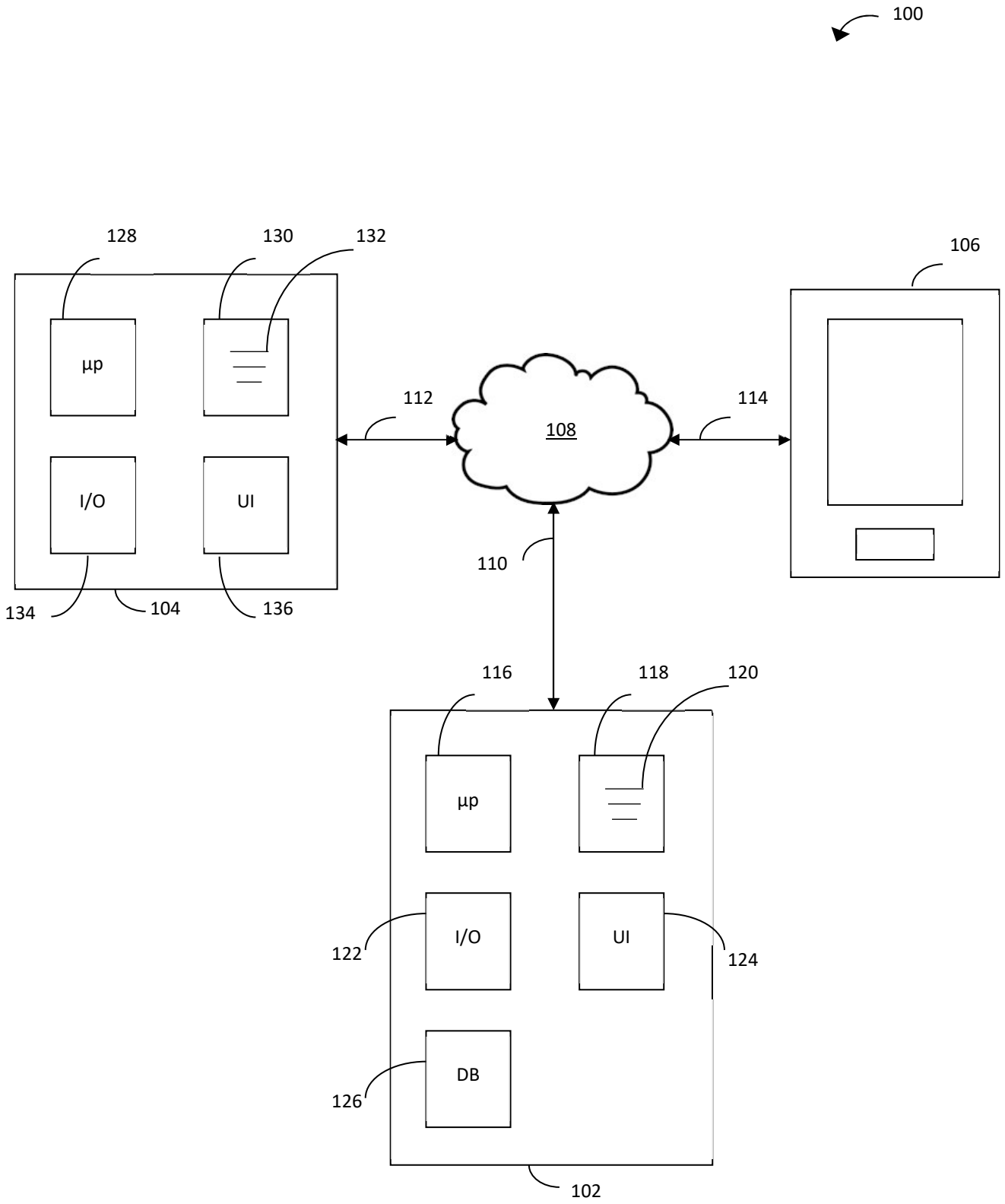
100
128
130
132
106
µp
112
108
114
I/O
UI
110
134
104
136
116
118
120
µp
I/O
UI
122
124
DB
126
102

**FIG. 1**

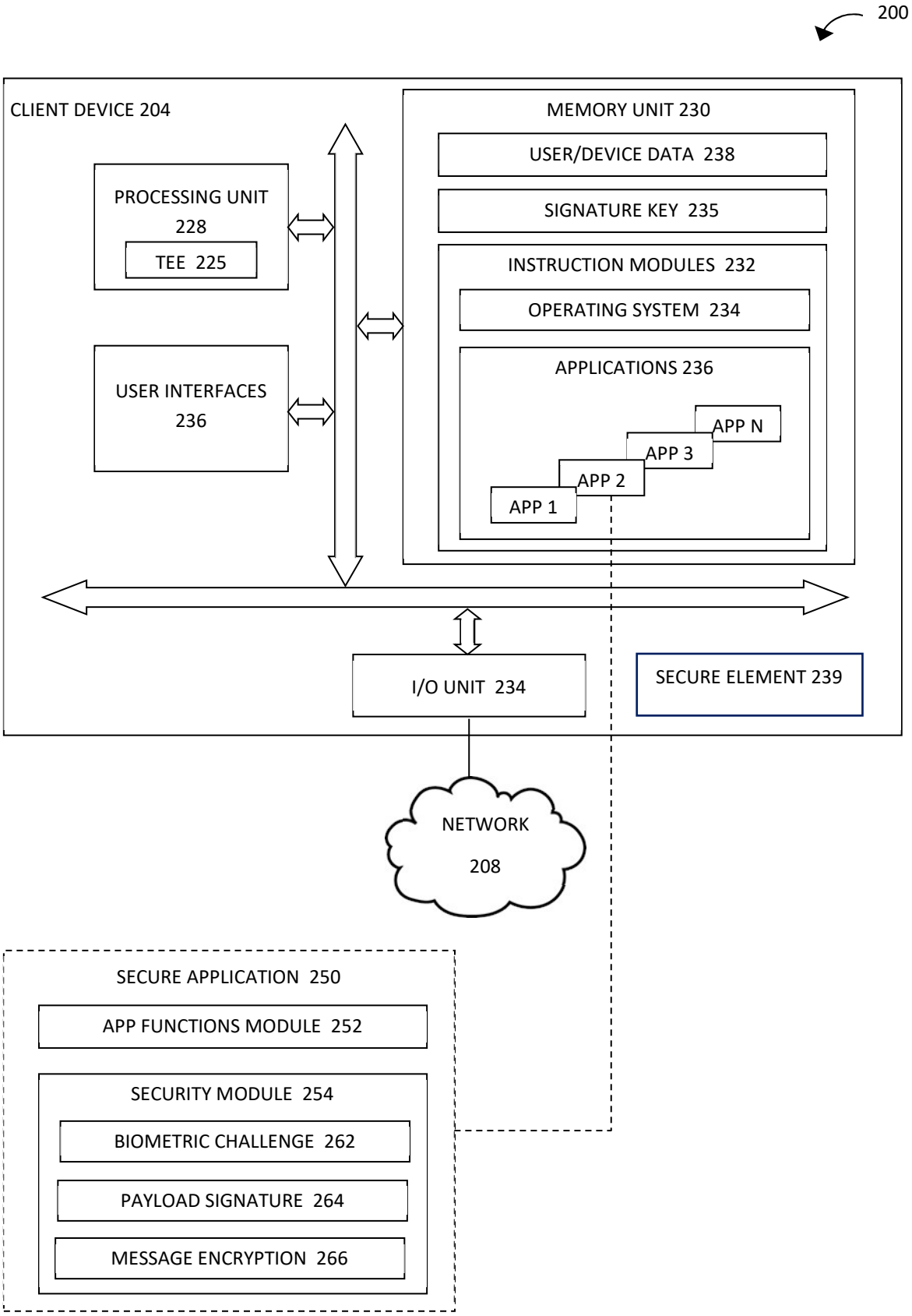
200
CLIENT DEVICE 204
MEMORY UNIT 230
USER/DEVICE DATA 238
SIGNATURE KEY 235
PROCESSING UNIT 228
TEE 225
INSTRUCTION MODULES 232
OPERATING SYSTEM 234
APPLICATIONS 236
USER INTERFACES 236
APP N
APP 3
APP 2
APP 1
I/O UNIT 234
SECURE ELEMENT 239
NETWORK 208
SECURE APPLICATION 250
APP FUNCTIONS MODULE 252
SECURITY MODULE 254
BIOMETRIC CHALLENGE 262
PAYLOAD SIGNATURE 264
MESSAGE ENCRYPTION 266

**FIG. 2**

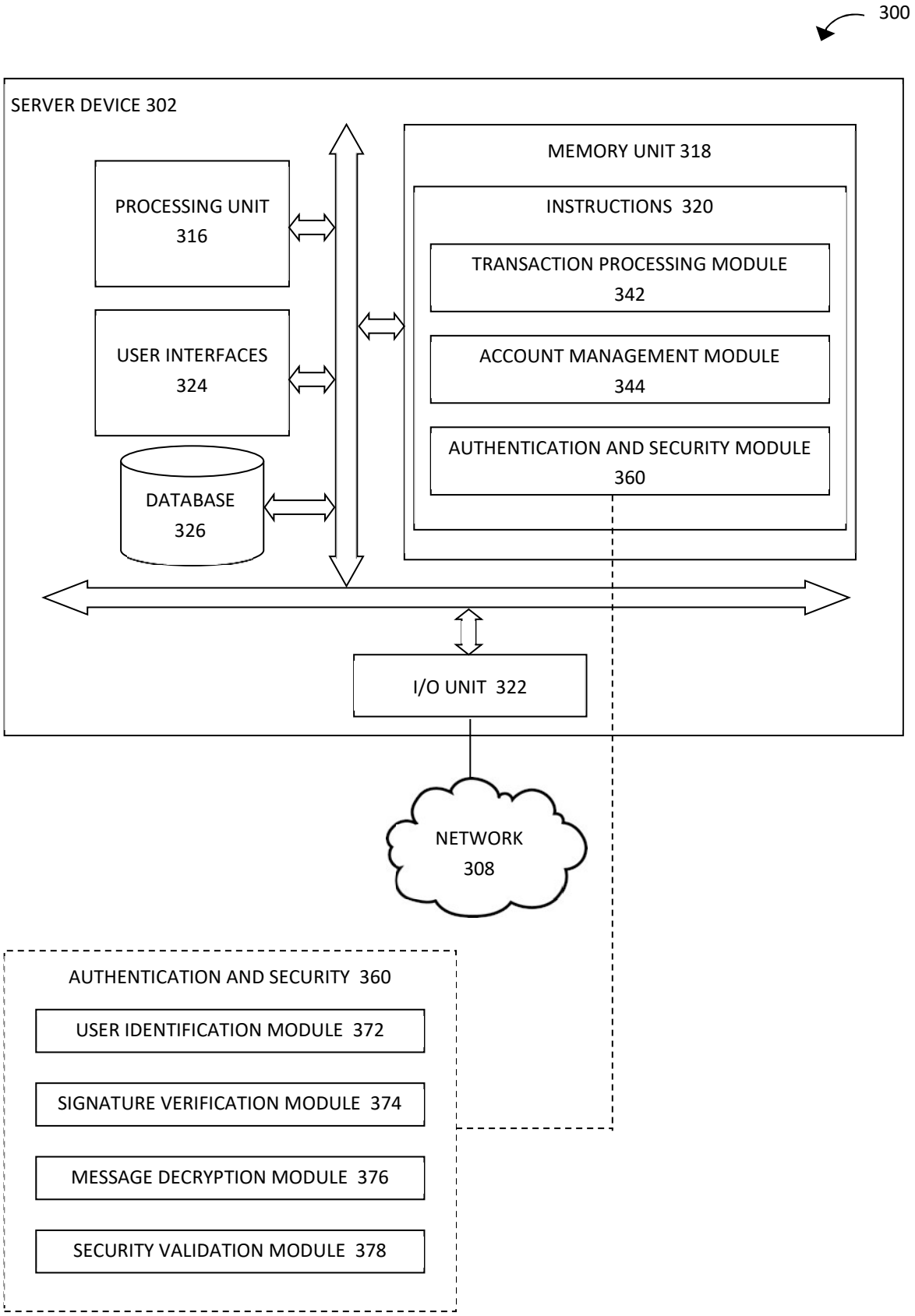
300
SERVER DEVICE 302
PROCESSING UNIT 316
USER INTERFACES 324
DATABASE 326
MEMORY UNIT 318
INSTRUCTIONS 320
TRANSACTION PROCESSING MODULE 342
ACCOUNT MANAGEMENT MODULE 344
AUTHENTICATION AND SECURITY MODULE 360
I/O UNIT 322
NETWORK 308
AUTHENTICATION AND SECURITY 360
USER IDENTIFICATION MODULE 372
SIGNATURE VERIFICATION MODULE 374
MESSAGE DECRYPTION MODULE 376
SECURITY VALIDATION MODULE 378

**FIG. 3**

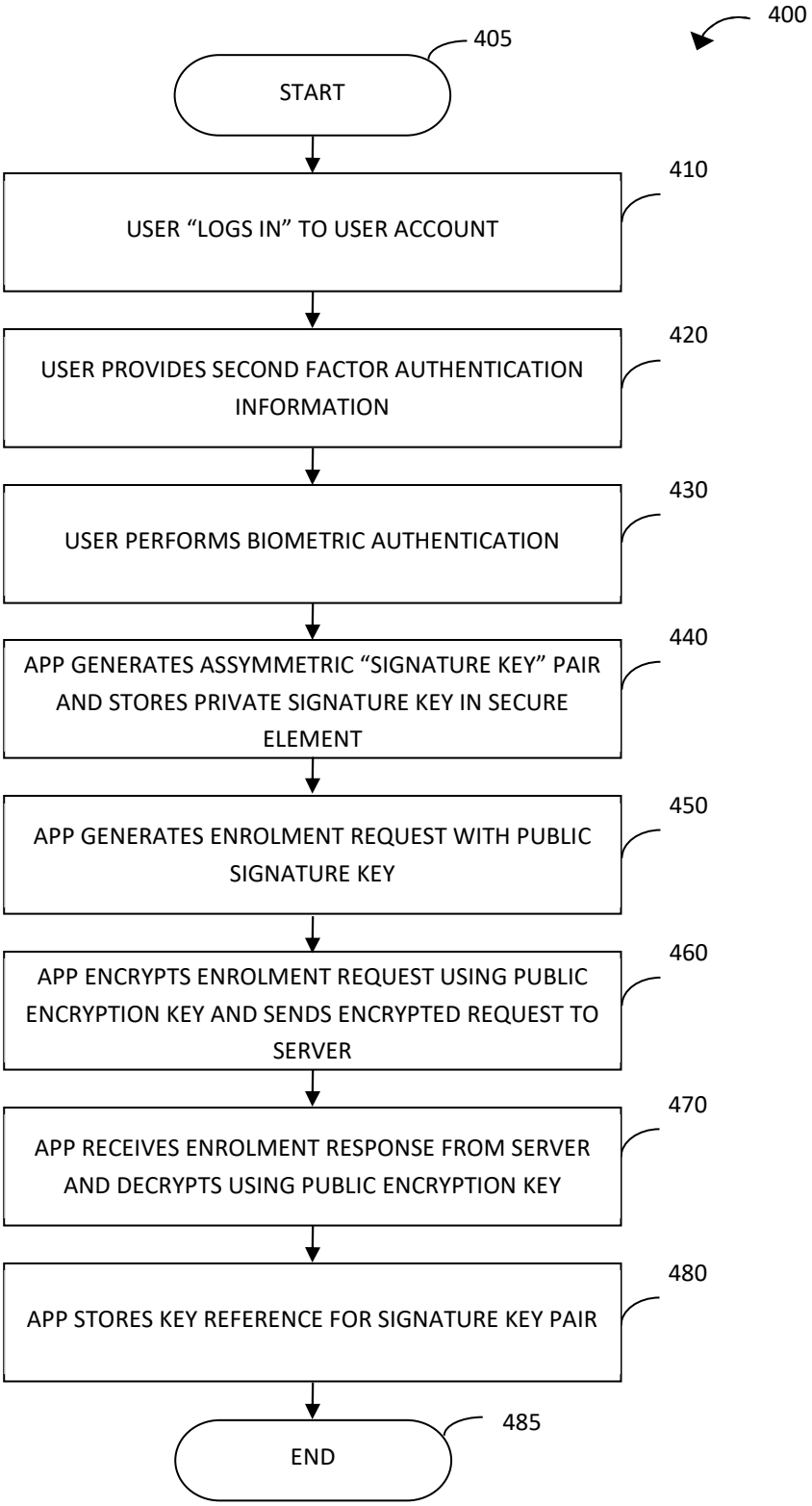
400
405
START
410
USER "LOGS IN" TO USER ACCOUNT
420
USER PROVIDES SECOND FACTOR AUTHENTICATION INFORMATION
430
USER PERFORMS BIOMETRIC AUTHENTICATION
440
APP GENERATES ASSYMMETRIC "SIGNATURE KEY" PAIR AND STORES PRIVATE SIGNATURE KEY IN SECURE ELEMENT
450
APP GENERATES ENROLMENT REQUEST WITH PUBLIC SIGNATURE KEY
460
APP ENCRYPTS ENROLMENT REQUEST USING PUBLIC ENCRYPTION KEY AND SENDS ENCRYPTED REQUEST TO SERVER
470
APP RECEIVES ENROLMENT RESPONSE FROM SERVER AND DECRYPTS USING PUBLIC ENCRYPTION KEY
480
APP STORES KEY REFERENCE FOR SIGNATURE KEY PAIR
485
END

**FIG. 4**

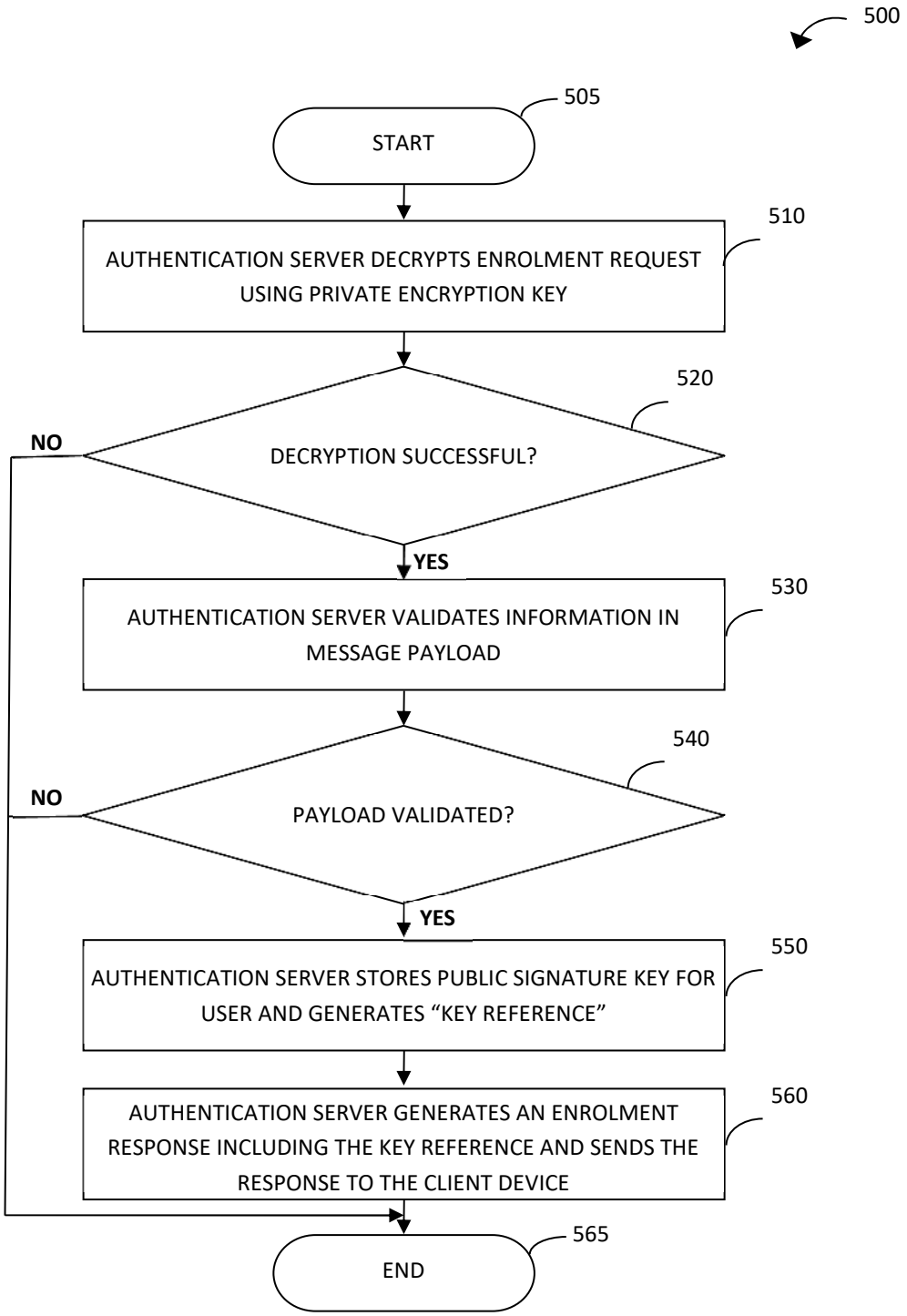
500
505
START
510
AUTHENTICATION SERVER DECRYPTS ENROLMENT REQUEST USING PRIVATE ENCRYPTION KEY
520
DECRYPTION SUCCESSFUL?
NO
YES
530
AUTHENTICATION SERVER VALIDATES INFORMATION IN MESSAGE PAYLOAD
540
PAYLOAD VALIDATED?
NO
YES
550
AUTHENTICATION SERVER STORES PUBLIC SIGNATURE KEY FOR USER AND GENERATES "KEY REFERENCE"
560
AUTHENTICATION SERVER GENERATES AN ENROLMENT RESPONSE INCLUDING THE KEY REFERENCE AND SENDS THE RESPONSE TO THE CLIENT DEVICE
565
END

**FIG. 5**

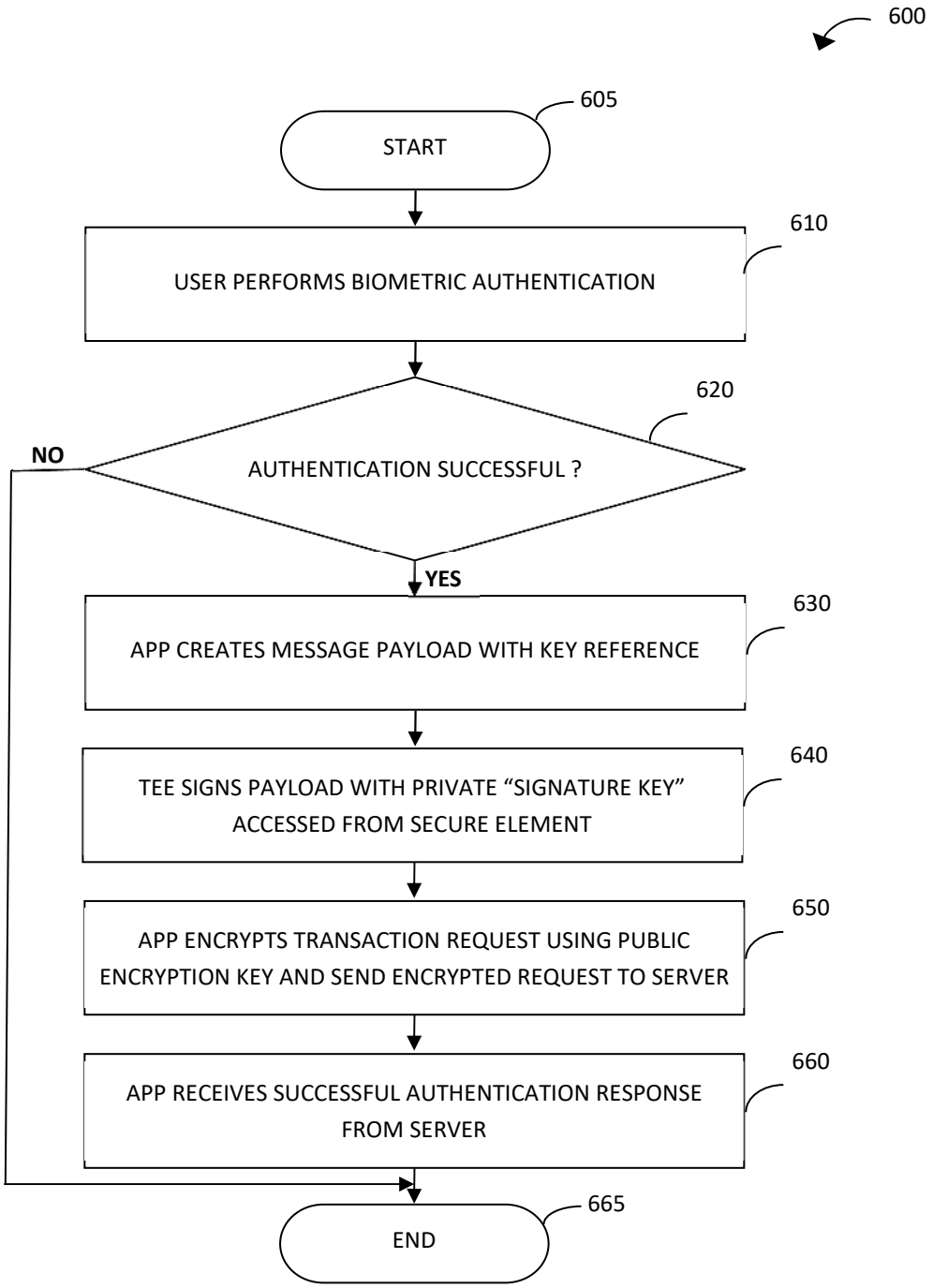
600
605
START
610
USER PERFORMS BIOMETRIC AUTHENTICATION
620
NO
AUTHENTICATION SUCCESSFUL ?
YES
630
APP CREATES MESSAGE PAYLOAD WITH KEY REFERENCE
640
TEE SIGNS PAYLOAD WITH PRIVATE "SIGNATURE KEY" ACCESSED FROM SECURE ELEMENT
650
APP ENCRYPTS TRANSACTION REQUEST USING PUBLIC ENCRYPTION KEY AND SEND ENCRYPTED REQUEST TO SERVER
660
APP RECEIVES SUCCESSFUL AUTHENTICATION RESPONSE FROM SERVER
665
END

**FIG. 6**

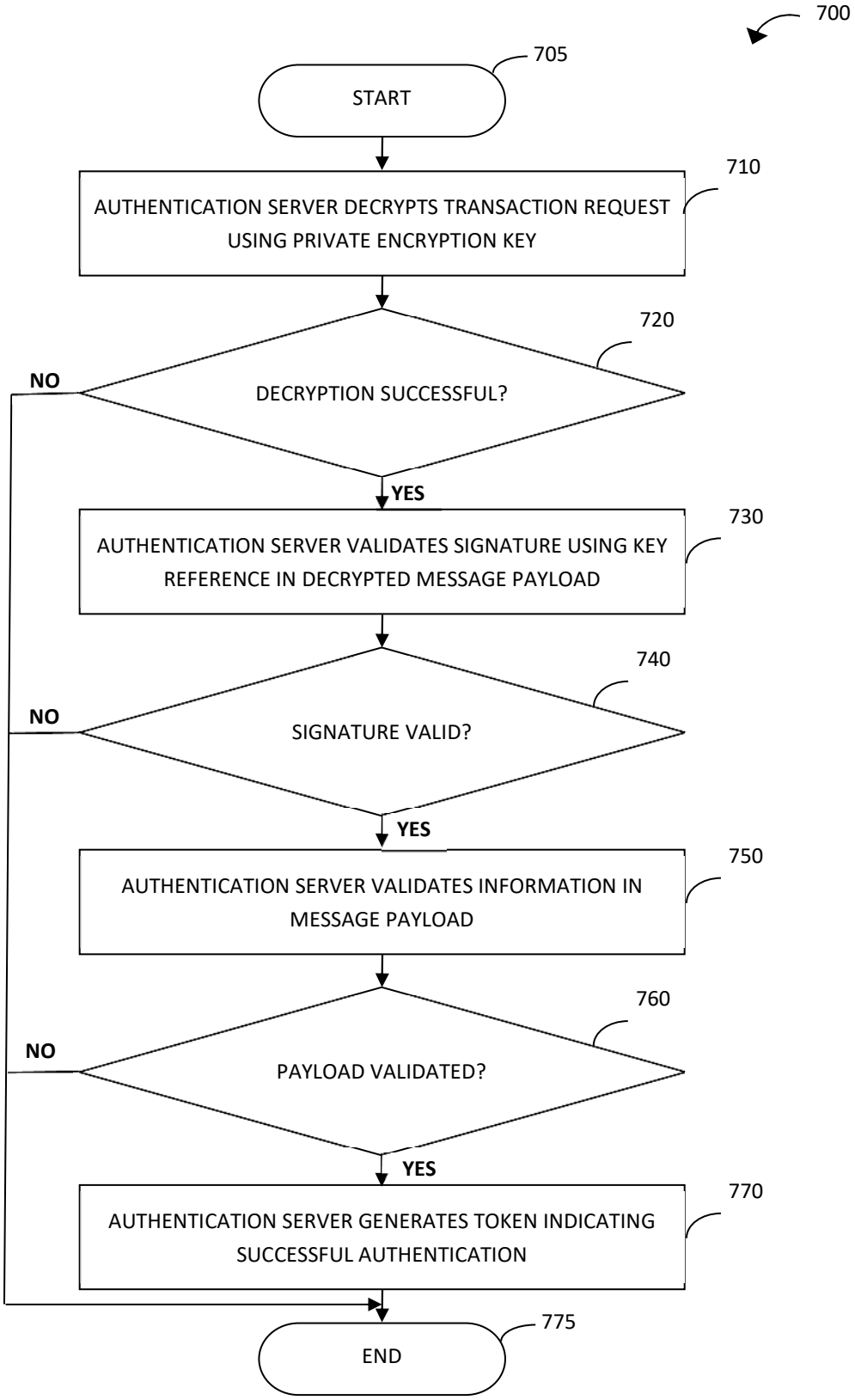
700
705
START
710
AUTHENTICATION SERVER DECRYPTS TRANSACTION REQUEST USING PRIVATE ENCRYPTION KEY
720
DECRYPTION SUCCESSFUL?
NO
YES
730
AUTHENTICATION SERVER VALIDATES SIGNATURE USING KEY REFERENCE IN DECRYPTED MESSAGE PAYLOAD
740
SIGNATURE VALID?
NO
YES
750
AUTHENTICATION SERVER VALIDATES INFORMATION IN MESSAGE PAYLOAD
760
PAYLOAD VALIDATED?
NO
YES
770
AUTHENTICATION SERVER GENERATES TOKEN INDICATING SUCCESSFUL AUTHENTICATION
775
END

**FIG. 7**