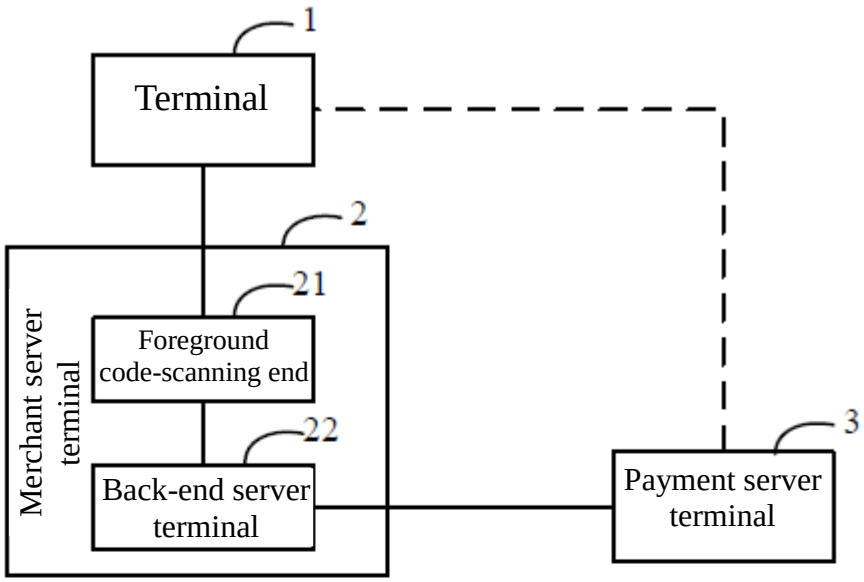

1
Terminal
2
Merchant server terminal
21
Foreground code-scanning end
22
Back-end server terminal
3
Payment server terminal

FIG. 1

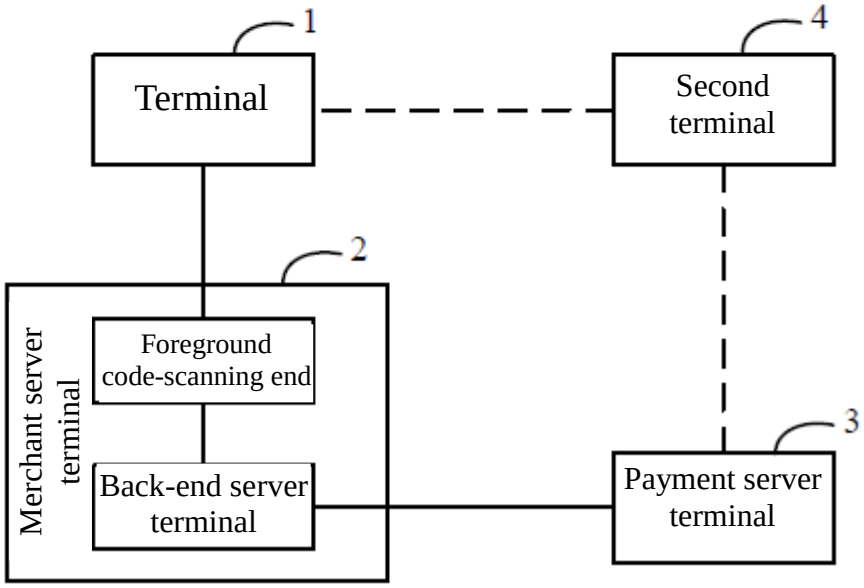

1
Terminal
4
Second terminal
2
Merchant server terminal
Foreground code-scanning end
Back-end server terminal
3
Payment server terminal

FIG. 2

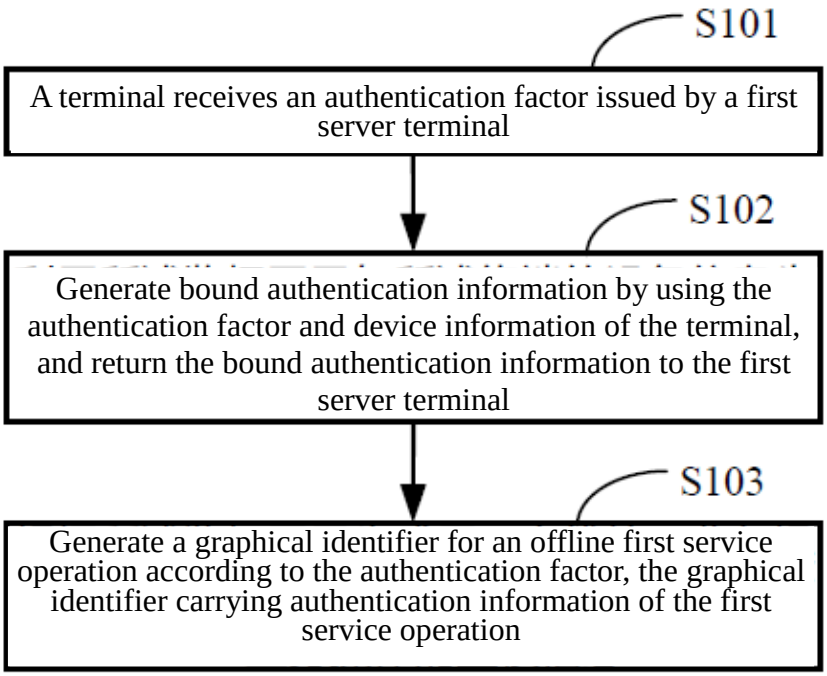

S101
A terminal receives an authentication factor issued by a first server terminal
S102
Generate bound authentication information by using the authentication factor and device information of the terminal, and return the bound authentication information to the first server terminal
S103
Generate a graphical identifier for an offline first service operation according to the authentication factor, the graphical identifier carrying authentication information of the first service operation

FIG. 3a

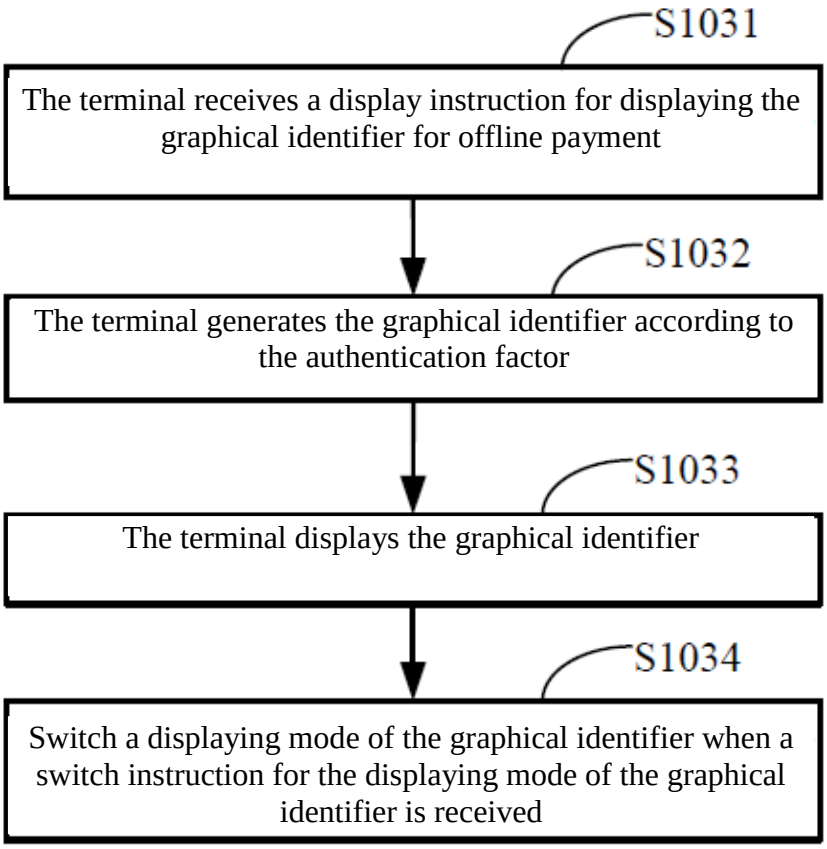

S1031
The terminal receives a display instruction for displaying the graphical identifier for offline payment
S1032
The terminal generates the graphical identifier according to the authentication factor
S1033
The terminal displays the graphical identifier
S1034
Switch a displaying mode of the graphical identifier when a switch instruction for the displaying mode of the graphical identifier is received

FIG. 3b

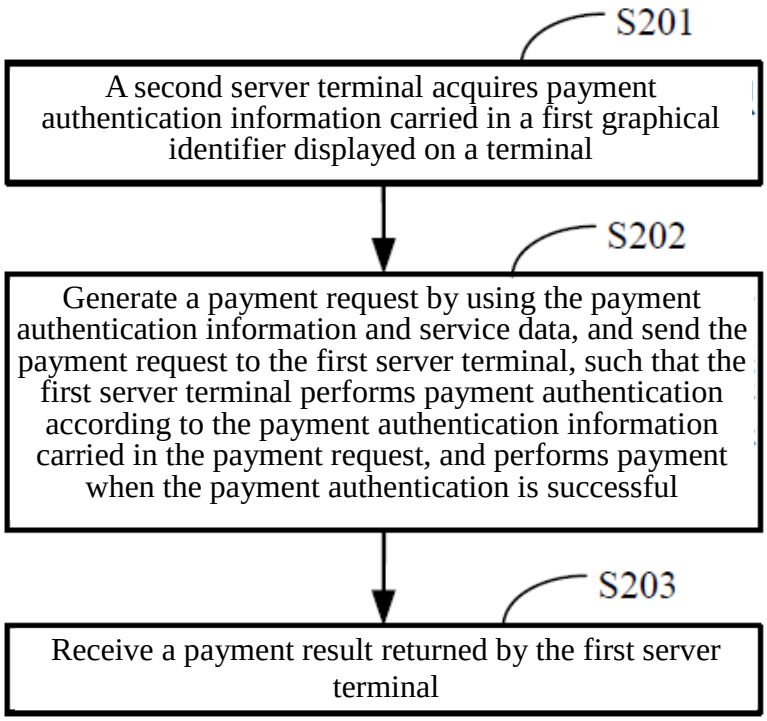

S201
A second server terminal acquires payment authentication information carried in a first graphical identifier displayed on a terminal
S202
Generate a payment request by using the payment authentication information and service data, and send the payment request to the first server terminal, such that the first server terminal performs payment authentication according to the payment authentication information carried in the payment request, and performs payment when the payment authentication is successful
S203
Receive a payment result returned by the first server terminal

FIG. 4 4

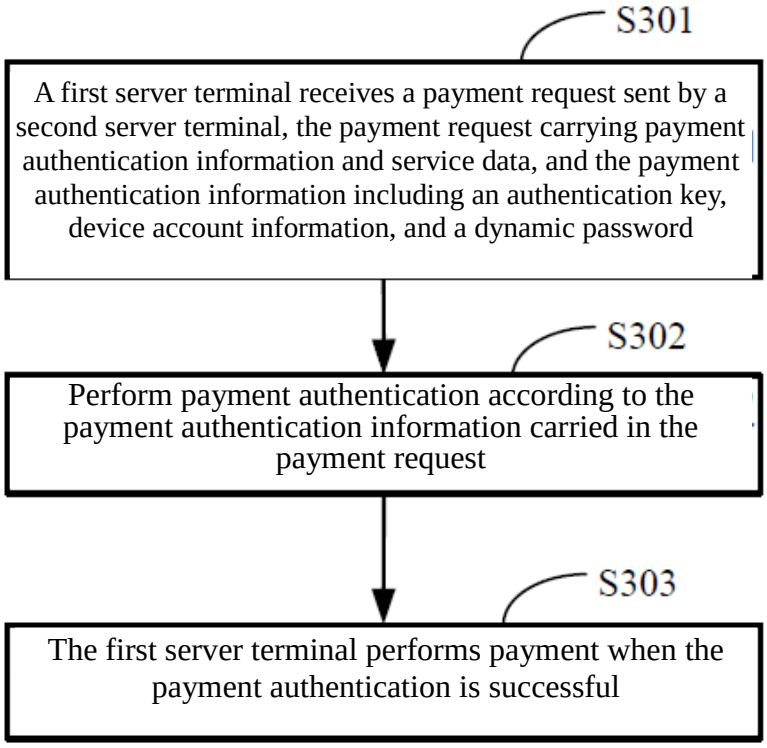

S301
A first server terminal receives a payment request sent by a second server terminal, the payment request carrying payment authentication information and service data, and the payment authentication information including an authentication key, device account information, and a dynamic password
S302
Perform payment authentication according to the payment authentication information carried in the payment request
S303
The first server terminal performs payment when the payment authentication is successful

FIG. 5a

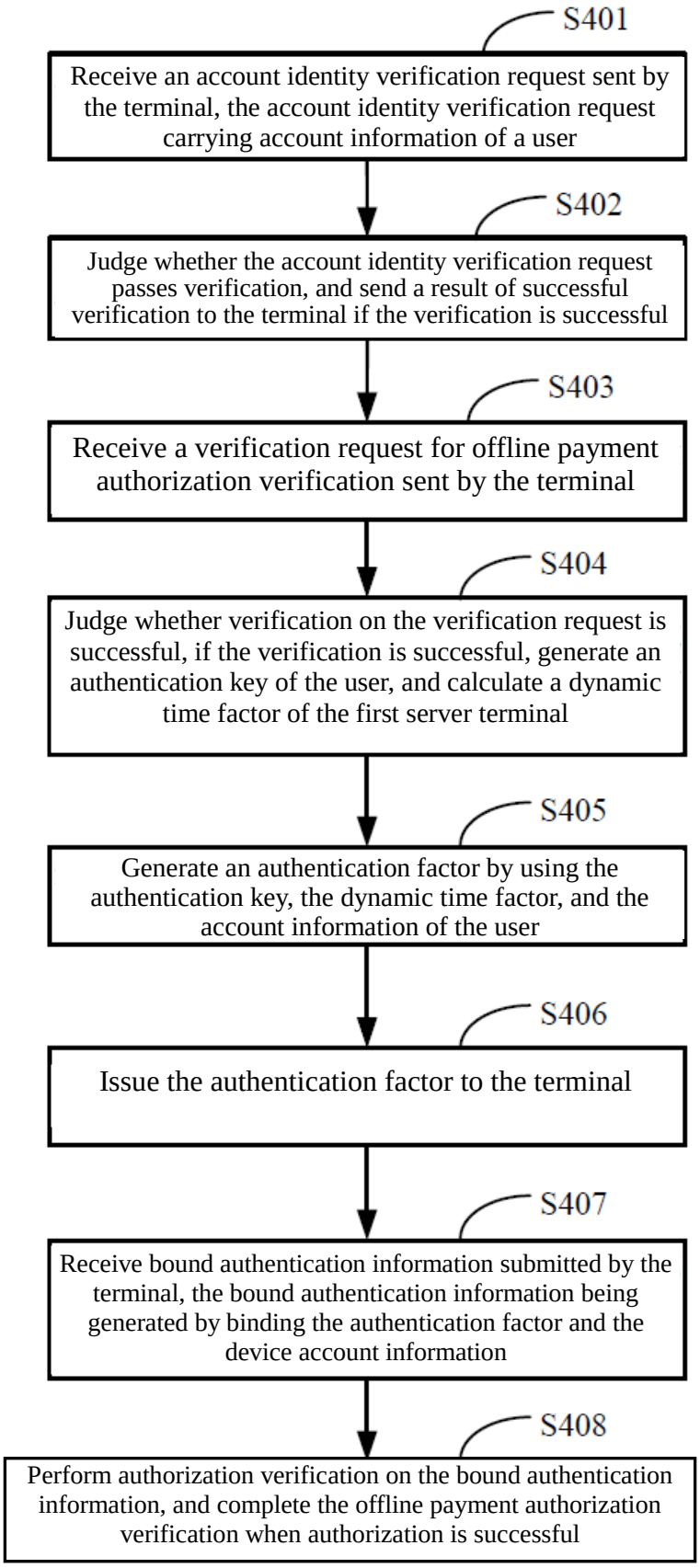

S401
Receive an account identity verification request sent by the terminal, the account identity verification request carrying account information of a user
S402
Judge whether the account identity verification request passes verification, and send a result of successful verification to the terminal if the verification is successful
S403
Receive a verification request for offline payment authorization verification sent by the terminal
S404
Judge whether verification on the verification request is successful, if the verification is successful, generate an authentication key of the user, and calculate a dynamic time factor of the first server terminal
S405
Generate an authentication factor by using the authentication key, the dynamic time factor, and the account information of the user
S406
Issue the authentication factor to the terminal
S407
Receive bound authentication information submitted by the terminal, the bound authentication information being generated by binding the authentication factor and the device account information
S408
Perform authorization verification on the bound authentication information, and complete the offline payment authorization verification when authorization is successful

FIG. 5b

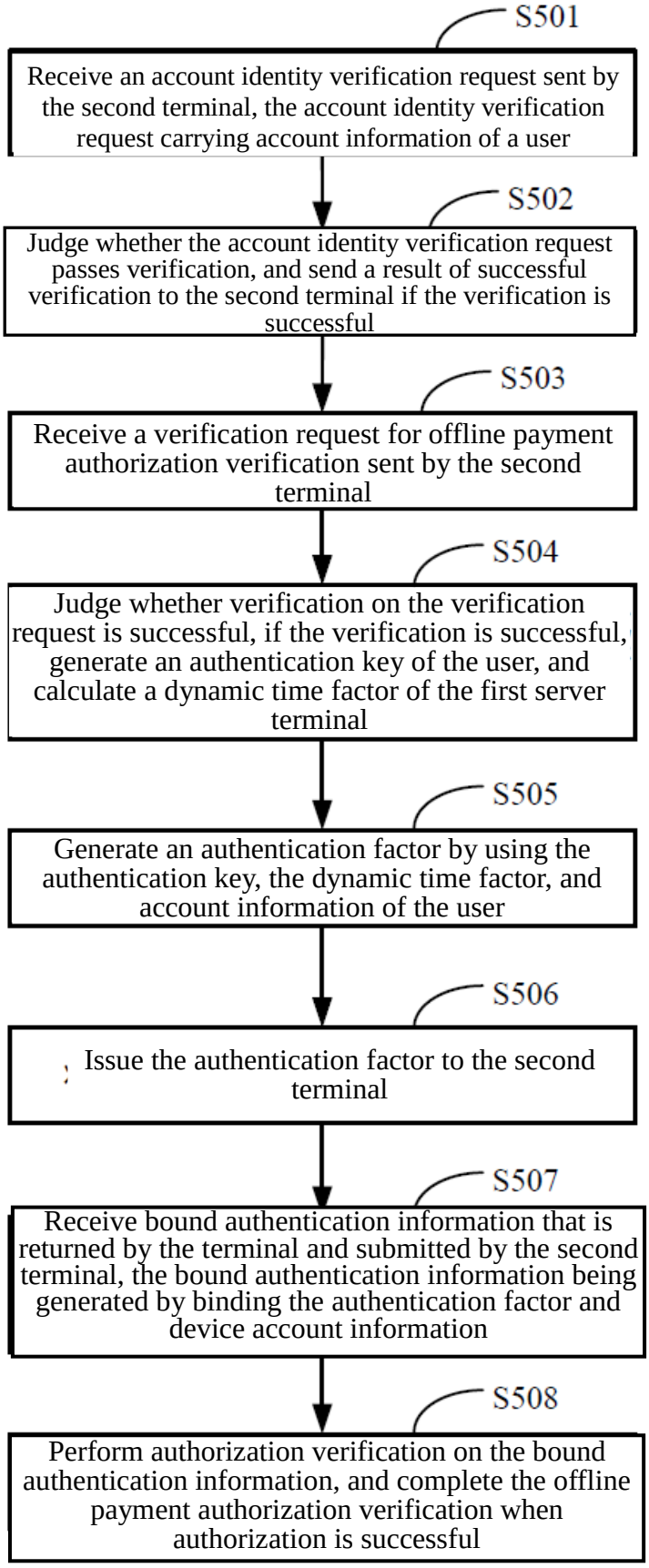

S501
Receive an account identity verification request sent by the second terminal, the account identity verification request carrying account information of a user
S502
Judge whether the account identity verification request passes verification, and send a result of successful verification to the second terminal if the verification is successful
S503
Receive a verification request for offline payment authorization verification sent by the second terminal
S504
Judge whether verification on the verification request is successful, if the verification is successful, generate an authentication key of the user, and calculate a dynamic time factor of the first server terminal
S505
Generate an authentication factor by using the authentication key, the dynamic time factor, and account information of the user
S506
Issue the authentication factor to the second terminal
S507
Receive bound authentication information that is returned by the terminal and submitted by the second terminal, the bound authentication information being generated by binding the authentication factor and device account information
S508
Perform authorization verification on the bound authentication information, and complete the offline payment authorization verification when authorization is successful

FIG. 5c

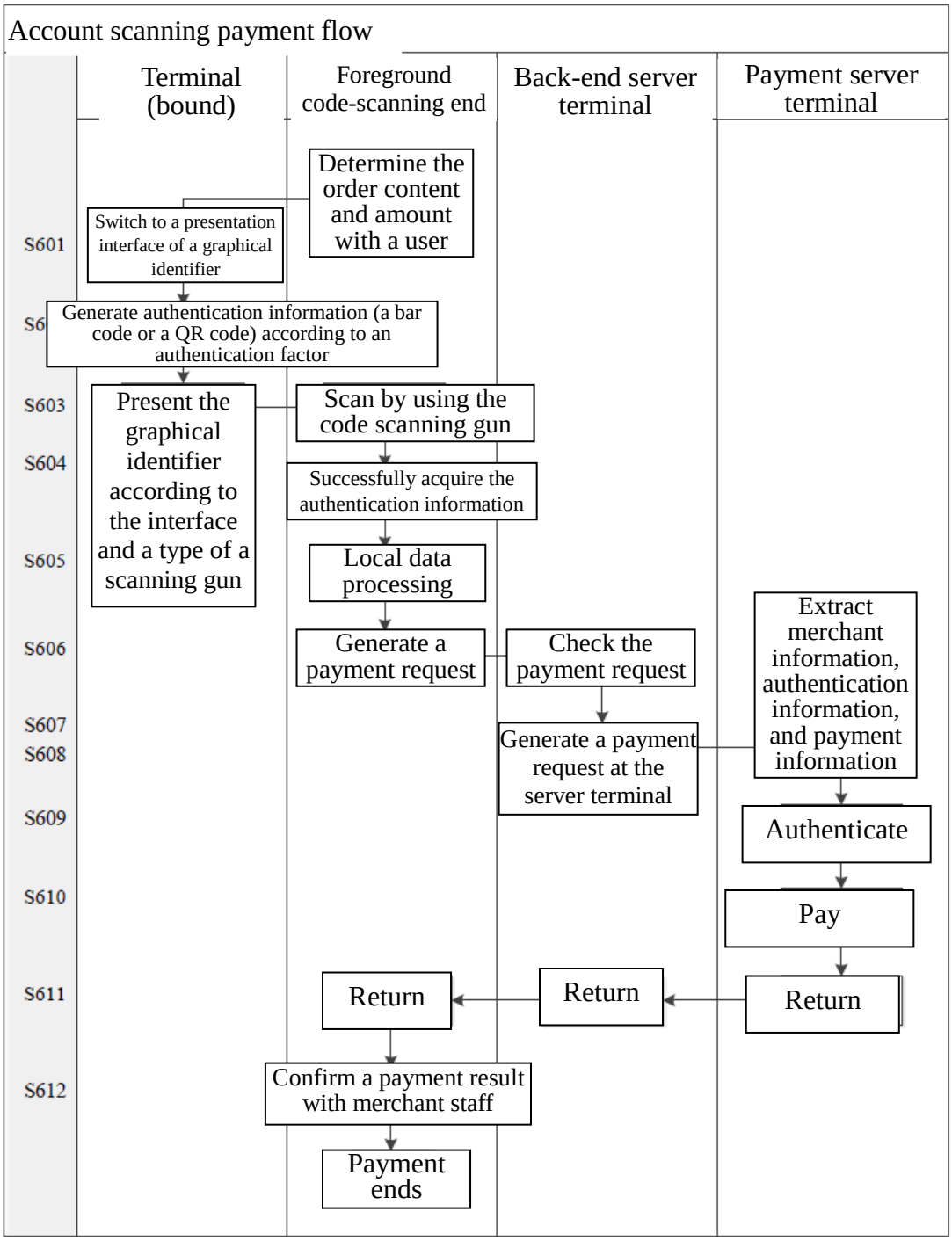

Account scanning payment flow
Terminal (bound)
Foreground code-scanning end
Back-end server terminal
Payment server terminal
Determine the order content and amount with a user
S601
Switch to a presentation interface of a graphical identifier
S6
Generate authentication information (a bar code or a QR code) according to an authentication factor
S603
Present the graphical identifier according to the interface and a type of a scanning gun
Scan by using the code scanning gun
S604
Successfully acquire the authentication information
S605
Local data processing
S606
Generate a payment request
Check the payment request
S607
S608
Generate a payment request at the server terminal
Extract merchant information, authentication information, and payment information
S609
Authenticate
S610
Pay
S611
Return
Return
Return
S612
Confirm a payment result with merchant staff
Payment ends

FIG. 6

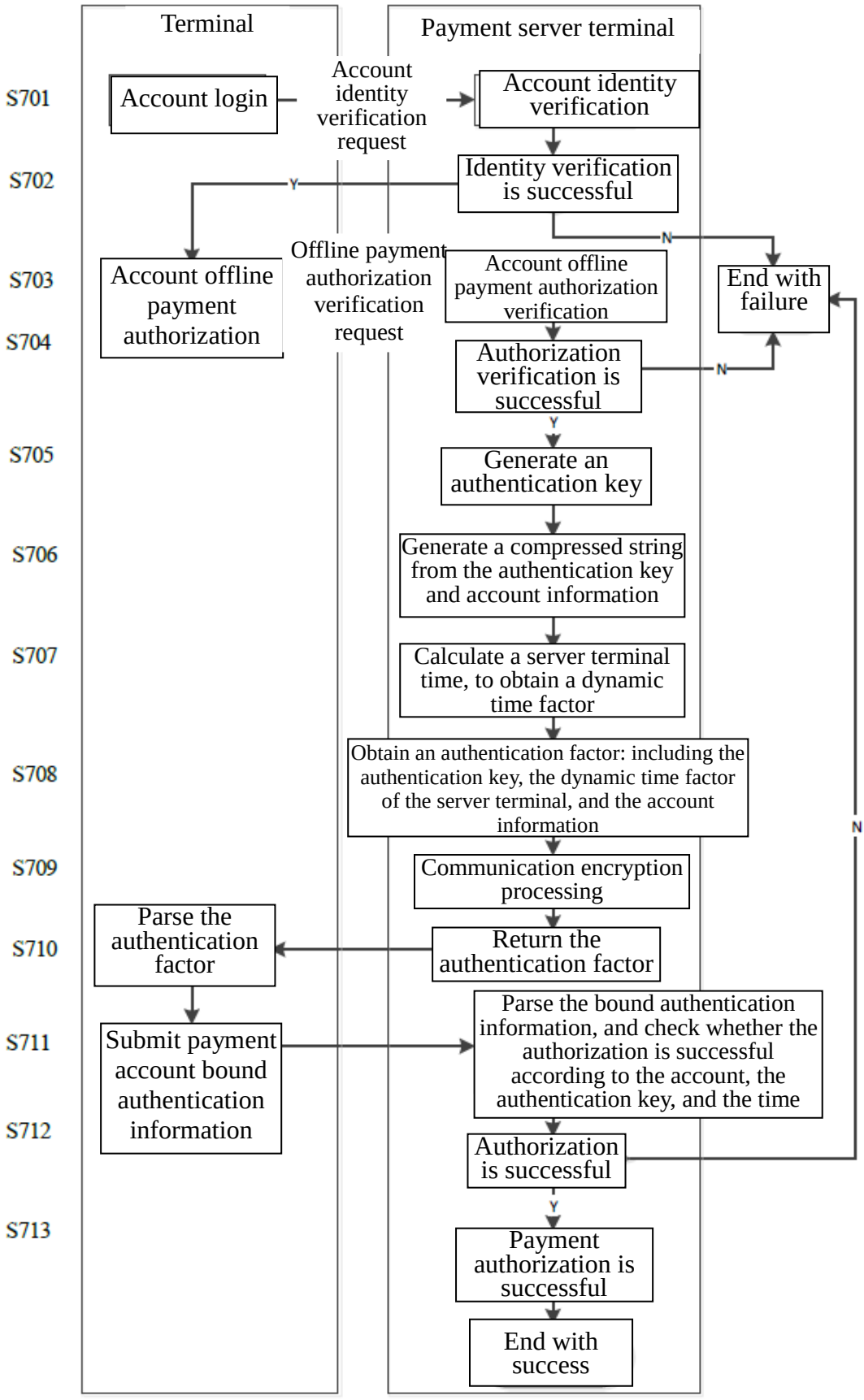

Terminal
Payment server terminal
S701
Account login
Account identity verification request
Account identity verification
S702
Identity verification is successful
Y
N
S703
Account offline payment authorization
Offline payment authorization verification request
Account offline payment authorization verification
End with failure
S704
Authorization verification is successful
N
Y
S705
Generate an authentication key
S706
Generate a compressed string from the authentication key and account information
S707
Calculate a server terminal time, to obtain a dynamic time factor
S708
Obtain an authentication factor: including the authentication key, the dynamic time factor of the server terminal, and the account information
S709
Communication encryption processing
S710
Parse the authentication factor
Return the authentication factor
S711
Submit payment account bound authentication information
Parse the bound authentication information, and check whether the authorization is successful according to the account, the authentication key, and the time
S712
Authorization is successful
N
Y
S713
Payment authorization is successful
End with success

FIG. 7

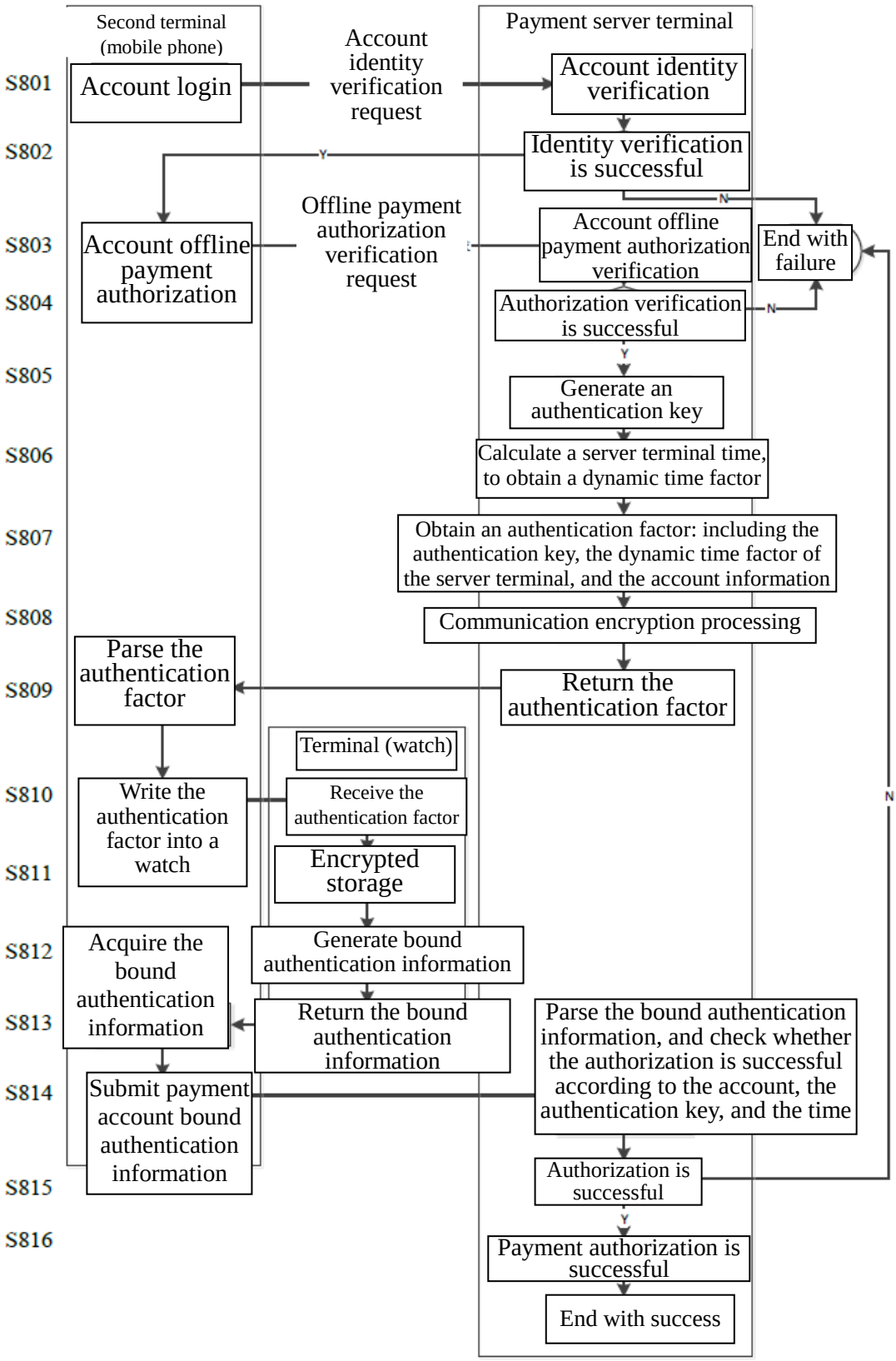

Second terminal (mobile phone)
Payment server terminal
S801
Account login
Account identity verification request
Account identity verification
S802
Identity verification is successful
Y
N
S803
Account offline payment authorization
Offline payment authorization verification request
Account offline payment authorization verification
End with failure
S804
Authorization verification is successful
N
Y
S805
Generate an authentication key
S806
Calculate a server terminal time, to obtain a dynamic time factor
S807
Obtain an authentication factor: including the authentication key, the dynamic time factor of the server terminal, and the account information
S808
Communication encryption processing
S809
Parse the authentication factor
Return the authentication factor
Terminal (watch)
S810
Write the authentication factor into a watch
Receive the authentication factor
S811
Encrypted storage
S812
Acquire the bound authentication information
Generate bound authentication information
S813
Return the bound authentication information
Parse the bound authentication information, and check whether the authorization is successful according to the account, the authentication key, and the time
S814
Submit payment account bound authentication information
S815
Authorization is successful
N
Y
S816
Payment authorization is successful
End with success

FIG. 8

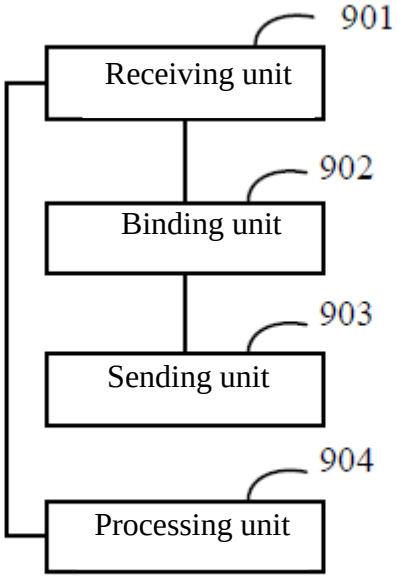

901
Receiving unit
902
Binding unit
903
Sending unit
904
Processing unit

FIG. 9

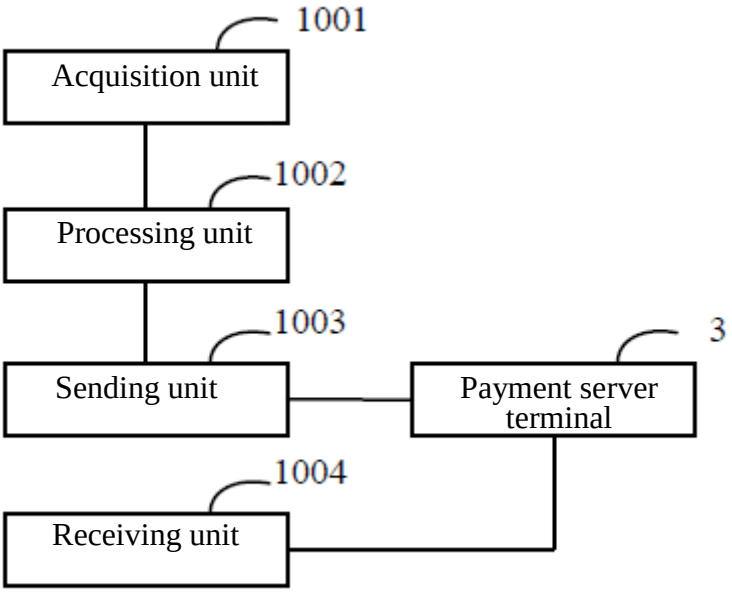

1001
Acquisition unit
1002
Processing unit
1003
Sending unit
3
Payment server terminal
1004
Receiving unit

FIG. 10

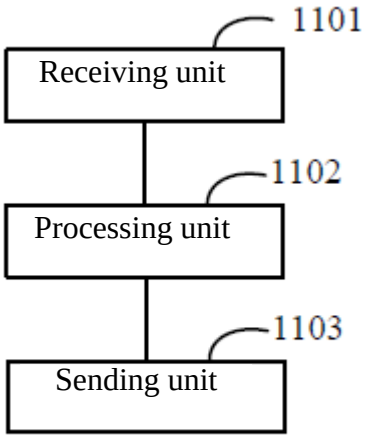

1101
Receiving unit
1102
Processing unit
1103
Sending unit

FIG. 11

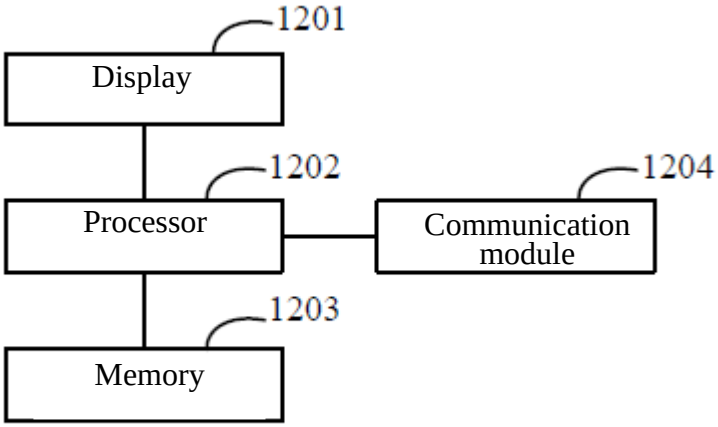

1201
Display
1202
Processor
1204
Communication module
1203
Memory

FIG. 12