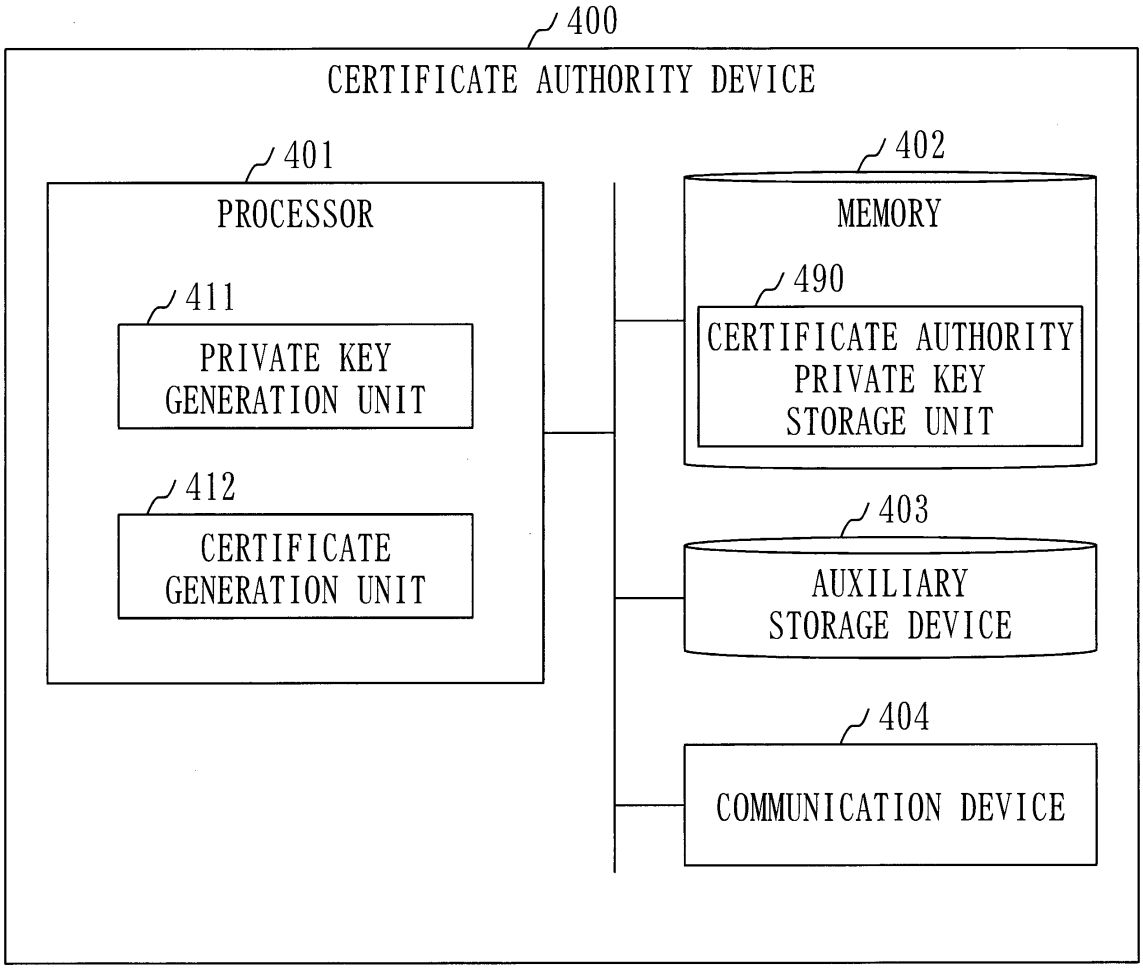

400
CERTIFICATE AUTHORITY DEVICE
401
PROCESSOR
411
PRIVATE KEY GENERATION UNIT
412
CERTIFICATE GENERATION UNIT
402
MEMORY
490
CERTIFICATE AUTHORITY PRIVATE KEY STORAGE UNIT
403
AUXILIARY STORAGE DEVICE
404
COMMUNICATION DEVICE

Fig. 9

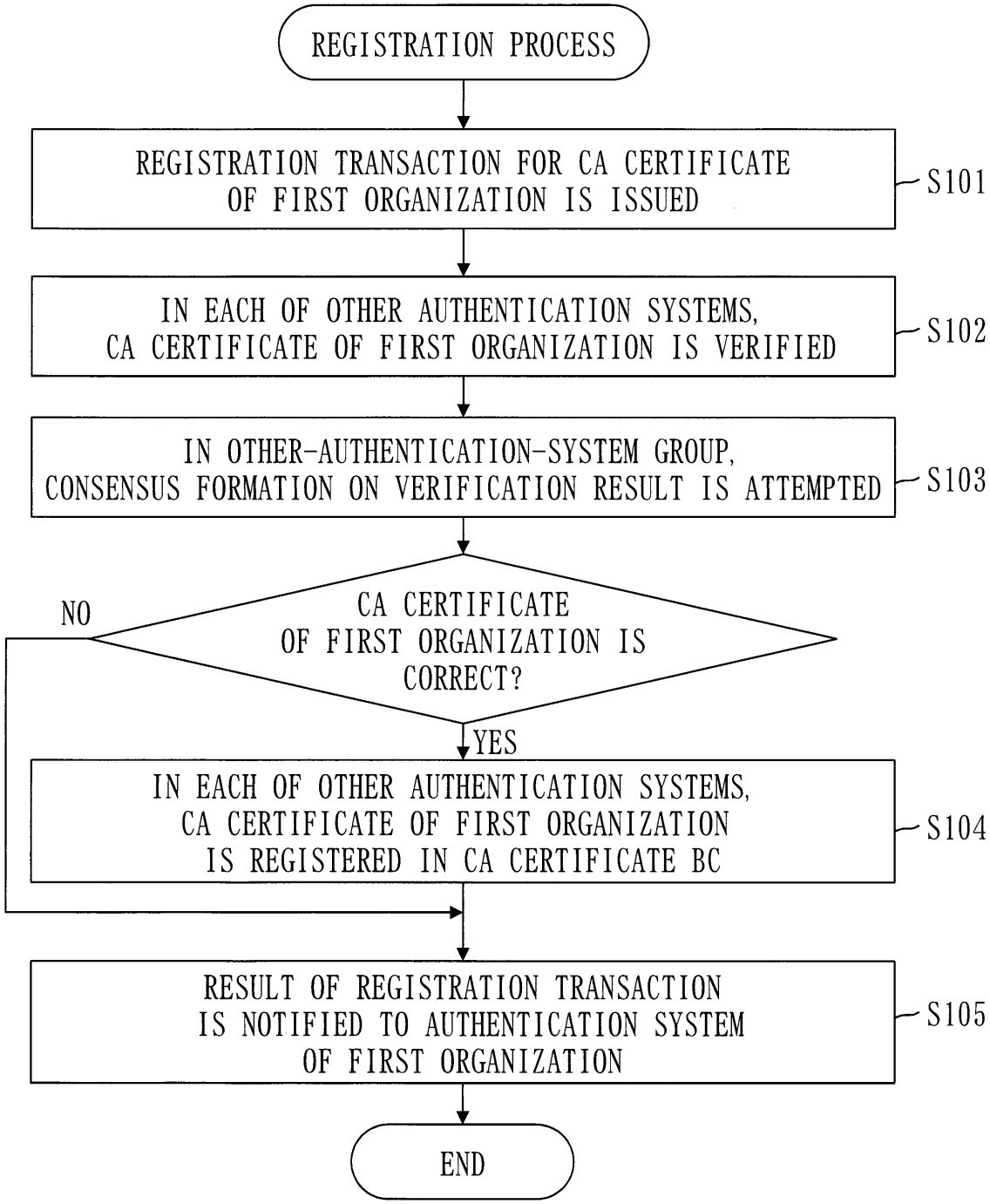

REGISTRATION PROCESS
REGISTRATION TRANSACTION FOR CA CERTIFICATE OF FIRST ORGANIZATION IS ISSUED
S101
IN EACH OF OTHER AUTHENTICATION SYSTEMS, CA CERTIFICATE OF FIRST ORGANIZATION IS VERIFIED
S102
IN OTHER-AUTHENTICATION-SYSTEM GROUP, CONSENSUS FORMATION ON VERIFICATION RESULT IS ATTEMPTED
S103
CA CERTIFICATE OF FIRST ORGANIZATION IS CORRECT?
NO
YES
IN EACH OF OTHER AUTHENTICATION SYSTEMS, CA CERTIFICATE OF FIRST ORGANIZATION IS REGISTERED IN CA CERTIFICATE BC
S104
RESULT OF REGISTRATION TRANSACTION IS NOTIFIED TO AUTHENTICATION SYSTEM OF FIRST ORGANIZATION
S105
END

Fig.10

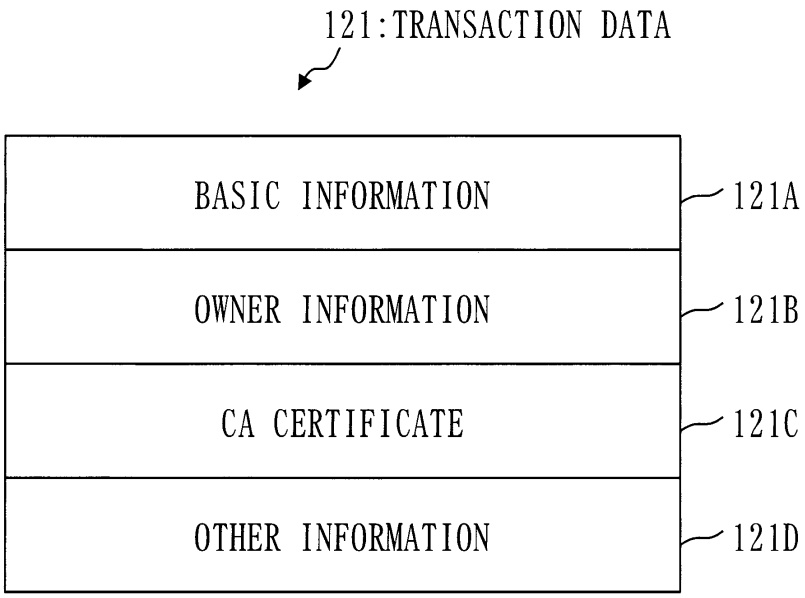

121:TRANSACTION DATA
BASIC INFORMATION
121A
OWNER INFORMATION
121B
CA CERTIFICATE
121C
OTHER INFORMATION
121D

Fig. 11

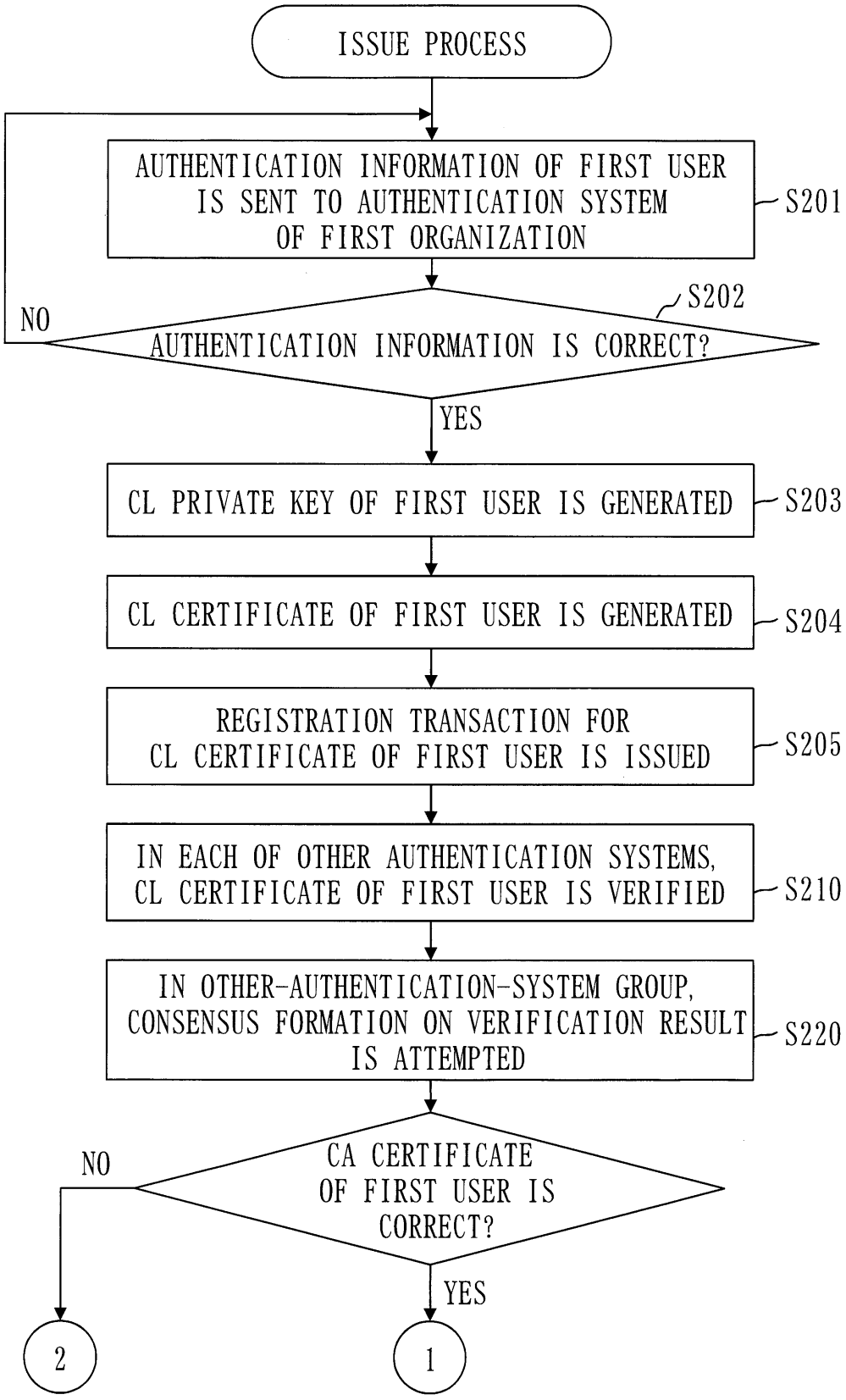

ISSUE PROCESS
AUTHENTICATION INFORMATION OF FIRST USER IS SENT TO AUTHENTICATION SYSTEM OF FIRST ORGANIZATION
S201
S202
NO
AUTHENTICATION INFORMATION IS CORRECT?
YES
CL PRIVATE KEY OF FIRST USER IS GENERATED
S203
CL CERTIFICATE OF FIRST USER IS GENERATED
S204
REGISTRATION TRANSACTION FOR CL CERTIFICATE OF FIRST USER IS ISSUED
S205
IN EACH OF OTHER AUTHENTICATION SYSTEMS, CL CERTIFICATE OF FIRST USER IS VERIFIED
S210
IN OTHER-AUTHENTICATION-SYSTEM GROUP, CONSENSUS FORMATION ON VERIFICATION RESULT IS ATTEMPTED
S220
NO
CA CERTIFICATE OF FIRST USER IS CORRECT?
YES
2
1

Fig.12

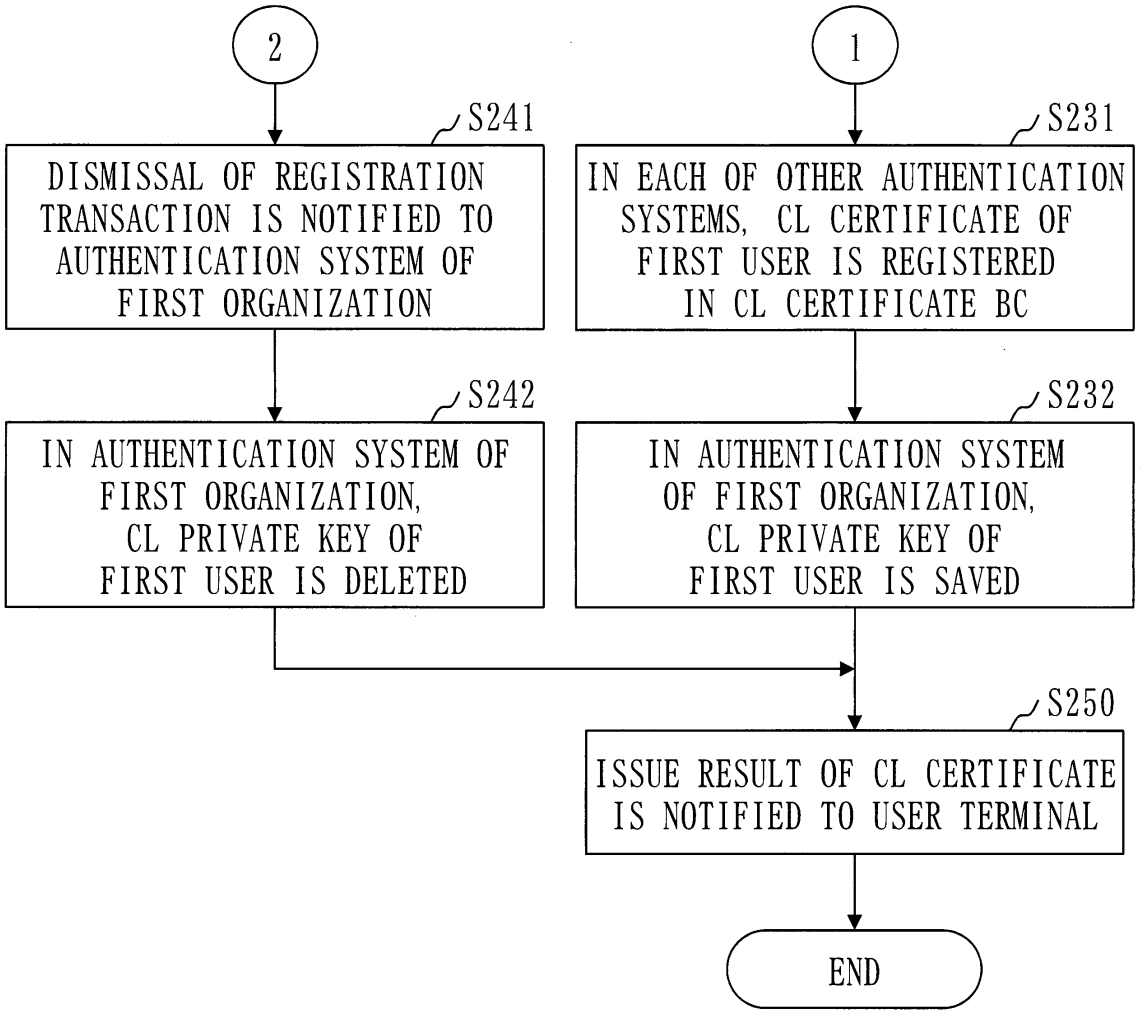

2
1
S241
S231
DISMISSAL OF REGISTRATION TRANSACTION IS NOTIFIED TO AUTHENTICATION SYSTEM OF FIRST ORGANIZATION
IN EACH OF OTHER AUTHENTICATION SYSTEMS, CL CERTIFICATE OF FIRST USER IS REGISTERED IN CL CERTIFICATE BC
S242
S232
IN AUTHENTICATION SYSTEM OF FIRST ORGANIZATION, CL PRIVATE KEY OF FIRST USER IS DELETED
IN AUTHENTICATION SYSTEM OF FIRST ORGANIZATION, CL PRIVATE KEY OF FIRST USER IS SAVED
S250
ISSUE RESULT OF CL CERTIFICATE IS NOTIFIED TO USER TERMINAL
END

Fig.13

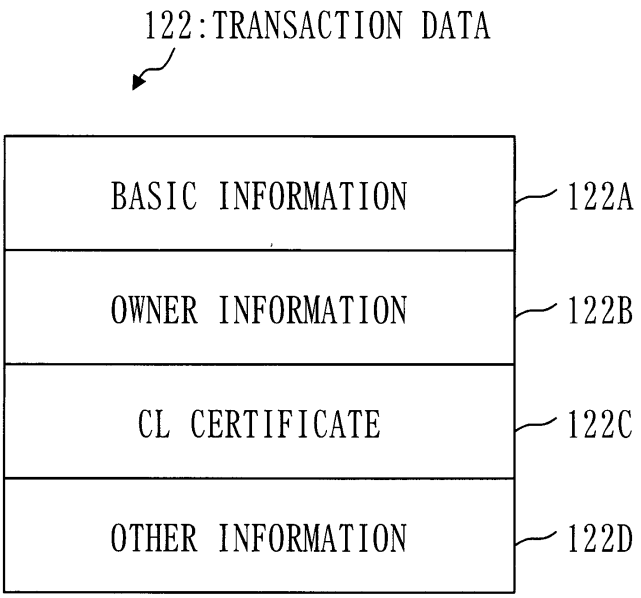

122:TRANSACTION DATA
BASIC INFORMATION
122A
OWNER INFORMATION
122B
CL CERTIFICATE
122C
OTHER INFORMATION
122D

Fig. 14

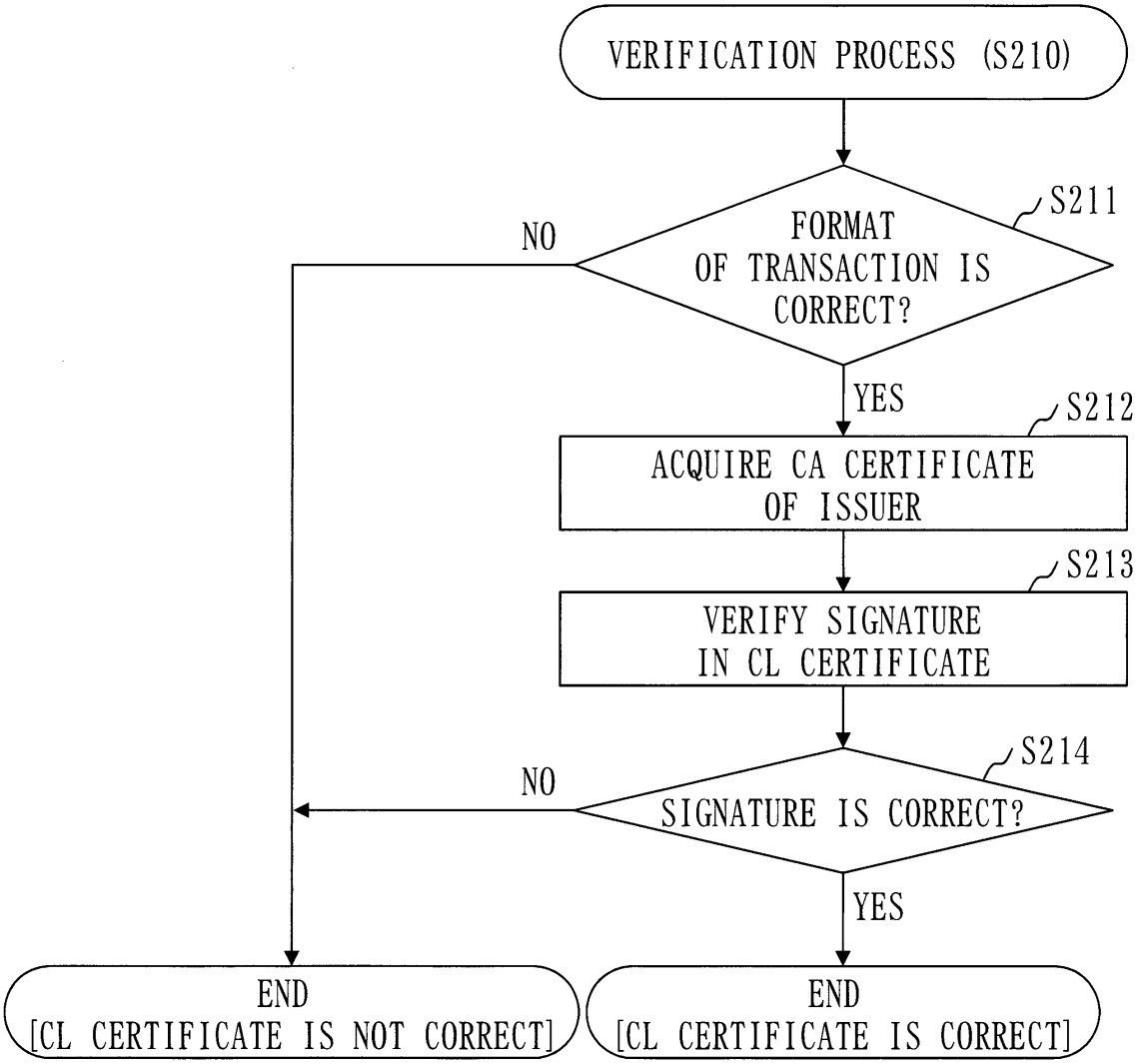

VERIFICATION PROCESS (S210)
S211
FORMAT OF TRANSACTION IS CORRECT?
NO
YES
S212
ACQUIRE CA CERTIFICATE OF ISSUER
S213
VERIFY SIGNATURE IN CL CERTIFICATE
S214
SIGNATURE IS CORRECT?
NO
YES
END [CL CERTIFICATE IS NOT CORRECT]
END [CL CERTIFICATE IS CORRECT]

Fig. 15

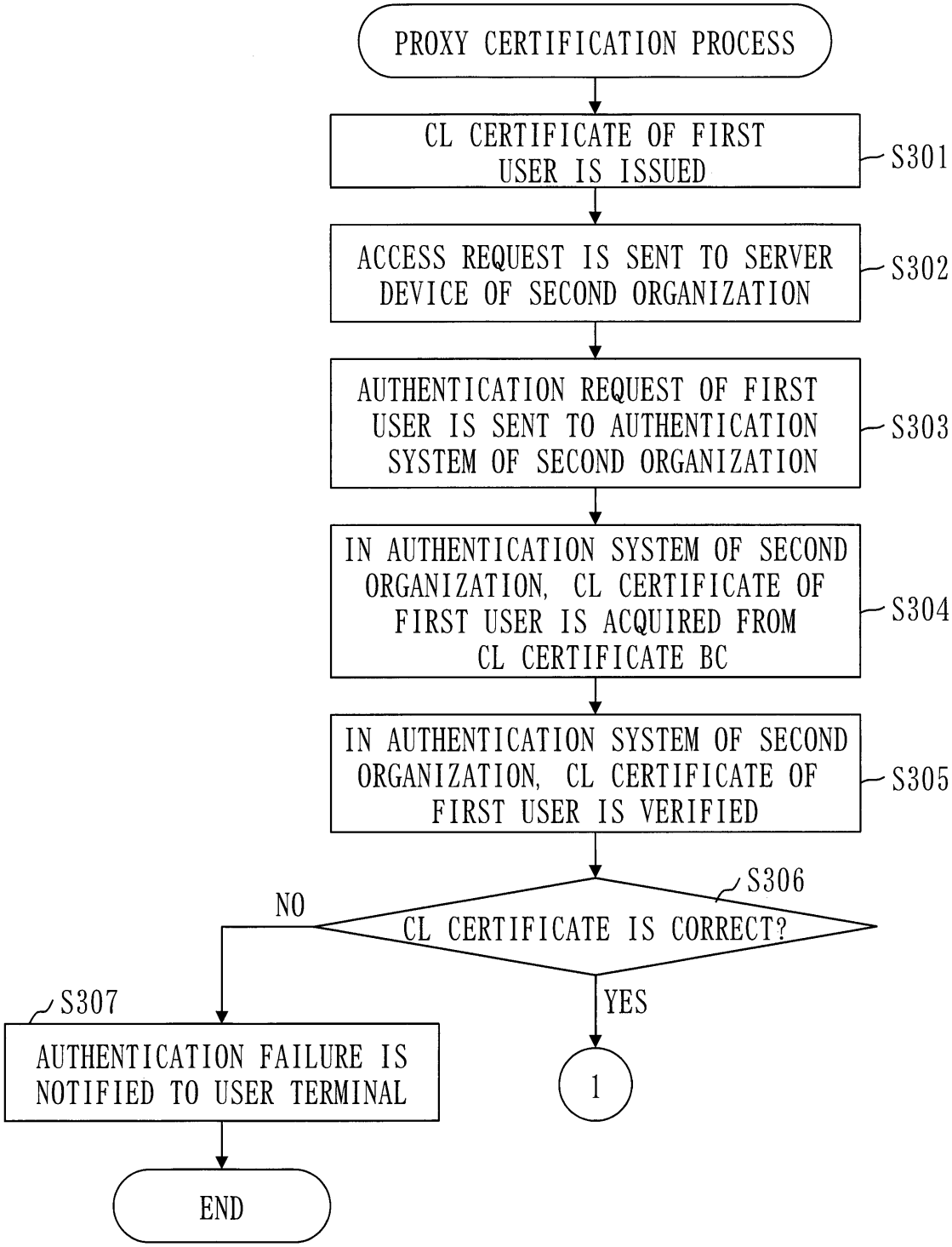

PROXY CERTIFICATION PROCESS
CL CERTIFICATE OF FIRST USER IS ISSUED
S301
ACCESS REQUEST IS SENT TO SERVER DEVICE OF SECOND ORGANIZATION
S302
AUTHENTICATION REQUEST OF FIRST USER IS SENT TO AUTHENTICATION SYSTEM OF SECOND ORGANIZATION
S303
IN AUTHENTICATION SYSTEM OF SECOND ORGANIZATION, CL CERTIFICATE OF FIRST USER IS ACQUIRED FROM CL CERTIFICATE BC
S304
IN AUTHENTICATION SYSTEM OF SECOND ORGANIZATION, CL CERTIFICATE OF FIRST USER IS VERIFIED
S305
S306
CL CERTIFICATE IS CORRECT?
NO
YES
S307
AUTHENTICATION FAILURE IS NOTIFIED TO USER TERMINAL
1
END

Fig.16

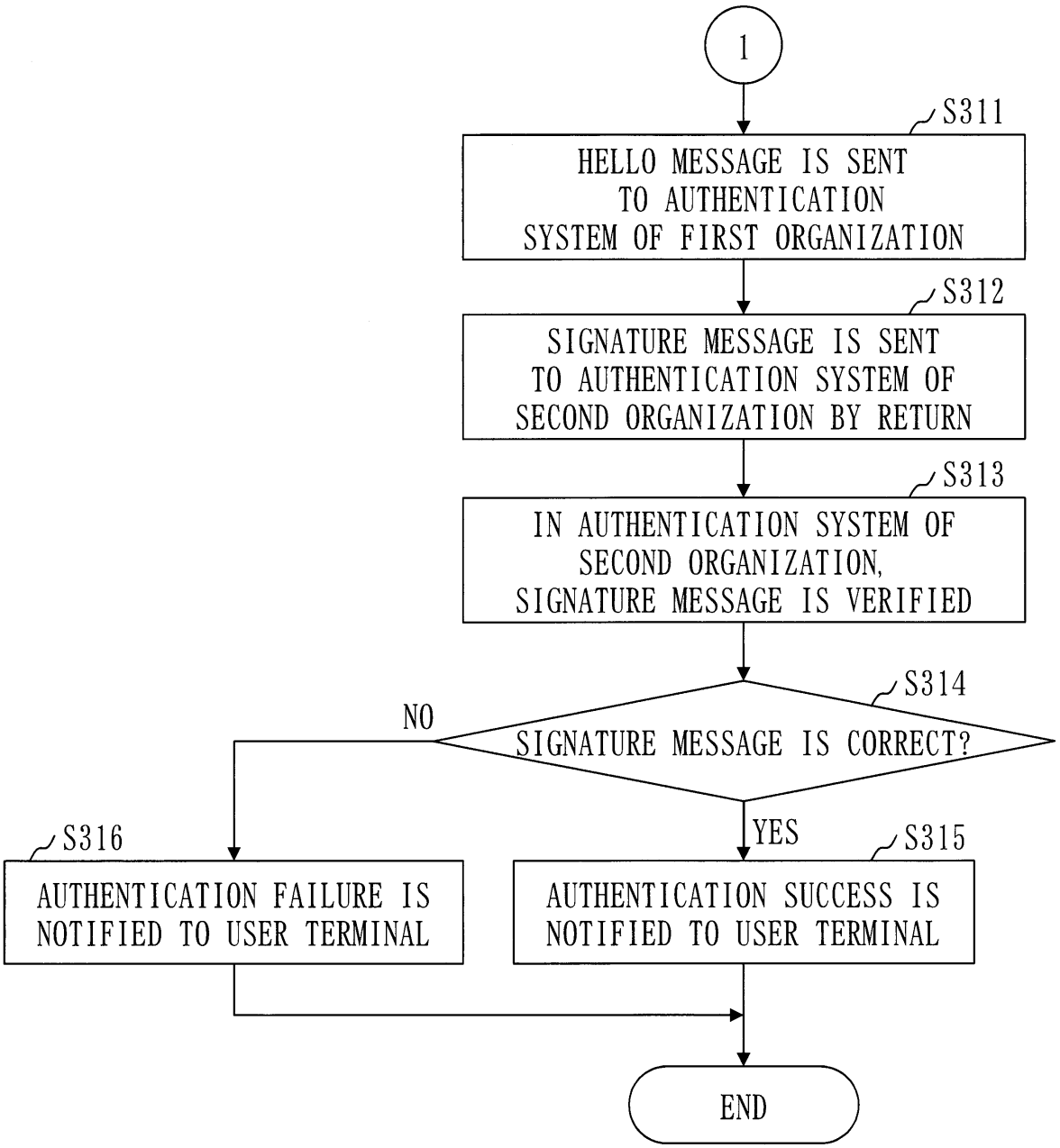

1
S311
HELLO MESSAGE IS SENT TO AUTHENTICATION SYSTEM OF FIRST ORGANIZATION
S312
SIGNATURE MESSAGE IS SENT TO AUTHENTICATION SYSTEM OF SECOND ORGANIZATION BY RETURN
S313
IN AUTHENTICATION SYSTEM OF SECOND ORGANIZATION, SIGNATURE MESSAGE IS VERIFIED
S314
SIGNATURE MESSAGE IS CORRECT?
NO
YES
S316
AUTHENTICATION FAILURE IS NOTIFIED TO USER TERMINAL
S315
AUTHENTICATION SUCCESS IS NOTIFIED TO USER TERMINAL
END

Fig. 17

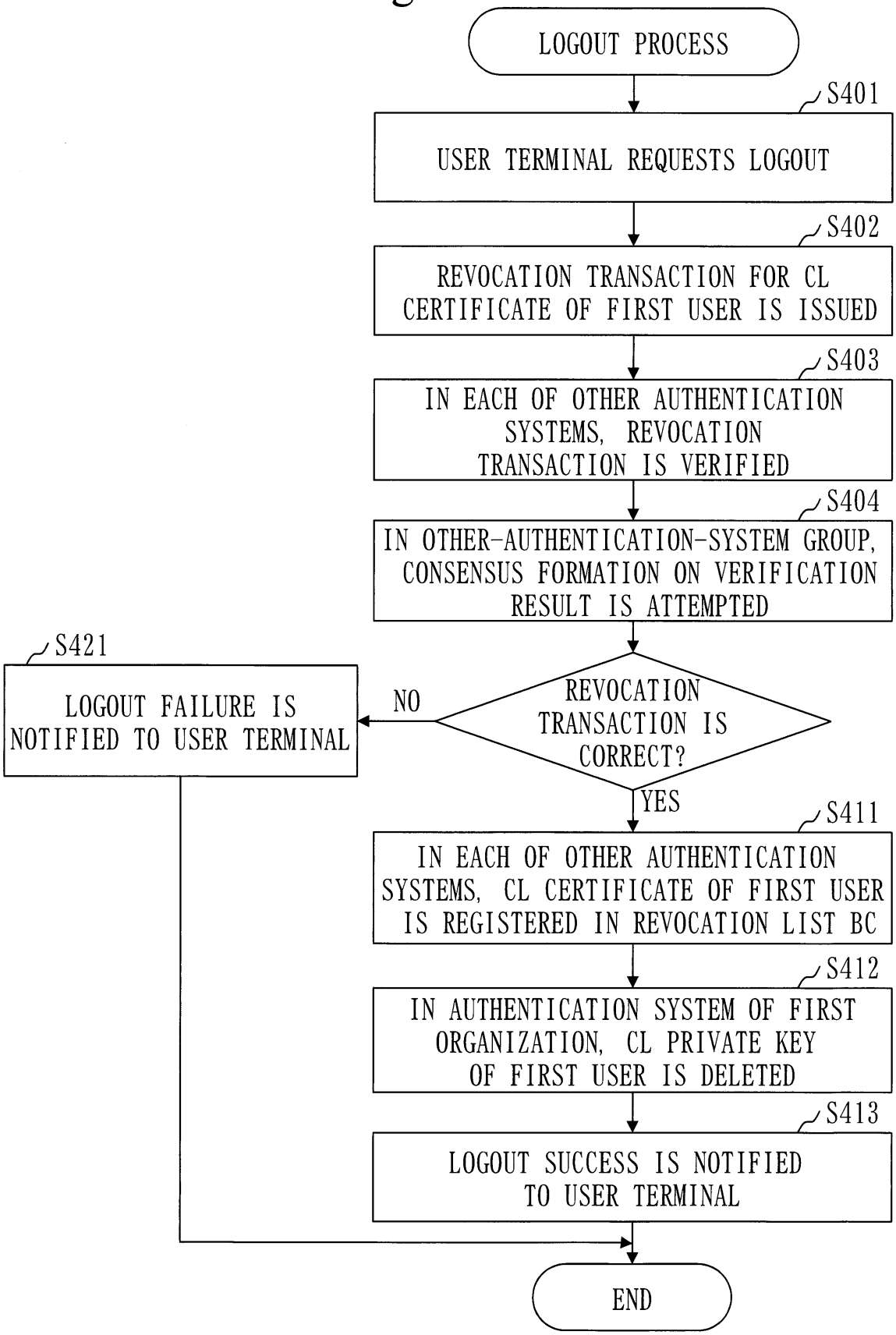

LOGOUT PROCESS
S401
USER TERMINAL REQUESTS LOGOUT
S402
REVOCATION TRANSACTION FOR CL CERTIFICATE OF FIRST USER IS ISSUED
S403
IN EACH OF OTHER AUTHENTICATION SYSTEMS, REVOCATION TRANSACTION IS VERIFIED
S404
IN OTHER-AUTHENTICATION-SYSTEM GROUP, CONSENSUS FORMATION ON VERIFICATION RESULT IS ATTEMPTED
REVOCATION TRANSACTION IS CORRECT?
NO
S421
LOGOUT FAILURE IS NOTIFIED TO USER TERMINAL
YES
S411
IN EACH OF OTHER AUTHENTICATION SYSTEMS, CL CERTIFICATE OF FIRST USER IS REGISTERED IN REVOCATION LIST BC
S412
IN AUTHENTICATION SYSTEM OF FIRST ORGANIZATION, CL PRIVATE KEY OF FIRST USER IS DELETED
S413
LOGOUT SUCCESS IS NOTIFIED TO USER TERMINAL
END

Fig.18

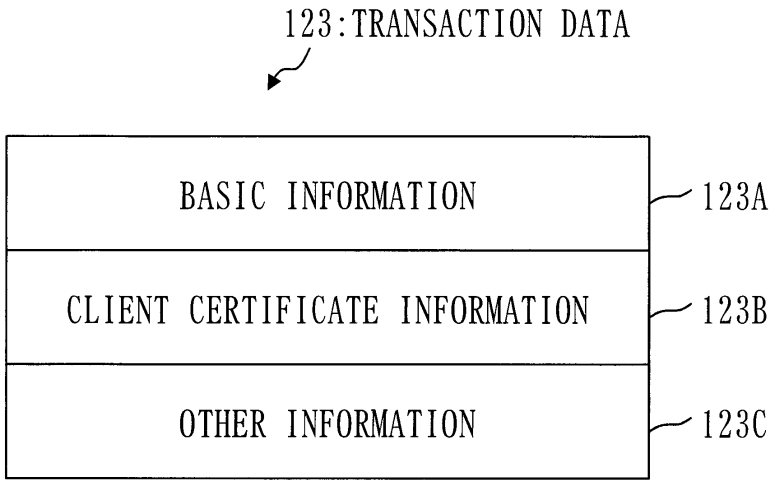

123:TRANSACTION DATA
BASIC INFORMATION
123A
CLIENT CERTIFICATE INFORMATION
123B
OTHER INFORMATION
123C

Fig. 19

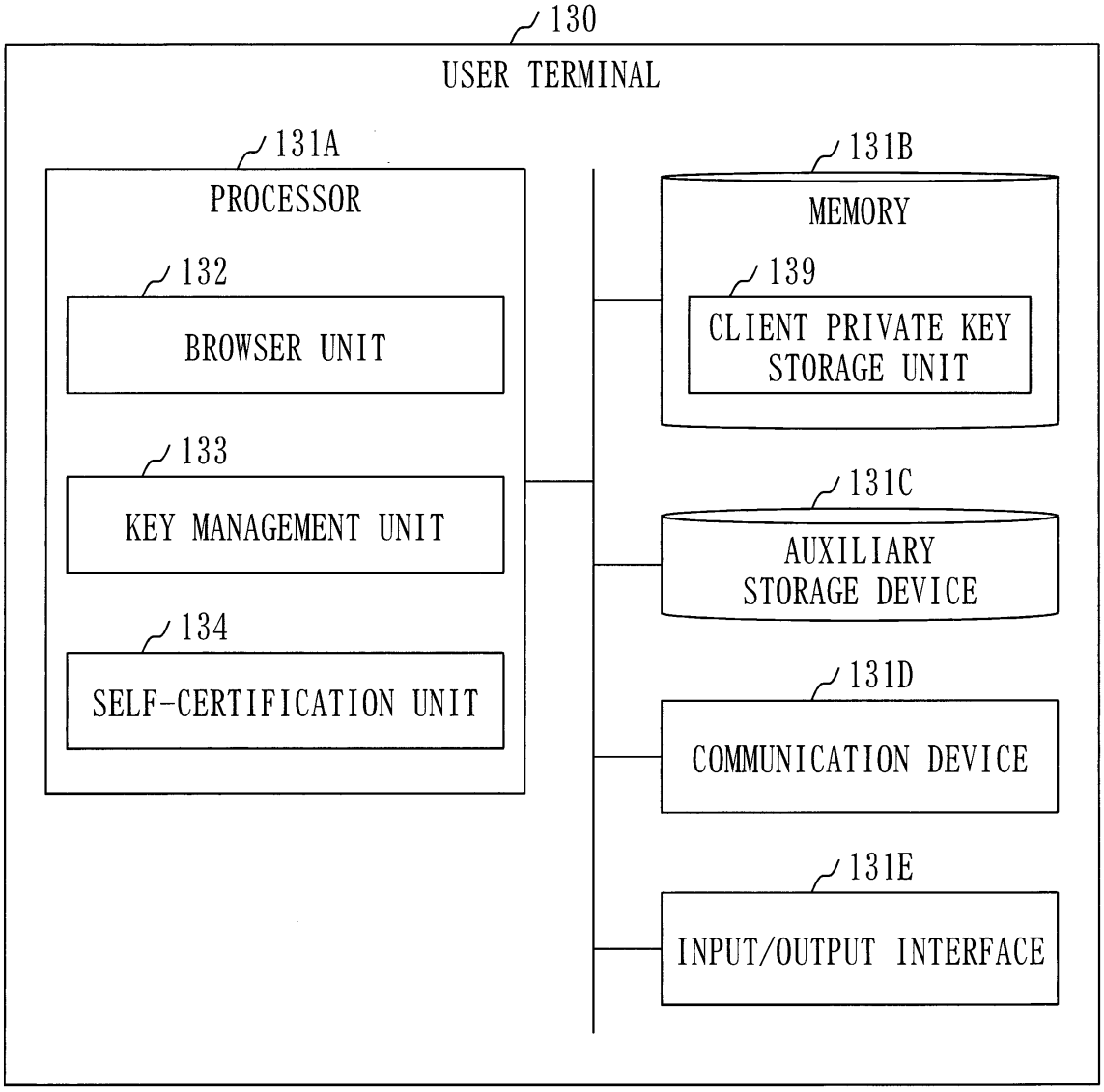

130
USER TERMINAL
131A
PROCESSOR
132
BROWSER UNIT
133
KEY MANAGEMENT UNIT
134
SELF-CERTIFICATION UNIT
131B
MEMORY
139
CLIENT PRIVATE KEY STORAGE UNIT
131C
AUXILIARY STORAGE DEVICE
131D
COMMUNICATION DEVICE
131E
INPUT/OUTPUT INTERFACE

Fig. 20

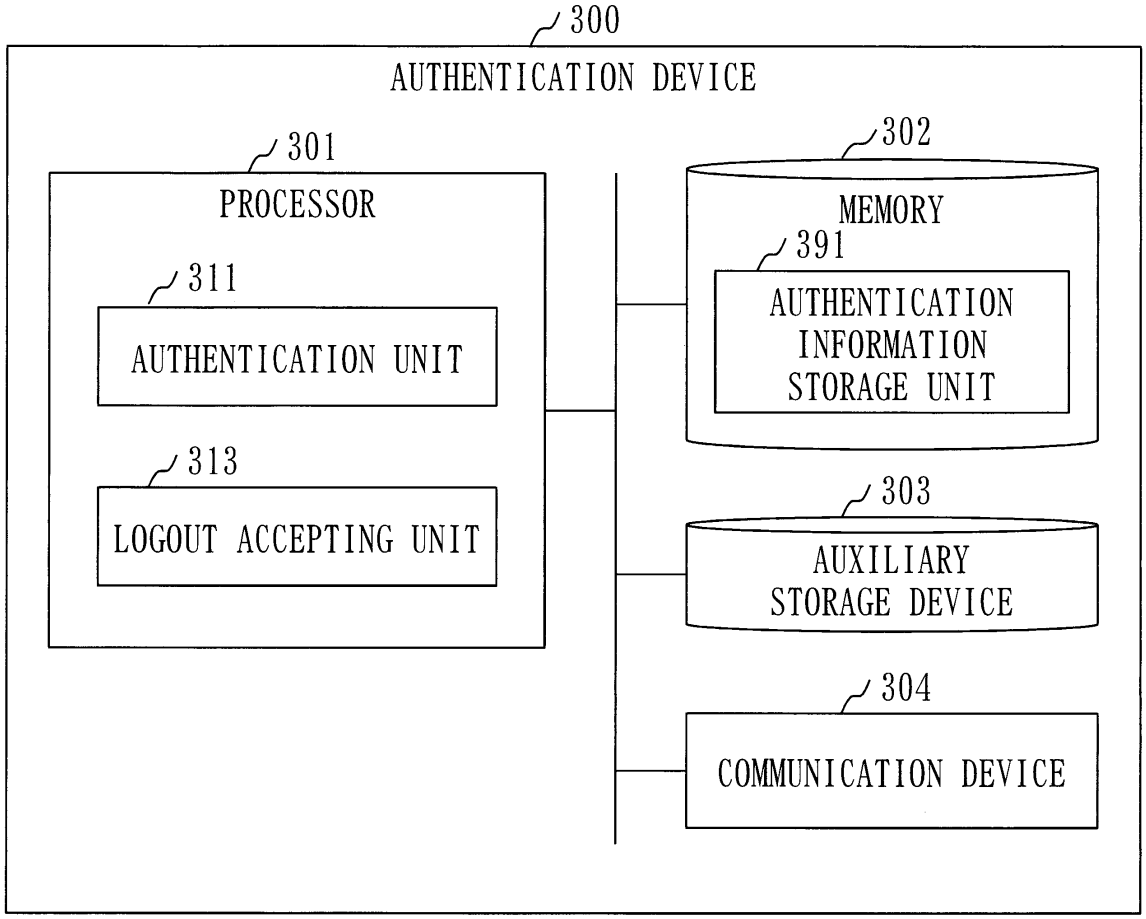

300
AUTHENTICATION DEVICE
301
PROCESSOR
311
AUTHENTICATION UNIT
313
LOGOUT ACCEPTING UNIT
302
MEMORY
391
AUTHENTICATION INFORMATION STORAGE UNIT
303
AUXILIARY STORAGE DEVICE
304
COMMUNICATION DEVICE

Fig. 21

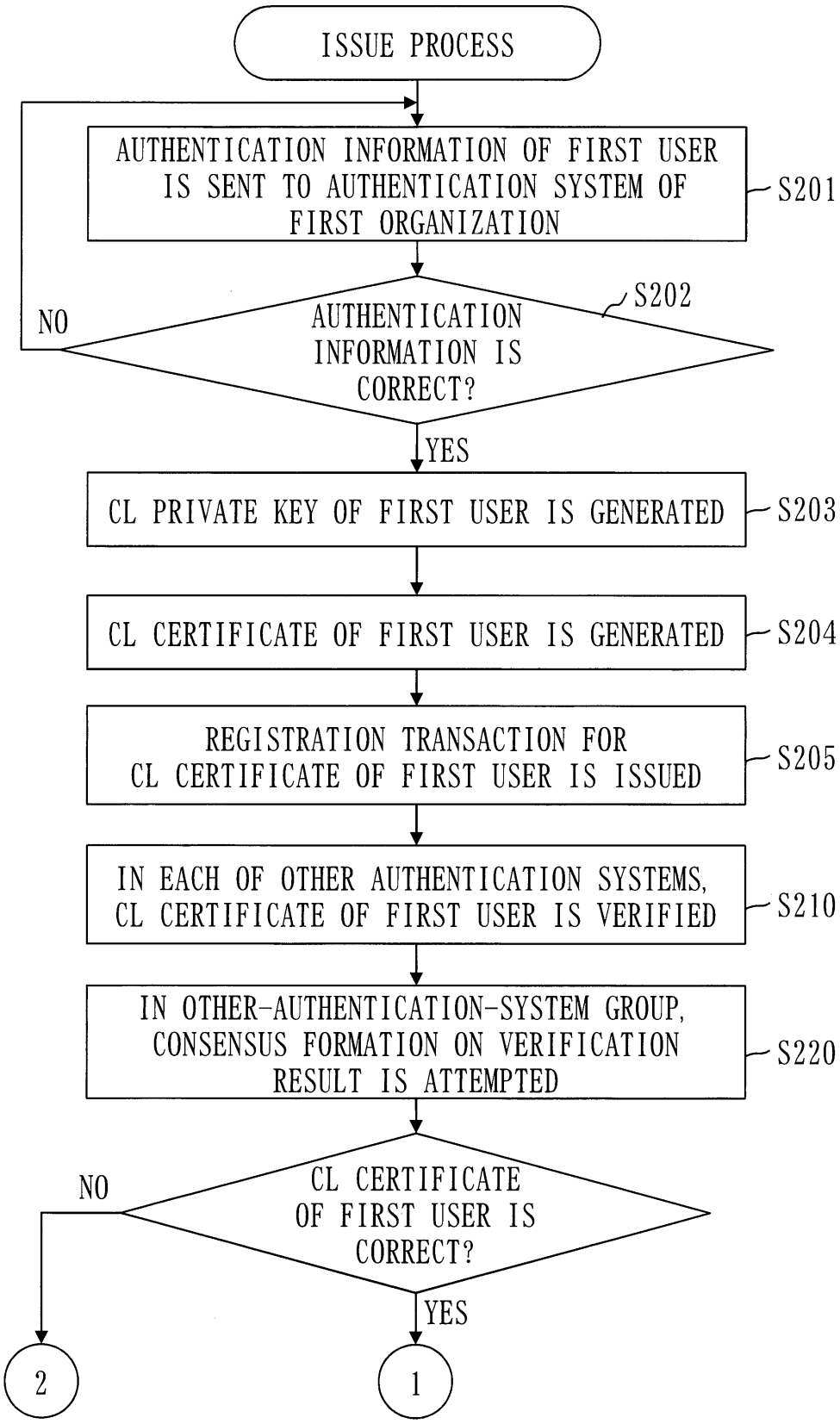

ISSUE PROCESS
AUTHENTICATION INFORMATION OF FIRST USER IS SENT TO AUTHENTICATION SYSTEM OF FIRST ORGANIZATION
S201
AUTHENTICATION INFORMATION IS CORRECT?
S202
NO
YES
CL PRIVATE KEY OF FIRST USER IS GENERATED
S203
CL CERTIFICATE OF FIRST USER IS GENERATED
S204
REGISTRATION TRANSACTION FOR CL CERTIFICATE OF FIRST USER IS ISSUED
S205
IN EACH OF OTHER AUTHENTICATION SYSTEMS, CL CERTIFICATE OF FIRST USER IS VERIFIED
S210
IN OTHER-AUTHENTICATION-SYSTEM GROUP, CONSENSUS FORMATION ON VERIFICATION RESULT IS ATTEMPTED
S220
CL CERTIFICATE OF FIRST USER IS CORRECT?
NO
YES
2
1

Fig. 22

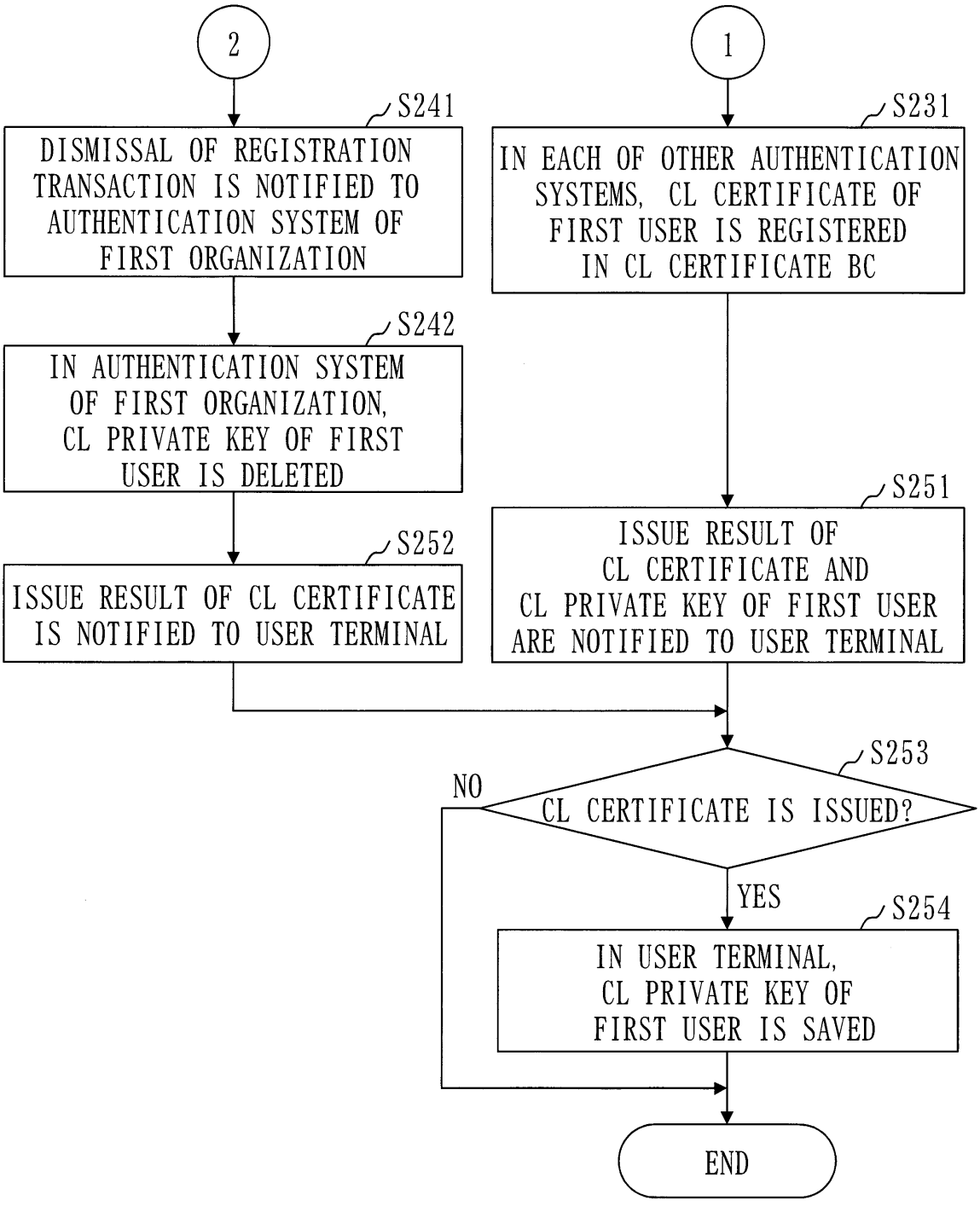

2
1
S241
DISMISSAL OF REGISTRATION TRANSACTION IS NOTIFIED TO AUTHENTICATION SYSTEM OF FIRST ORGANIZATION
S231
IN EACH OF OTHER AUTHENTICATION SYSTEMS, CL CERTIFICATE OF FIRST USER IS REGISTERED IN CL CERTIFICATE BC
S242
IN AUTHENTICATION SYSTEM OF FIRST ORGANIZATION, CL PRIVATE KEY OF FIRST USER IS DELETED
S251
ISSUE RESULT OF CL CERTIFICATE AND CL PRIVATE KEY OF FIRST USER ARE NOTIFIED TO USER TERMINAL
S252
ISSUE RESULT OF CL CERTIFICATE IS NOTIFIED TO USER TERMINAL
S253
NO
CL CERTIFICATE IS ISSUED?
YES
S254
IN USER TERMINAL, CL PRIVATE KEY OF FIRST USER IS SAVED
END

Fig. 23

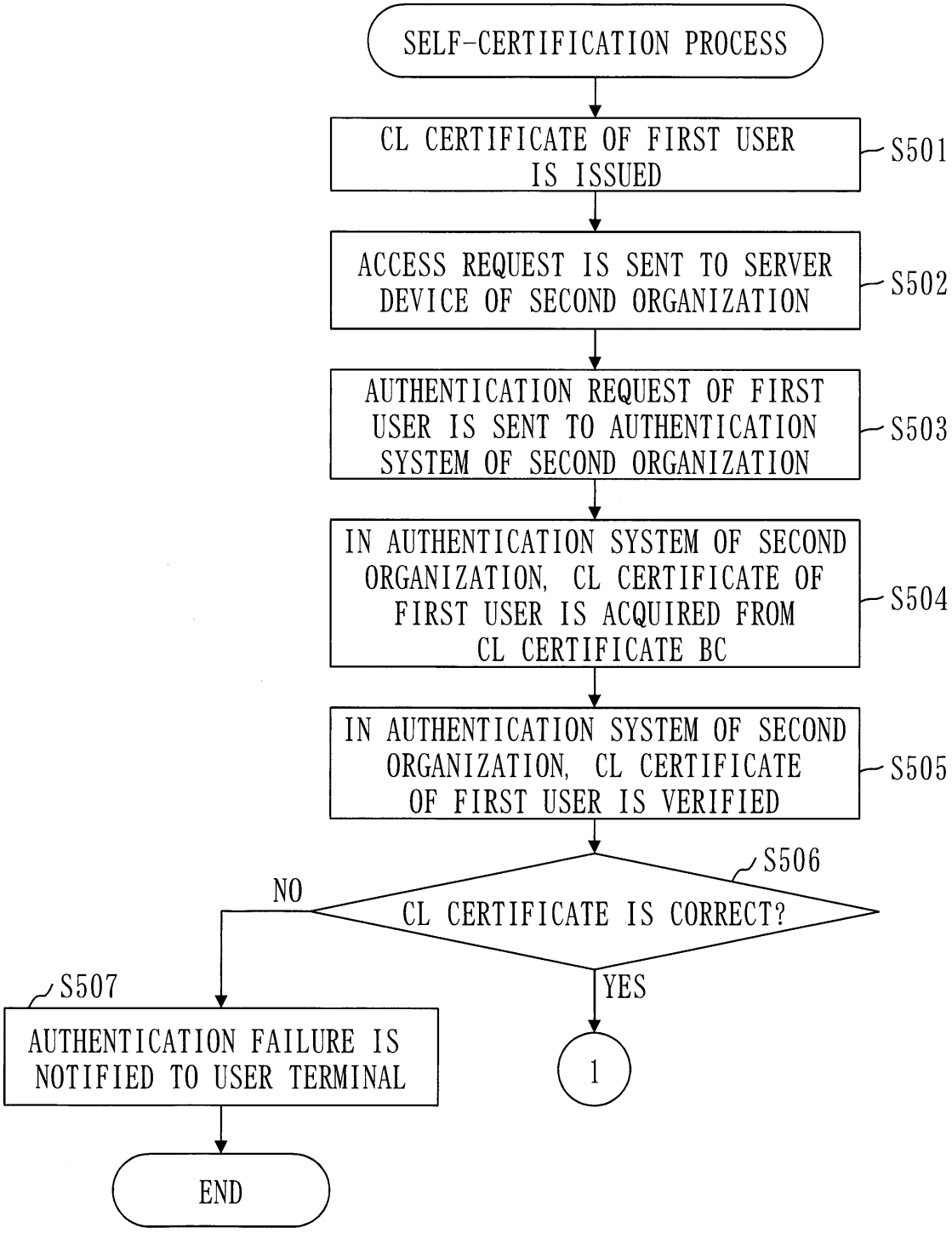

SELF-CERTIFICATION PROCESS
CL CERTIFICATE OF FIRST USER IS ISSUED
S501
ACCESS REQUEST IS SENT TO SERVER DEVICE OF SECOND ORGANIZATION
S502
AUTHENTICATION REQUEST OF FIRST USER IS SENT TO AUTHENTICATION SYSTEM OF SECOND ORGANIZATION
S503
IN AUTHENTICATION SYSTEM OF SECOND ORGANIZATION, CL CERTIFICATE OF FIRST USER IS ACQUIRED FROM CL CERTIFICATE BC
S504
IN AUTHENTICATION SYSTEM OF SECOND ORGANIZATION, CL CERTIFICATE OF FIRST USER IS VERIFIED
S505
S506
CL CERTIFICATE IS CORRECT?
NO
YES
S507
AUTHENTICATION FAILURE IS NOTIFIED TO USER TERMINAL
1
END

Fig. 24

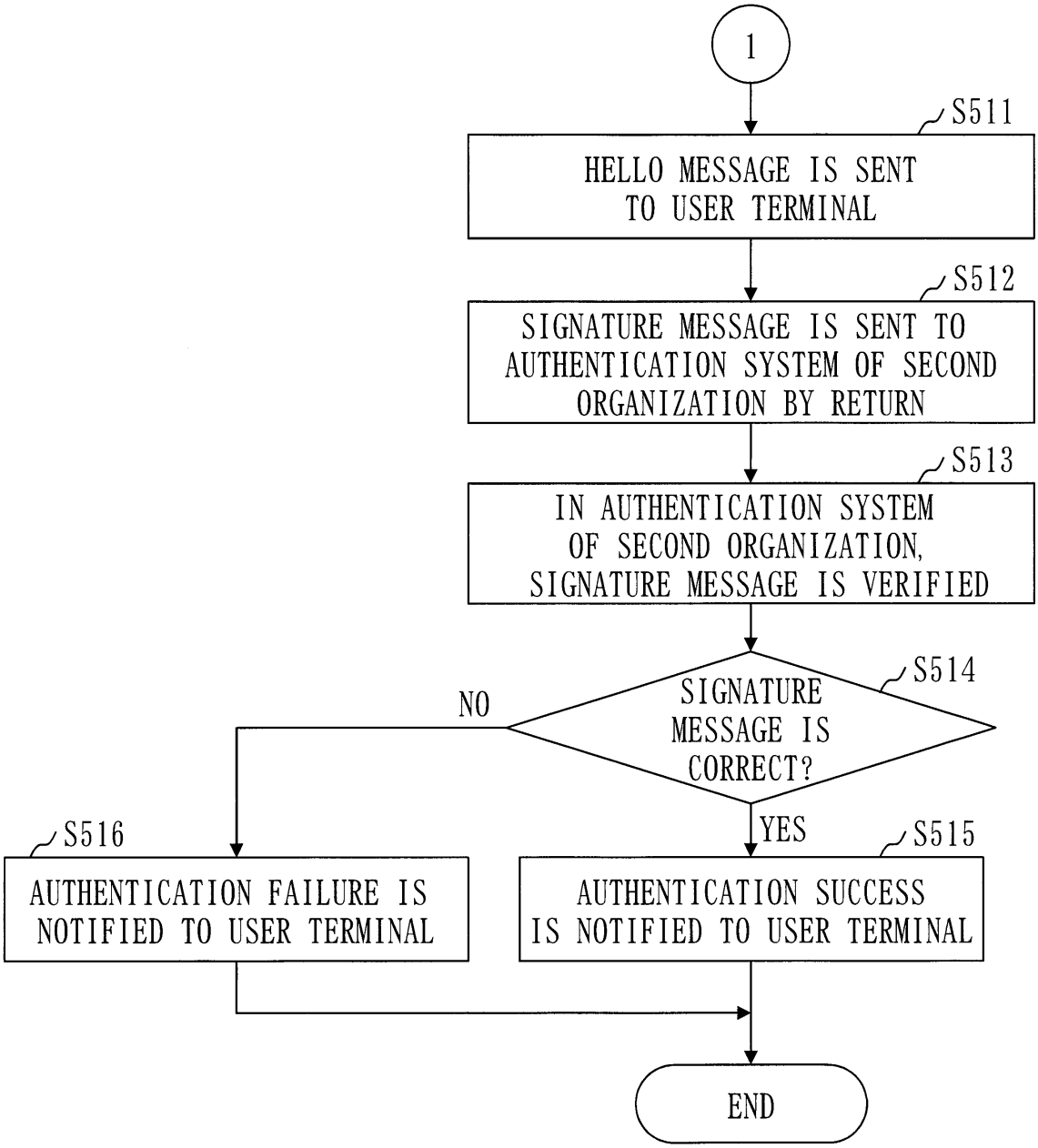

1
S511
HELLO MESSAGE IS SENT TO USER TERMINAL
S512
SIGNATURE MESSAGE IS SENT TO AUTHENTICATION SYSTEM OF SECOND ORGANIZATION BY RETURN
S513
IN AUTHENTICATION SYSTEM OF SECOND ORGANIZATION, SIGNATURE MESSAGE IS VERIFIED
S514
SIGNATURE MESSAGE IS CORRECT?
NO
YES
S516
AUTHENTICATION FAILURE IS NOTIFIED TO USER TERMINAL
S515
AUTHENTICATION SUCCESS IS NOTIFIED TO USER TERMINAL
END

Fig. 25

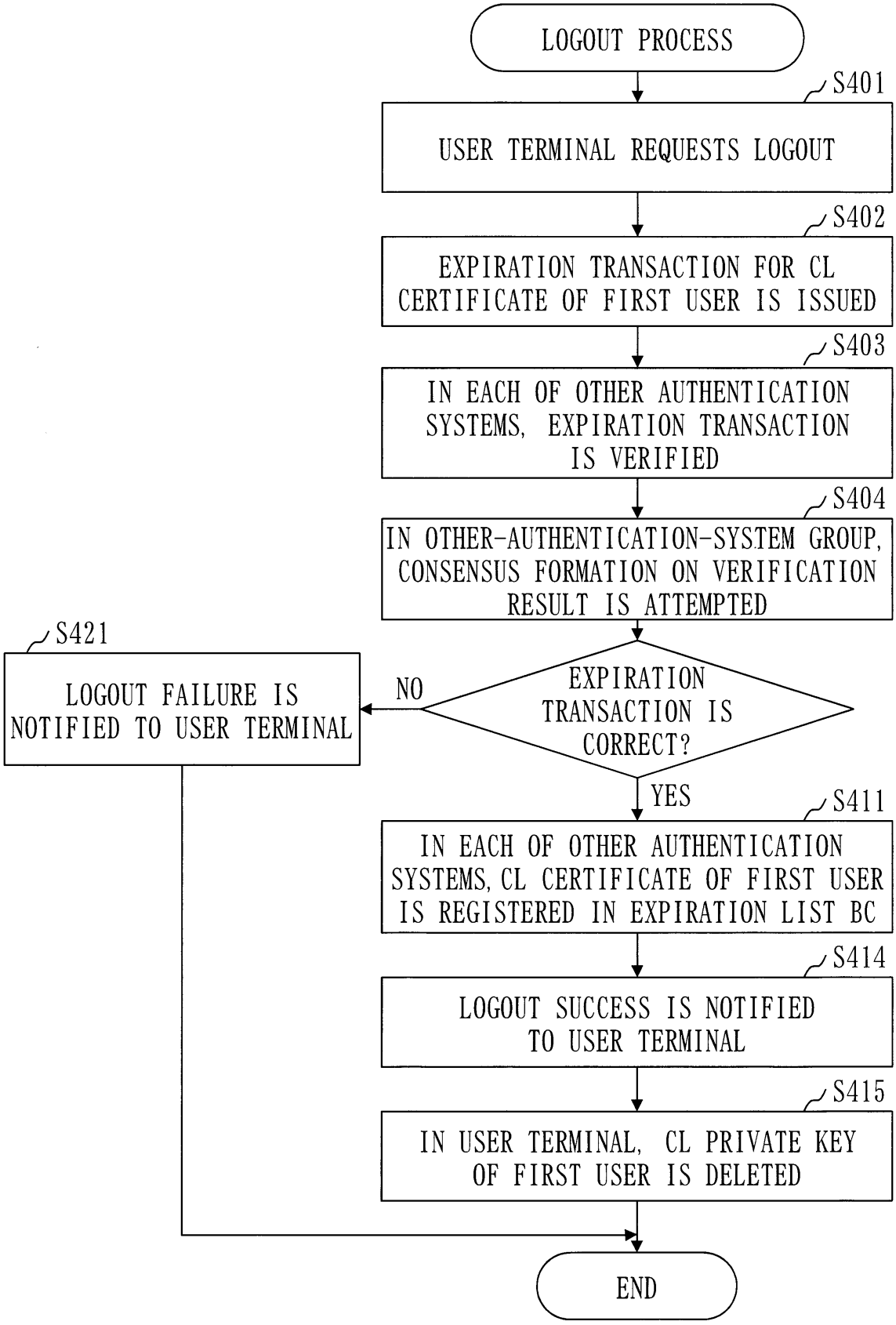

LOGOUT PROCESS
S401
USER TERMINAL REQUESTS LOGOUT
S402
EXPIRATION TRANSACTION FOR CL CERTIFICATE OF FIRST USER IS ISSUED
S403
IN EACH OF OTHER AUTHENTICATION SYSTEMS, EXPIRATION TRANSACTION IS VERIFIED
S404
IN OTHER-AUTHENTICATION-SYSTEM GROUP, CONSENSUS FORMATION ON VERIFICATION RESULT IS ATTEMPTED
EXPIRATION TRANSACTION IS CORRECT?
NO
S421
LOGOUT FAILURE IS NOTIFIED TO USER TERMINAL
YES
S411
IN EACH OF OTHER AUTHENTICATION SYSTEMS, CL CERTIFICATE OF FIRST USER IS REGISTERED IN EXPIRATION LIST BC
S414
LOGOUT SUCCESS IS NOTIFIED TO USER TERMINAL
S415
IN USER TERMINAL, CL PRIVATE KEY OF FIRST USER IS DELETED
END

Fig. 26

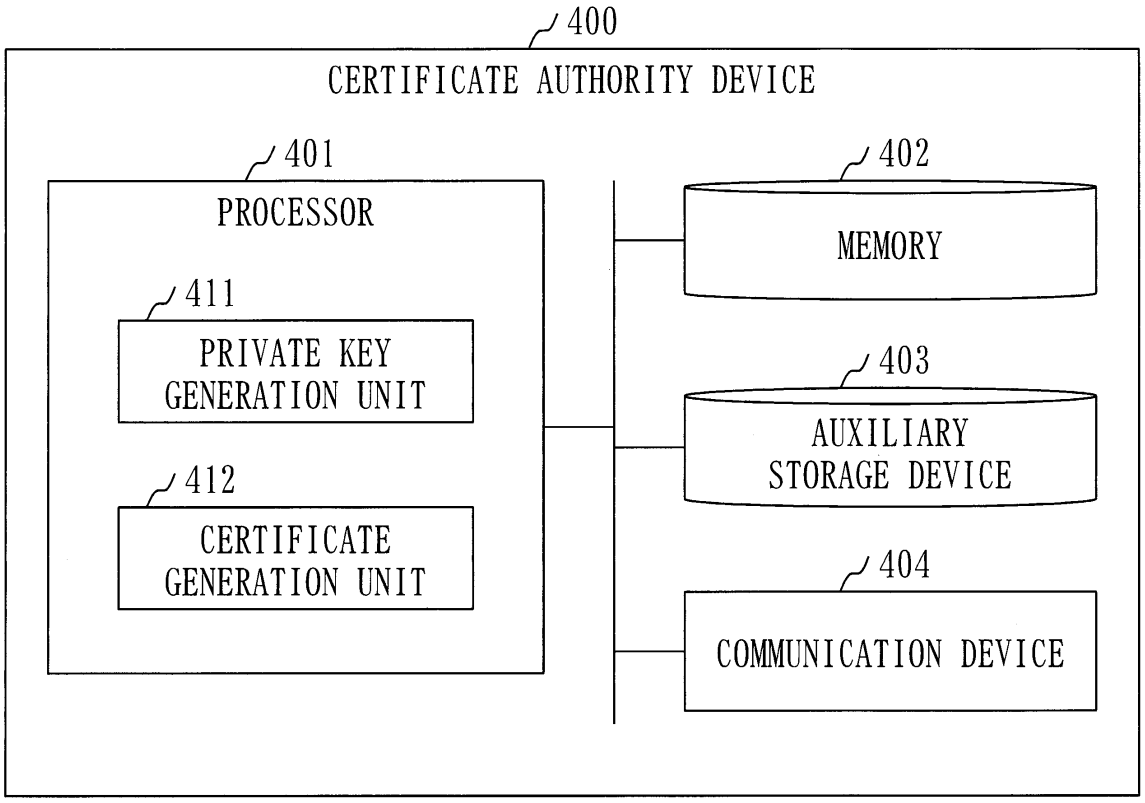

400
CERTIFICATE AUTHORITY DEVICE
401
PROCESSOR
411
PRIVATE KEY GENERATION UNIT
412
CERTIFICATE GENERATION UNIT
402
MEMORY
403
AUXILIARY STORAGE DEVICE
404
COMMUNICATION DEVICE

Fig. 27

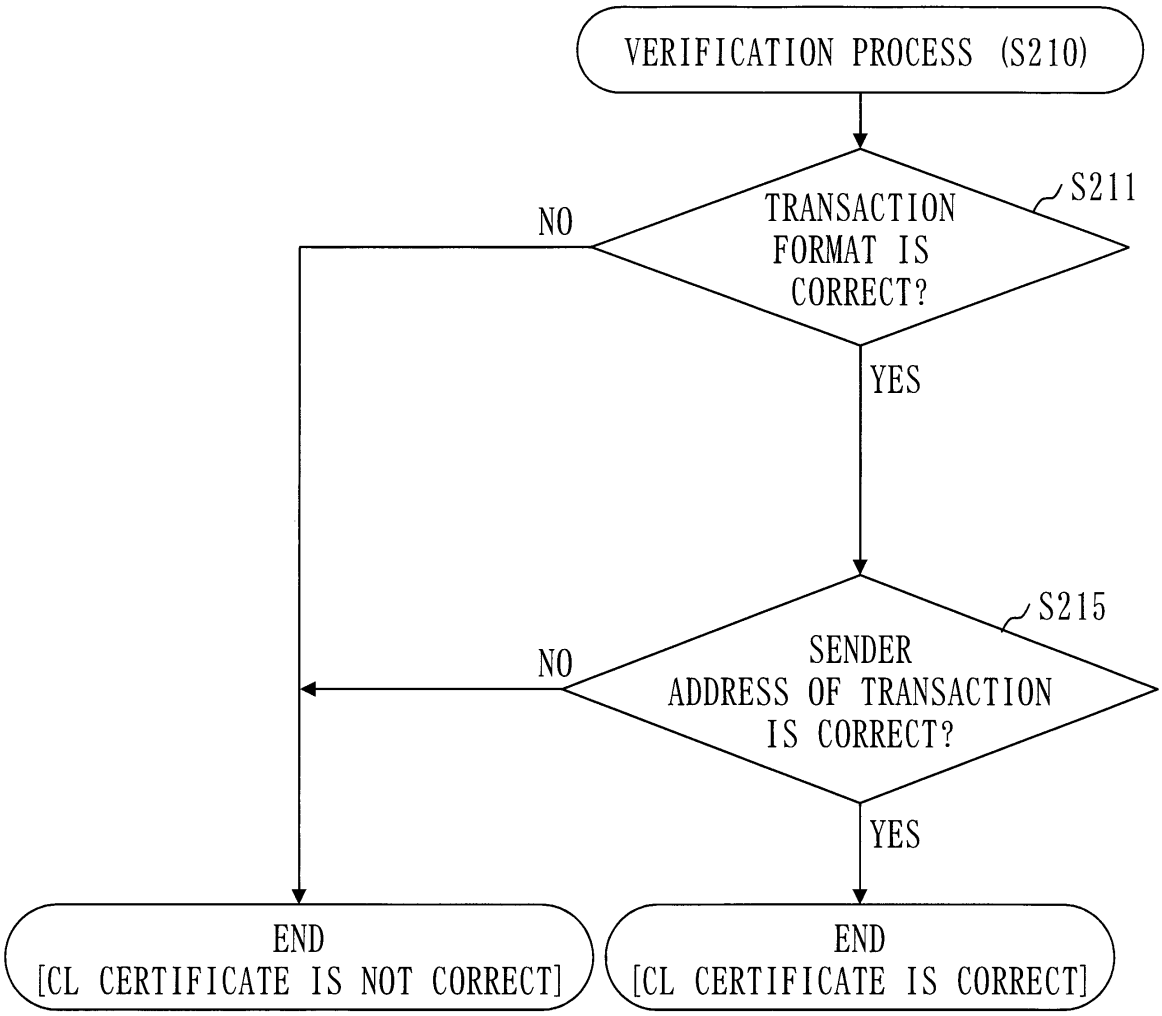

VERIFICATION PROCESS (S210)
S211
TRANSACTION FORMAT IS CORRECT?
NO
YES
S215
SENDER ADDRESS OF TRANSACTION IS CORRECT?
NO
YES
END [CL CERTIFICATE IS NOT CORRECT]
END [CL CERTIFICATE IS CORRECT]

Fig. 28

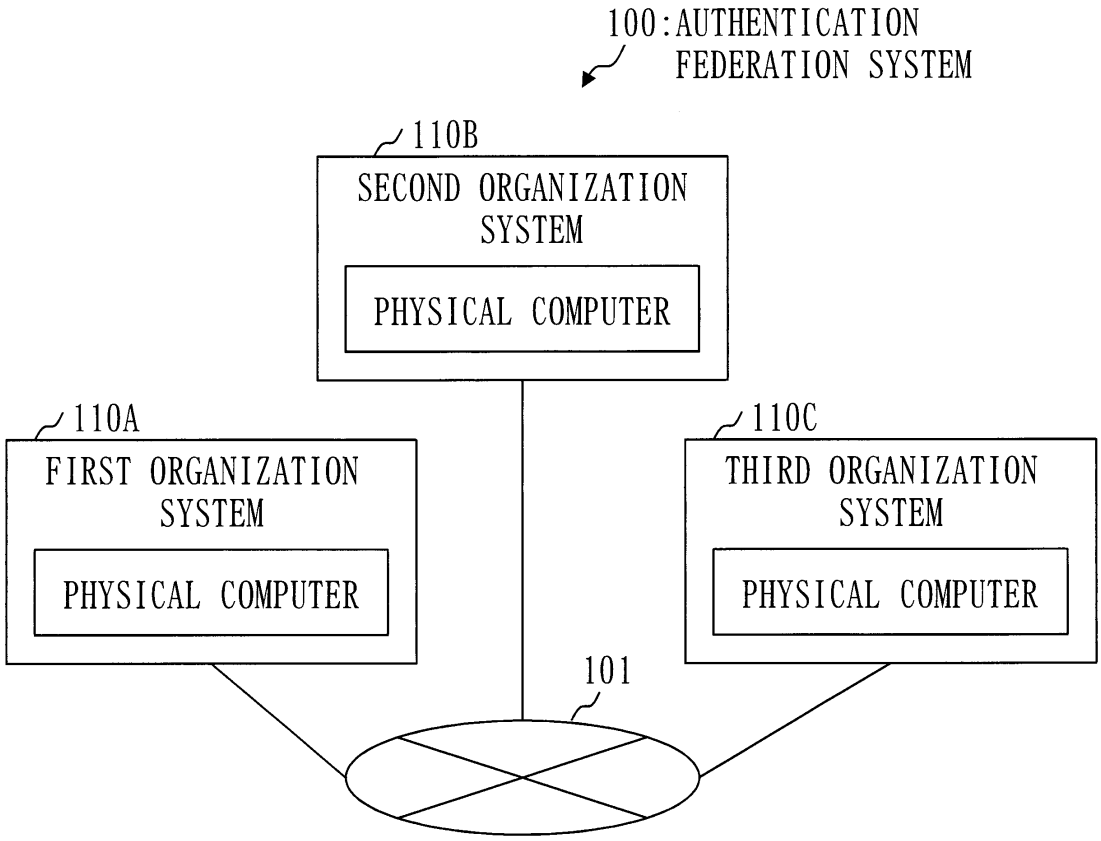

100:AUTHENTICATION FEDERATION SYSTEM
110B
SECOND ORGANIZATION SYSTEM
PHYSICAL COMPUTER
110A
FIRST ORGANIZATION SYSTEM
PHYSICAL COMPUTER
110C
THIRD ORGANIZATION SYSTEM
PHYSICAL COMPUTER
101

Fig. 29

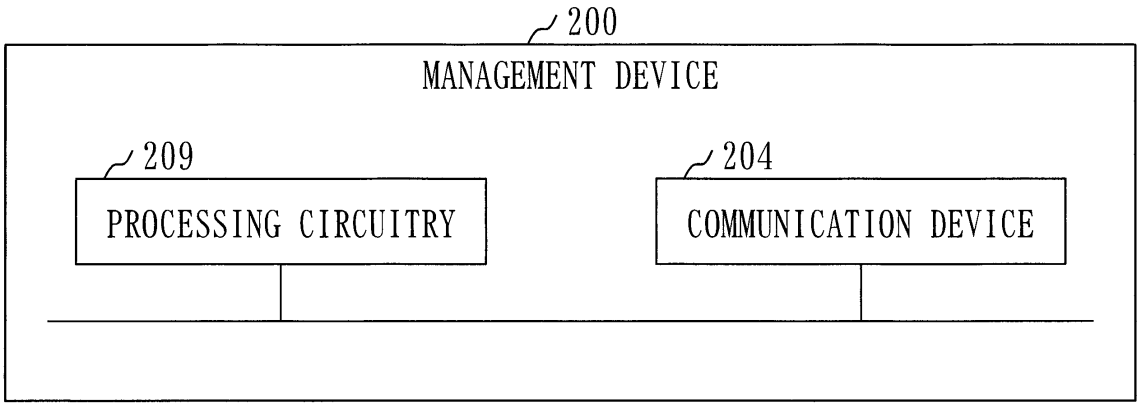

200
MANAGEMENT DEVICE
209
PROCESSING CIRCUITRY
204
COMMUNICATION DEVICE

Fig. 30

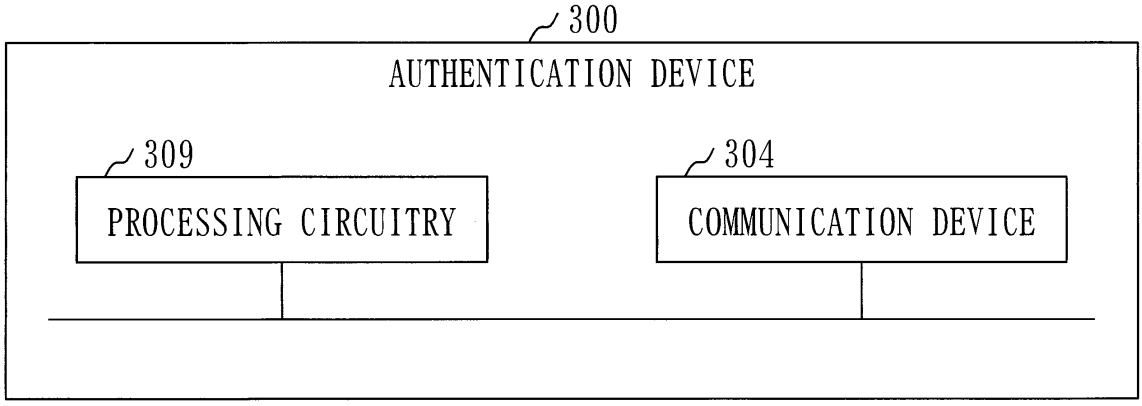
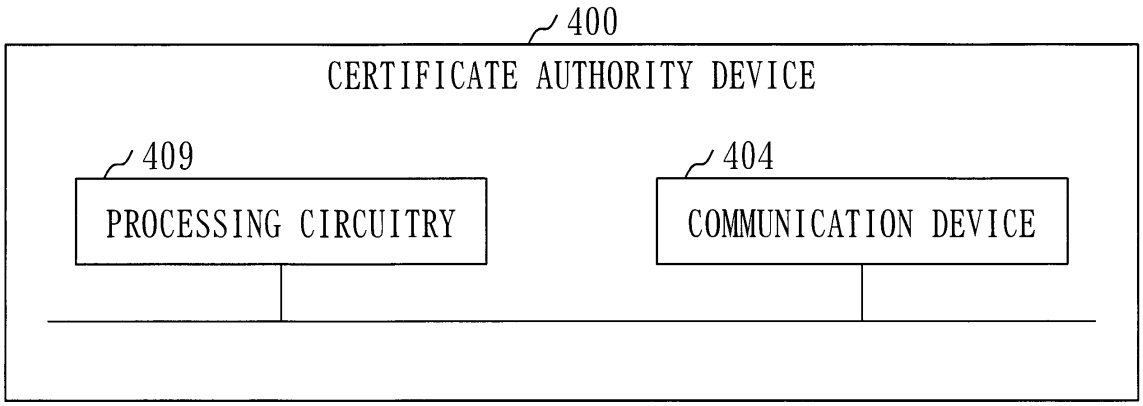

300
AUTHENTICATION DEVICE
309
PROCESSING CIRCUITRY
304
COMMUNICATION DEVICE

Fig. 31


400
CERTIFICATE AUTHORITY DEVICE
409
PROCESSING CIRCUITRY
404
COMMUNICATION DEVICE