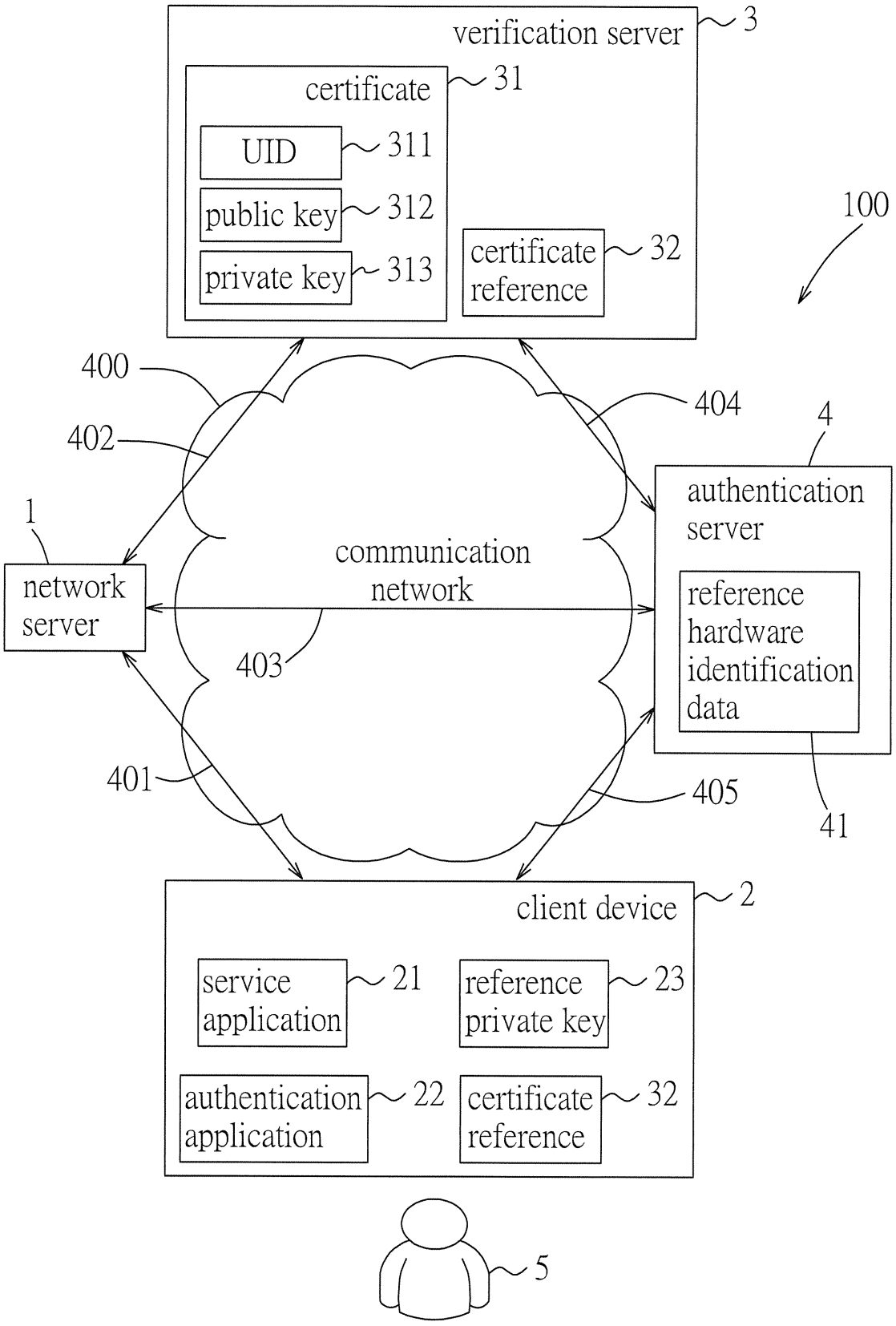
verification server
3
certificate
31
UID
311
public key
312
private key
313
certificate reference
32
100
400
402
404
4
authentication server
1
network server
communication network
reference hardware identification data
403
401
405
41
client device
2
service application
21
reference private key
23
authentication application
22
certificate reference
32
5

FIG.1

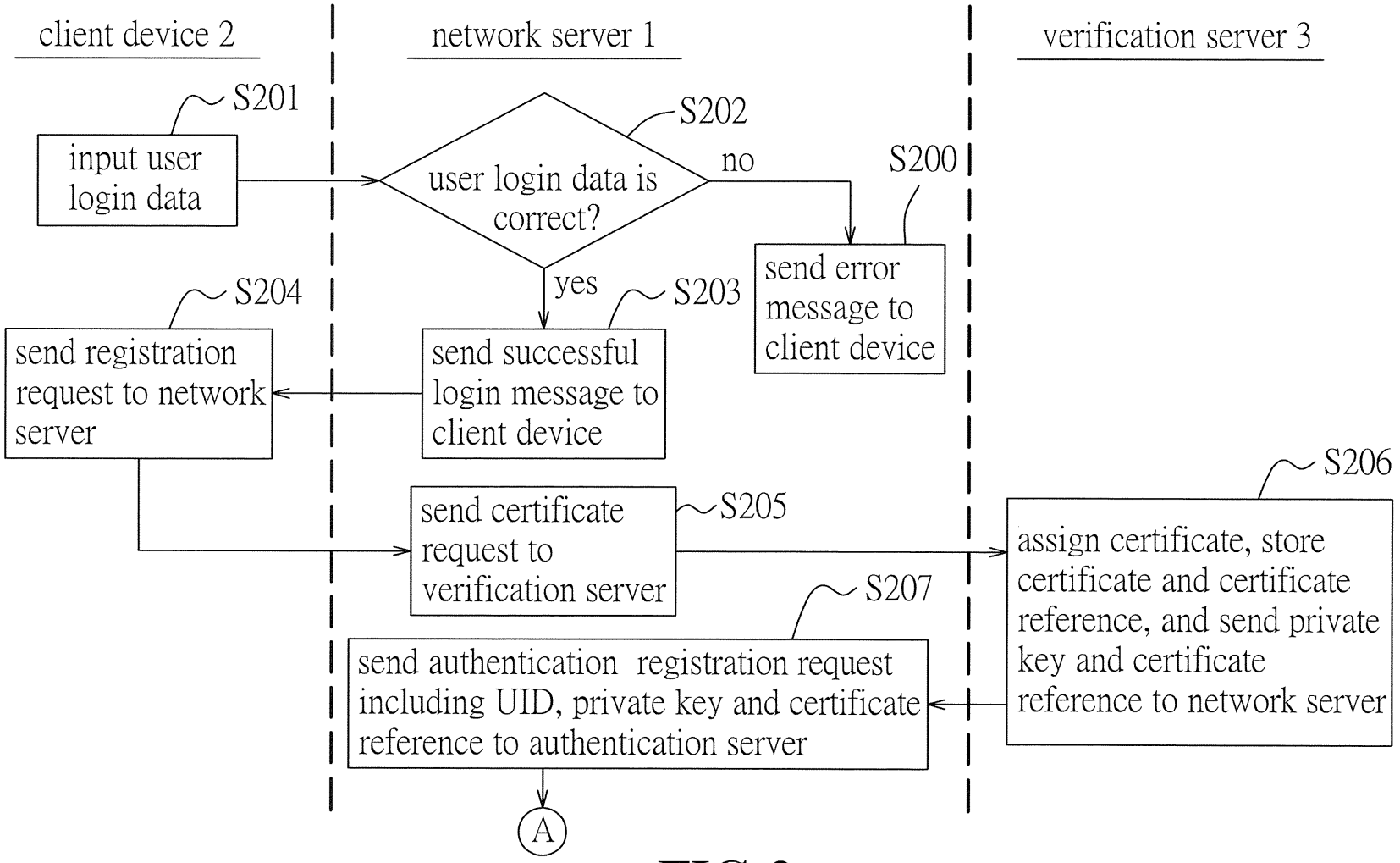
client device 2
network server 1
verification server 3
S201
input user login data
S202
user login data is correct?
no
S200
send error message to client device
yes
S203
send successful login message to client device
S204
send registration request to network server
send certificate request to verification server
S205
S206
assign certificate, store certificate and certificate reference, and send private key and certificate reference to network server
S207
send authentication registration request including UID, private key and certificate reference to authentication server
A

FIG.2a

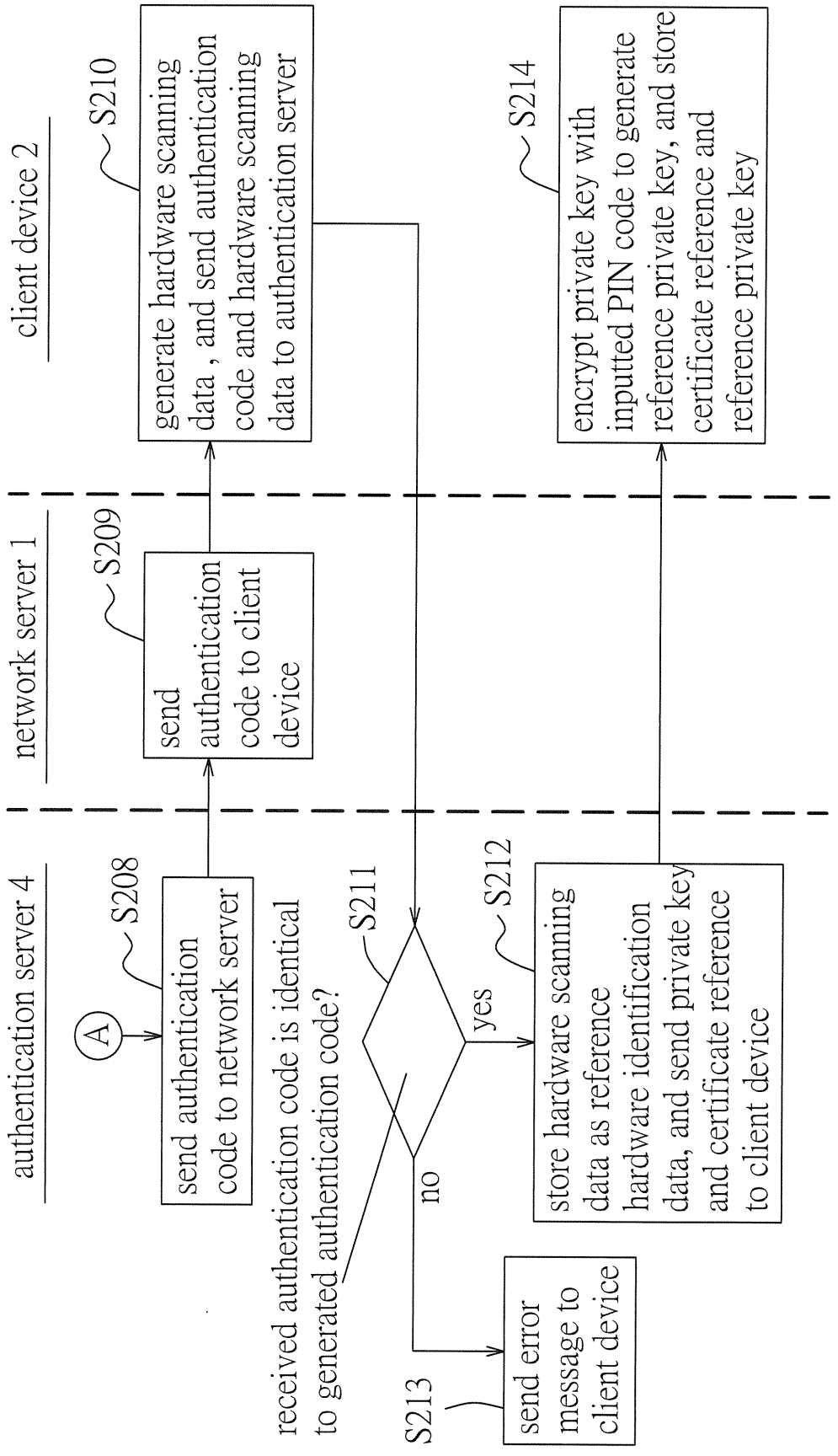
client device 2
network server 1
authentication server 4
S210
generate hardware scanning data , and send authentication code and hardware scanning data to authentication server
S209
send authentication code to client device
S214
encrypt private key with inputted PIN code to generate reference private key, and store certificate reference and reference private key
A
S208
send authentication code to network server
S211
received authentication code is identical to generated authentication code?
yes
S212
store hardware scanning data as reference hardware identification data, and send private key and certificate reference to client device
no
S213
send error message to client device

FIG.2b

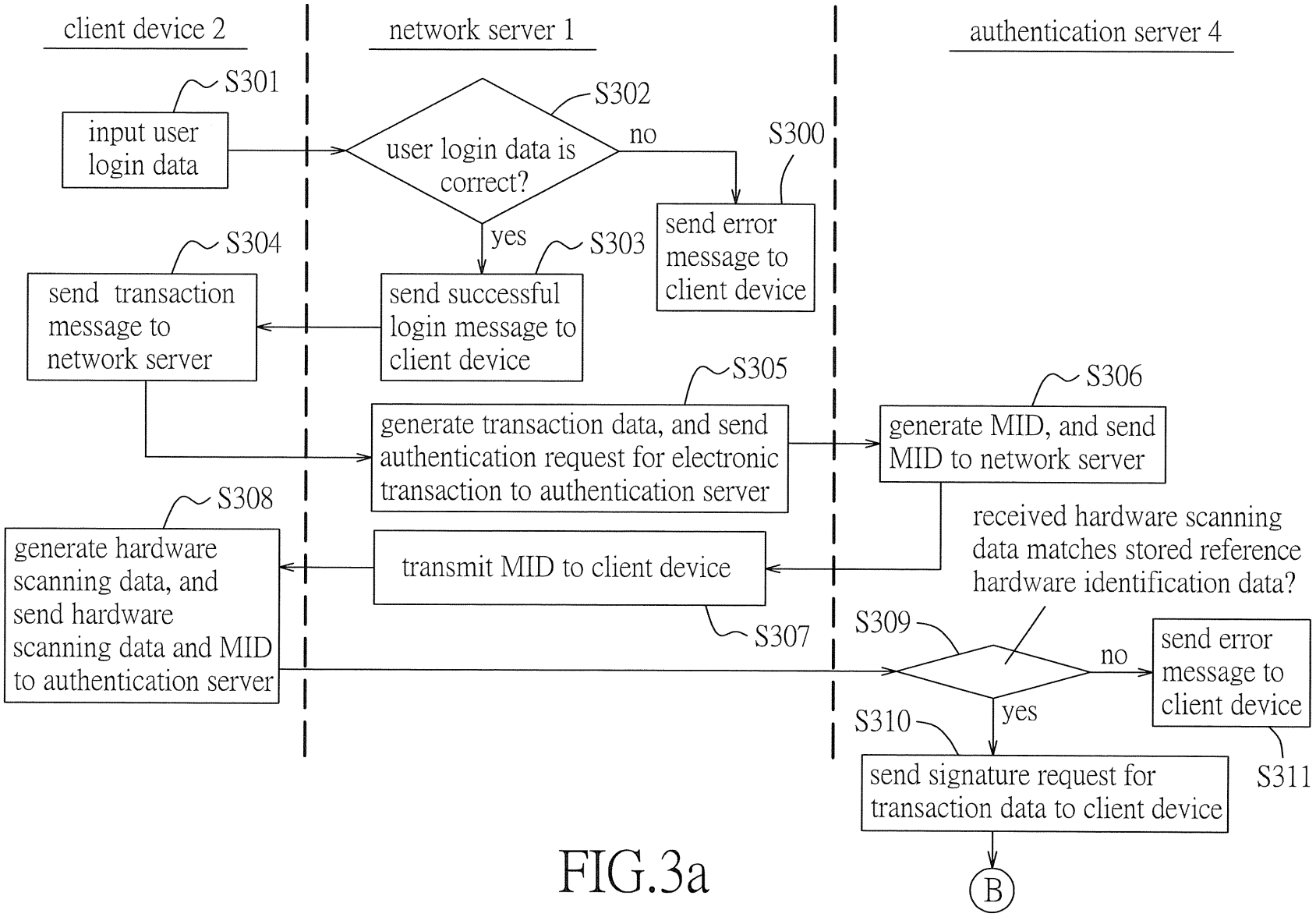
client device 2
network server 1
authentication server 4
S301
input user login data
S302
user login data is correct?
no
S300
send error message to client device
yes
S303
send successful login message to client device
S304
send transaction message to network server
S305
generate transaction data, and send authentication request for electronic transaction to authentication server
S306
generate MID, and send MID to network server
S308
generate hardware scanning data, and send hardware scanning data and MID to authentication server
transmit MID to client device
S307
received hardware scanning data matches stored reference hardware identification data?
S309
no
send error message to client device
S311
yes
S310
send signature request for transaction data to client device
B

FIG.3a

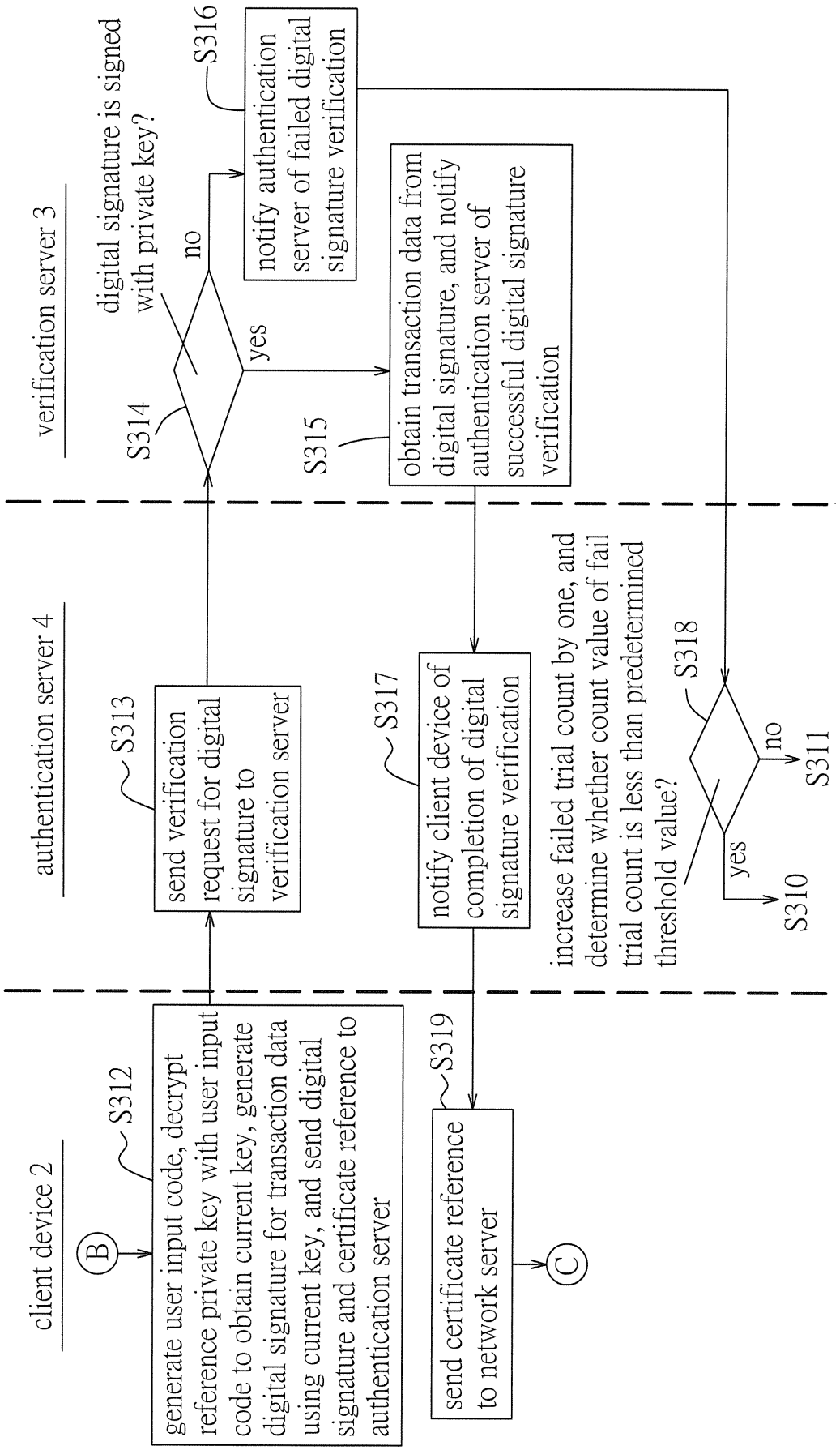
client device 2
authentication server 4
verification server 3
B
S312
generate user input code, decrypt reference private key with user input code to obtain current key, generate digital signature for transaction data using current key, and send digital signature and certificate reference to authentication server
S313
send verification request for digital signature to verification server
digital signature is signed with private key?
S314
no
yes
S316
notify authentication server of failed digital signature verification
S315
obtain transaction data from digital signature, and notify authentication server of successful digital signature verification
S317
notify client device of completion of digital signature verification
increase failed trial count by one, and determine whether count value of fail trial count is less than predetermined threshold value?
S318
yes
no
S310
S311
S319
send certificate reference to network server
C

FIG.3b

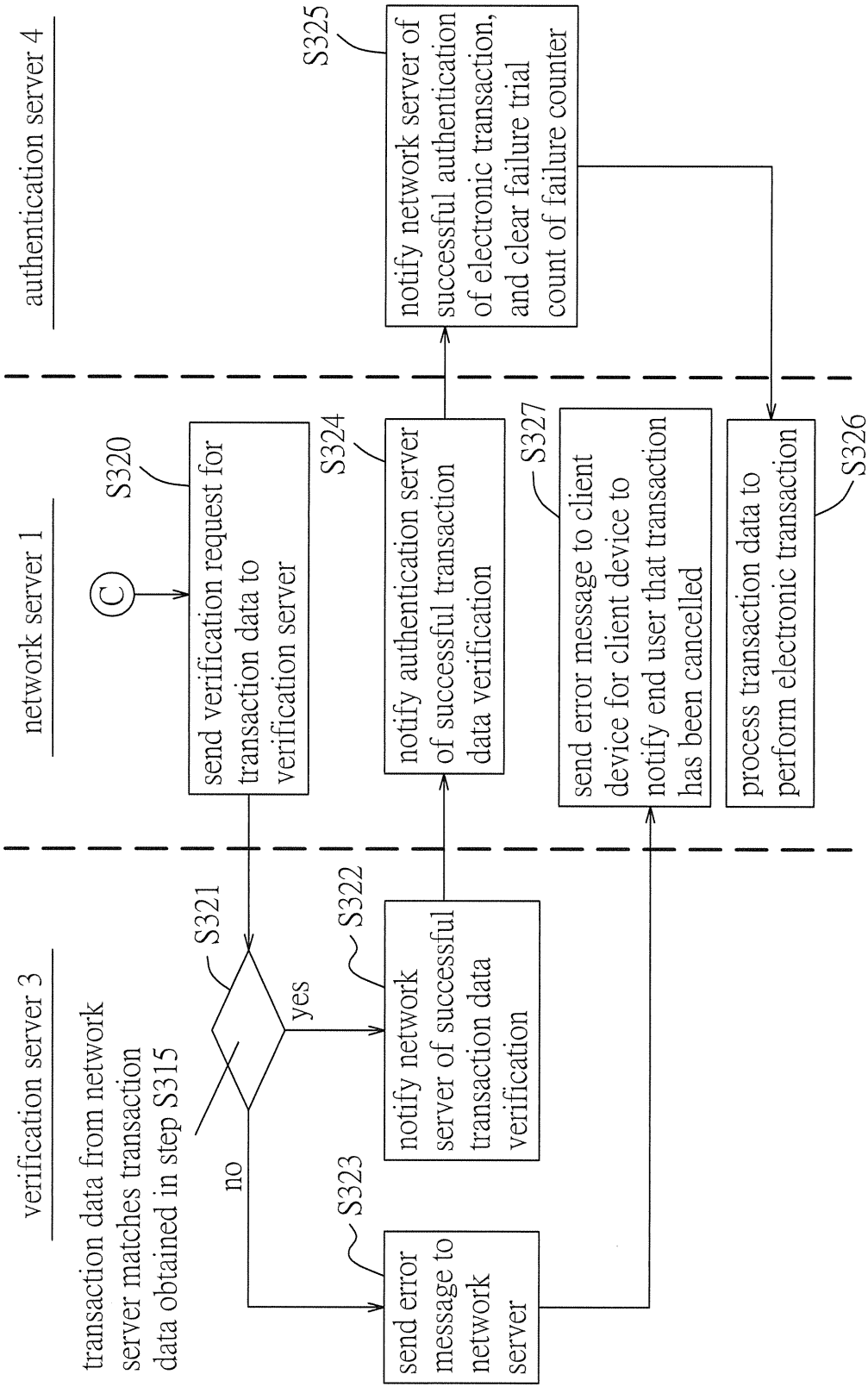
verification server 3
network server 1
authentication server 4
transaction data from network server matches transaction data obtained in step S315
S321
yes
no
S322
S323
S320
S324
S325
S326
S327
send error message to network server
notify network server of successful transaction data verification
send verification request for transaction data to verification server
notify authentication server of successful transaction data verification
notify network server of successful authentication of electronic transaction, and clear failure trial count of failure counter
send error message to client device for client device to notify end user that transaction has been cancelled
process transaction data to perform electronic transaction

FIG.3C