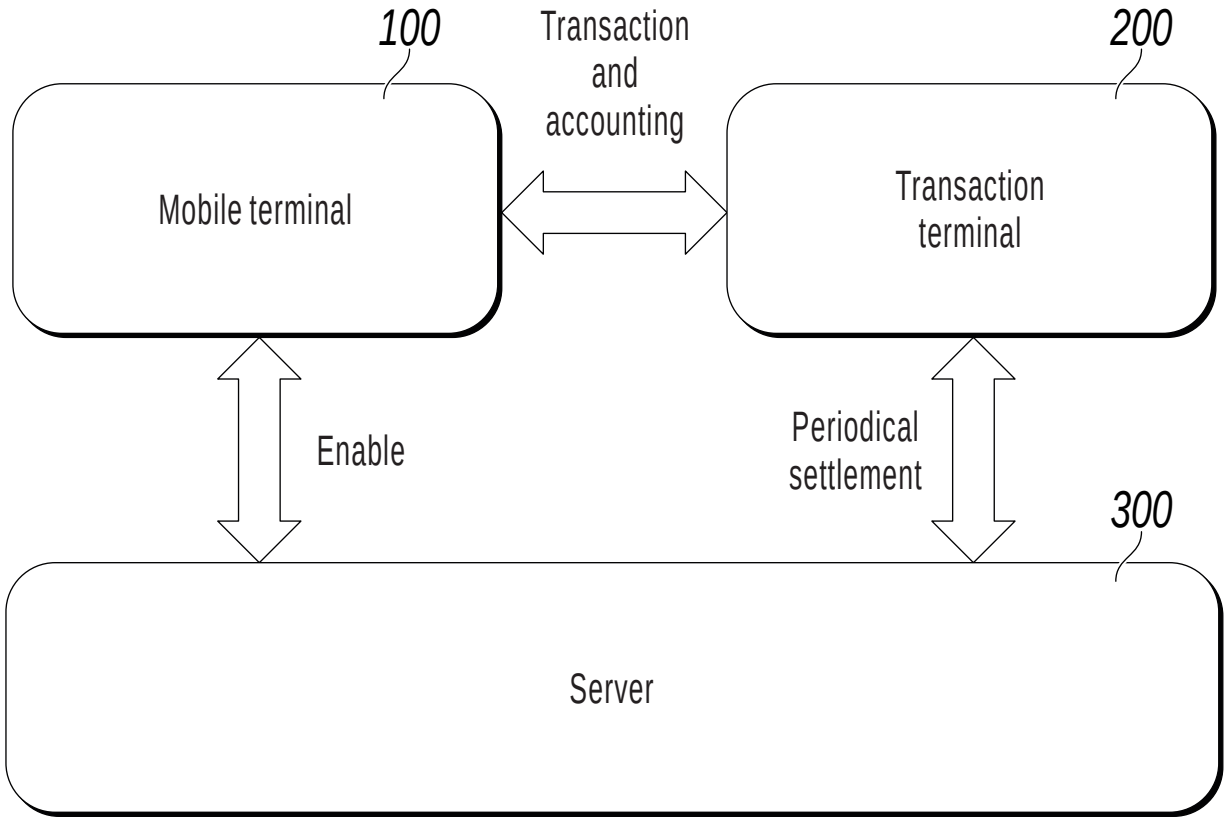

100
Transaction
and
accounting
200
Mobile terminal
Transaction
terminal
Enable
Periodical
settlement
300
Server

FIG. 1

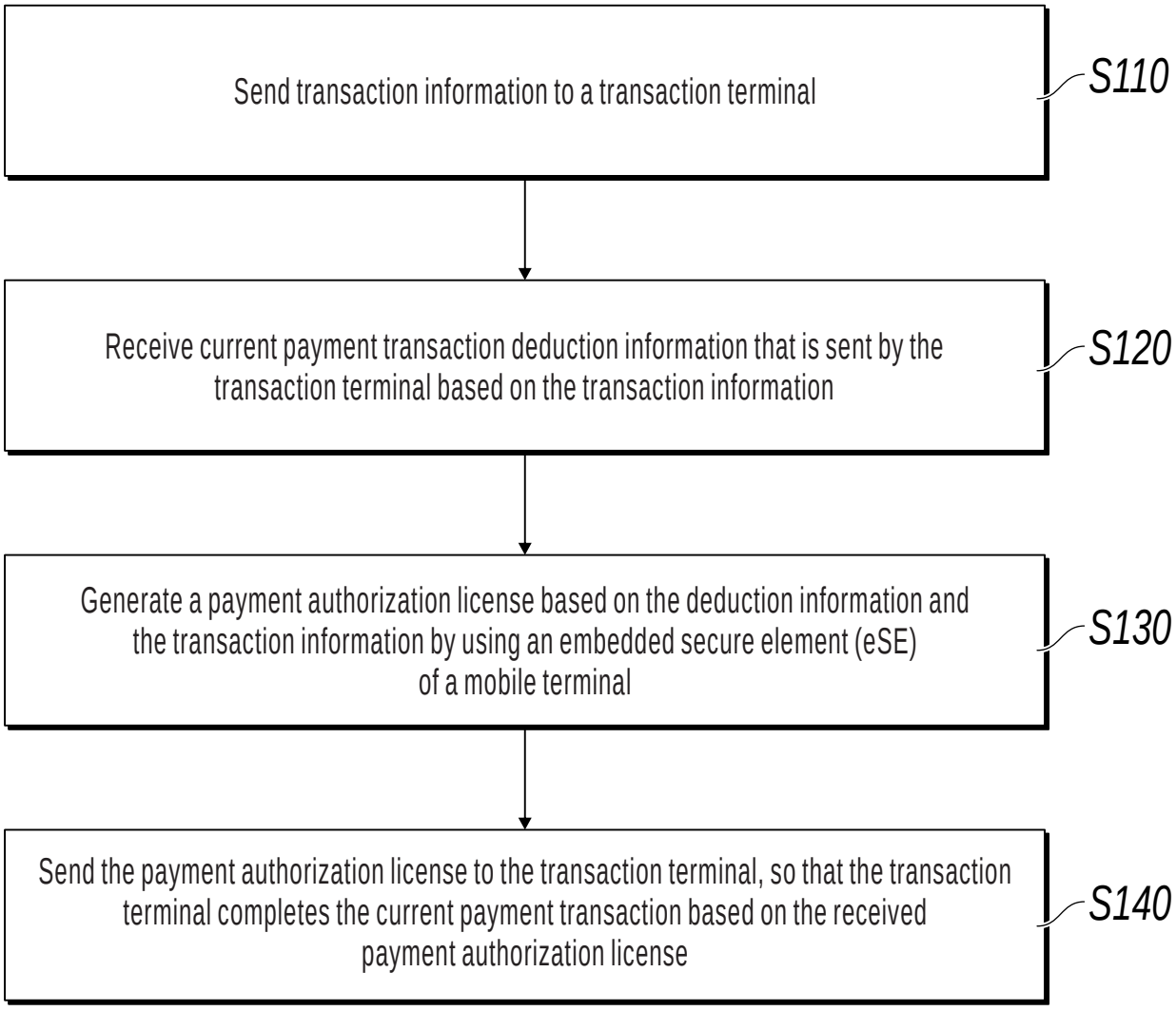

Send transaction information to a transaction terminal
S110
Receive current payment transaction deduction information that is sent by the transaction terminal based on the transaction information
S120
Generate a payment authorization license based on the deduction information and the transaction information by using an embedded secure element (eSE) of a mobile terminal
S130
Send the payment authorization license to the transaction terminal, so that the transaction terminal completes the current payment transaction based on the received payment authorization license
S140

FIG. 2

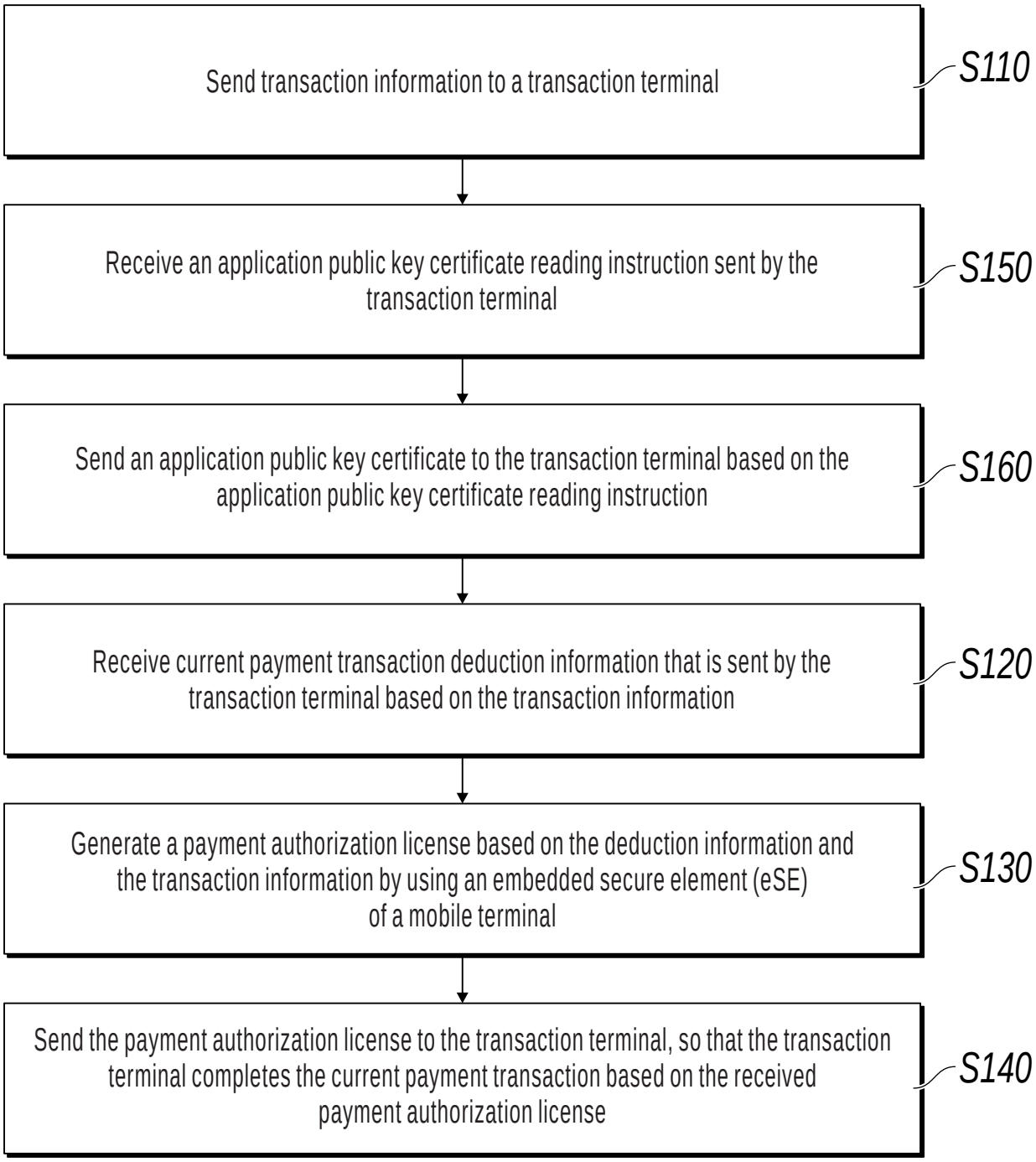

Send transaction information to a transaction terminal
S110
Receive an application public key certificate reading instruction sent by the transaction terminal
S150
Send an application public key certificate to the transaction terminal based on the application public key certificate reading instruction
S160
Receive current payment transaction deduction information that is sent by the transaction terminal based on the transaction information
S120
Generate a payment authorization license based on the deduction information and the transaction information by using an embedded secure element (eSE) of a mobile terminal
S130
Send the payment authorization license to the transaction terminal, so that the transaction terminal completes the current payment transaction based on the received payment authorization license
S140

FIG. 3

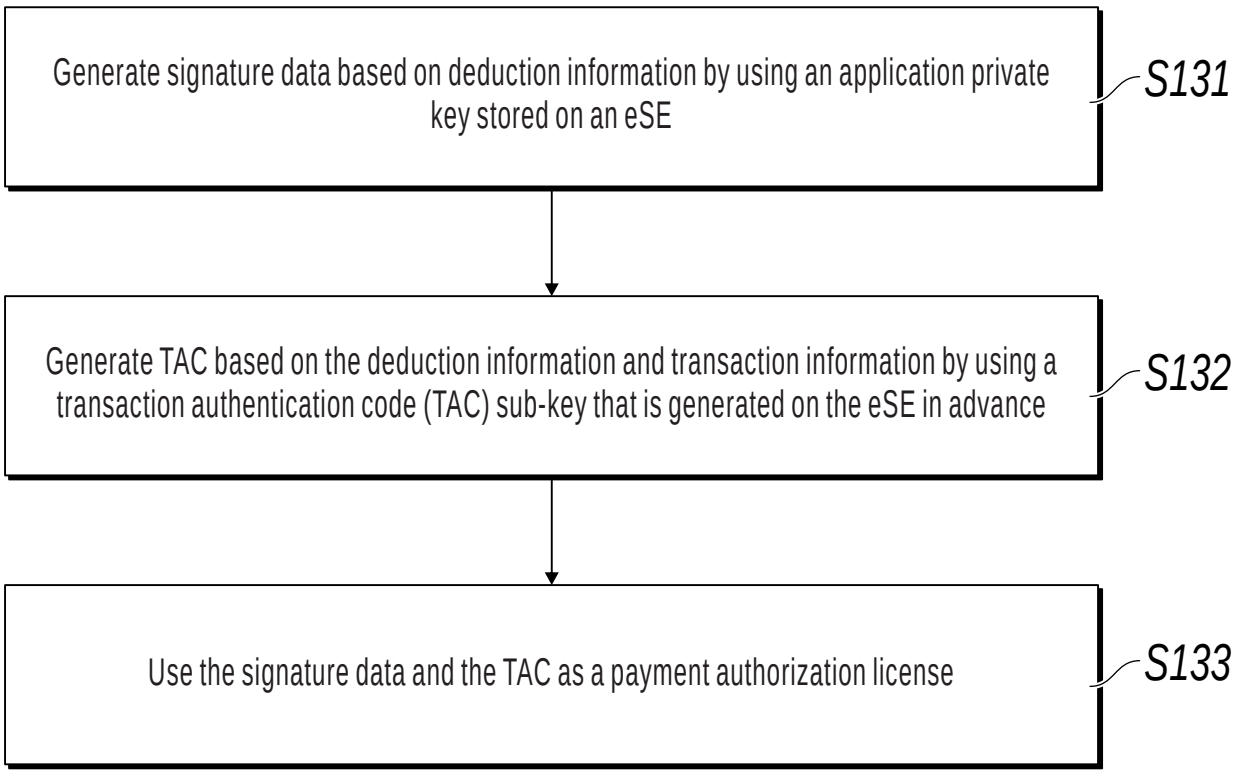

Generate signature data based on deduction information by using an application private key stored on an eSE
S131
Generate TAC based on the deduction information and transaction information by using a transaction authentication code (TAC) sub-key that is generated on the eSE in advance
S132
Use the signature data and the TAC as a payment authorization license
S133

FIG. 4

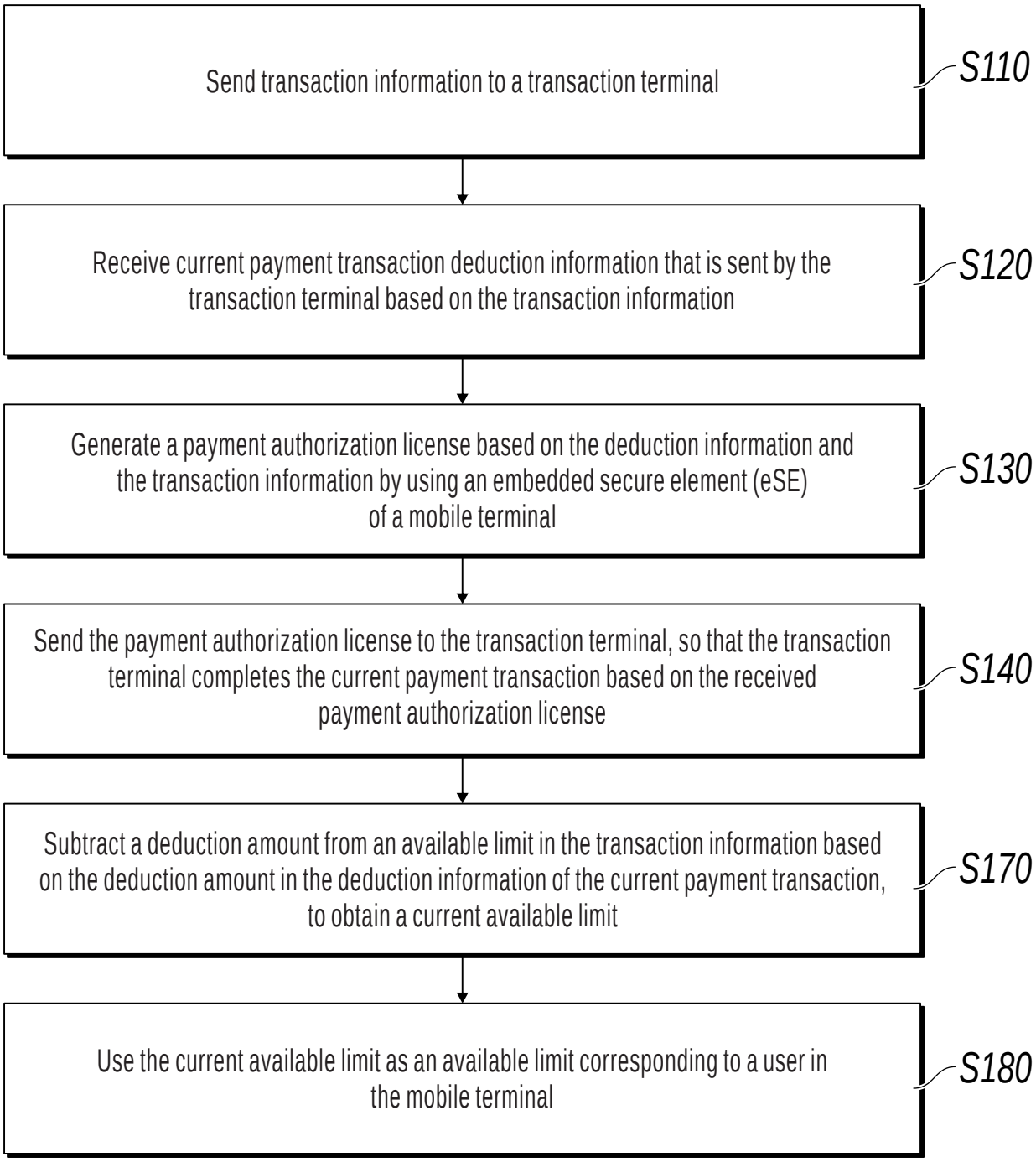

Send transaction information to a transaction terminal
S110
Receive current payment transaction deduction information that is sent by the transaction terminal based on the transaction information
S120
Generate a payment authorization license based on the deduction information and the transaction information by using an embedded secure element (eSE) of a mobile terminal
S130
Send the payment authorization license to the transaction terminal, so that the transaction terminal completes the current payment transaction based on the received payment authorization license
S140
Subtract a deduction amount from an available limit in the transaction information based on the deduction amount in the deduction information of the current payment transaction, to obtain a current available limit
S170
Use the current available limit as an available limit corresponding to a user in the mobile terminal
S180

FIG. 5

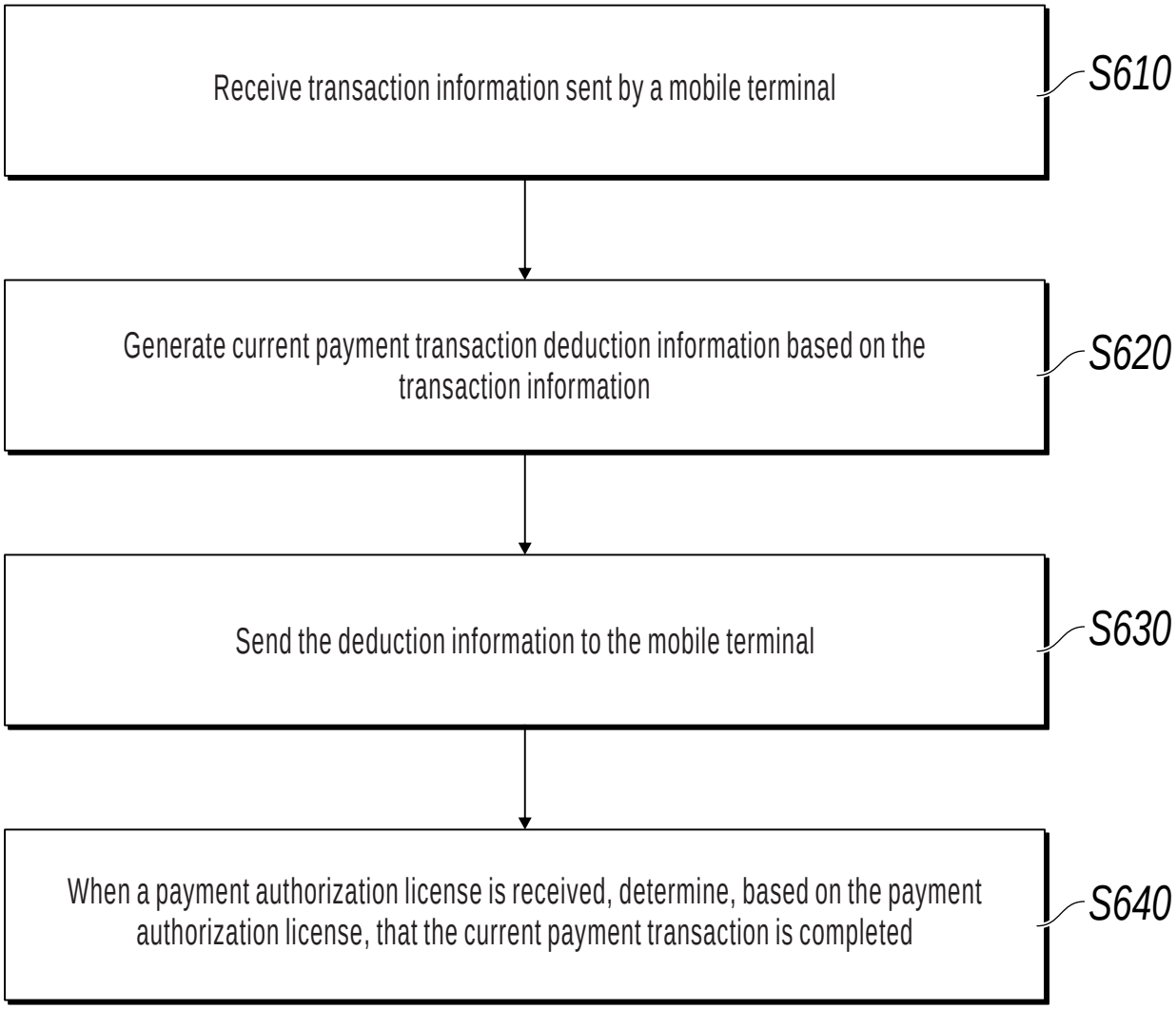

Receive transaction information sent by a mobile terminal
S610
Generate current payment transaction deduction information based on the transaction information
S620
Send the deduction information to the mobile terminal
S630
When a payment authorization license is received, determine, based on the payment authorization license, that the current payment transaction is completed
S640

FIG. 6

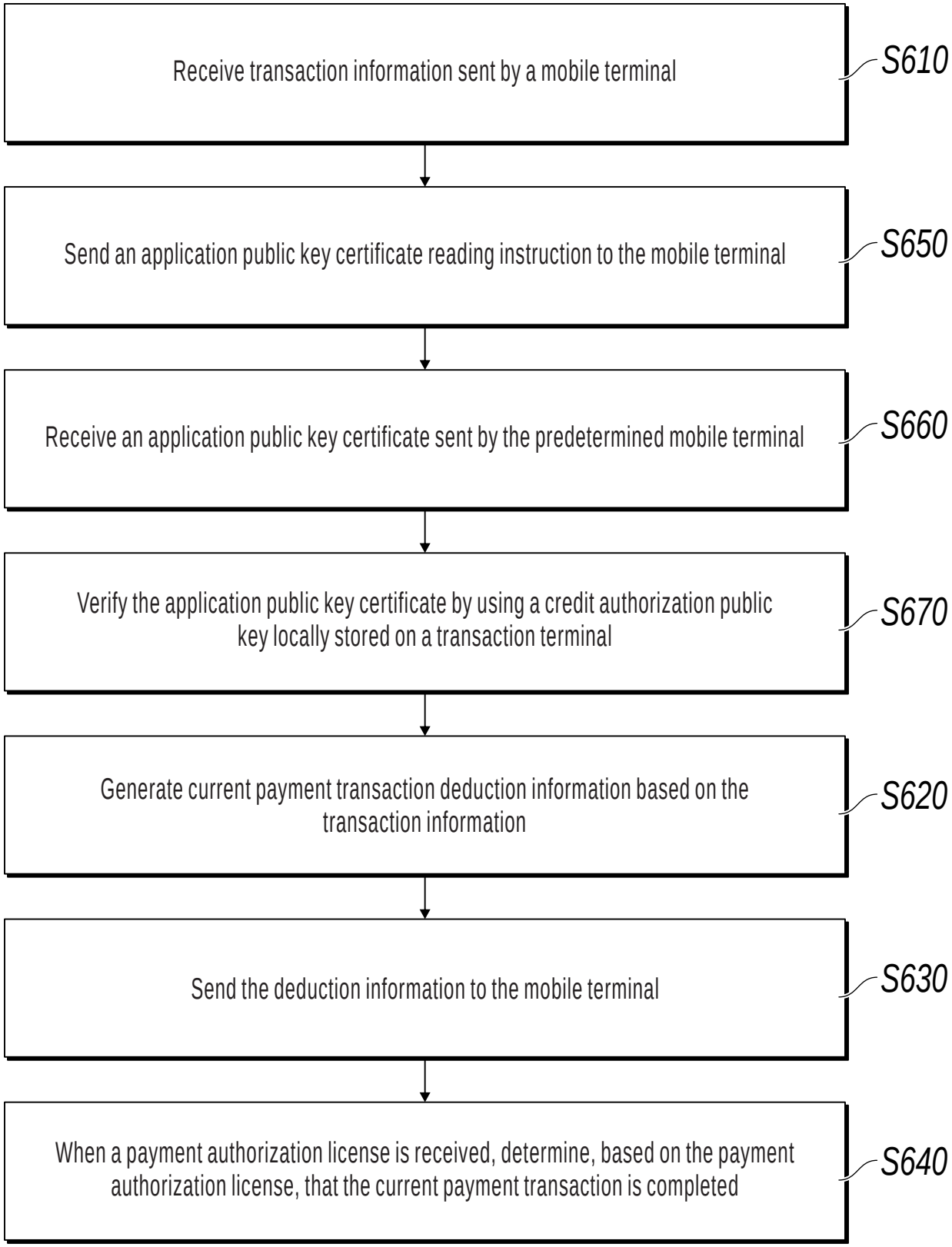

Receive transaction information sent by a mobile terminal
S610
Send an application public key certificate reading instruction to the mobile terminal
S650
Receive an application public key certificate sent by the predetermined mobile terminal
S660
Verify the application public key certificate by using a credit authorization public key locally stored on a transaction terminal
S670
Generate current payment transaction deduction information based on the transaction information
S620
Send the deduction information to the mobile terminal
S630
When a payment authorization license is received, determine, based on the payment authorization license, that the current payment transaction is completed
S640

FIG. 7

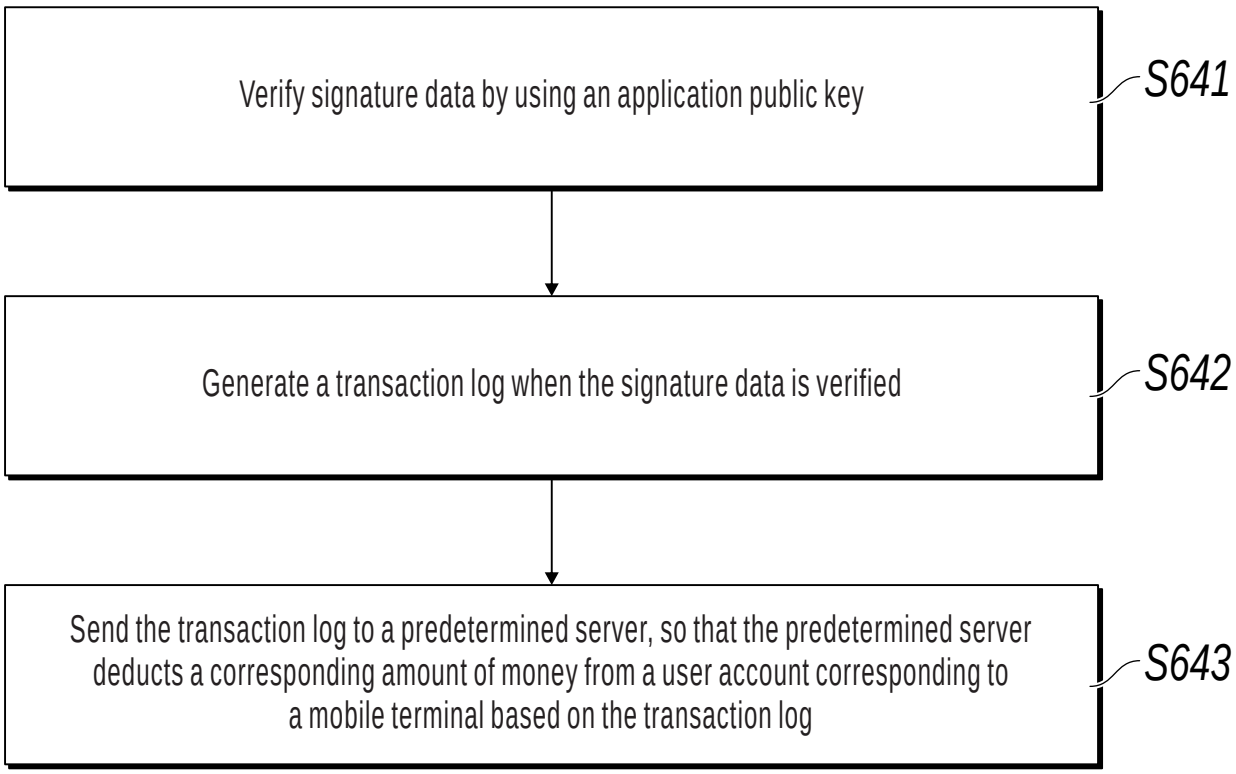

Verify signature data by using an application public key
S641
Generate a transaction log when the signature data is verified
S642
Send the transaction log to a predetermined server, so that the predetermined server deducts a corresponding amount of money from a user account corresponding to a mobile terminal based on the transaction log
S643

FIG. 8

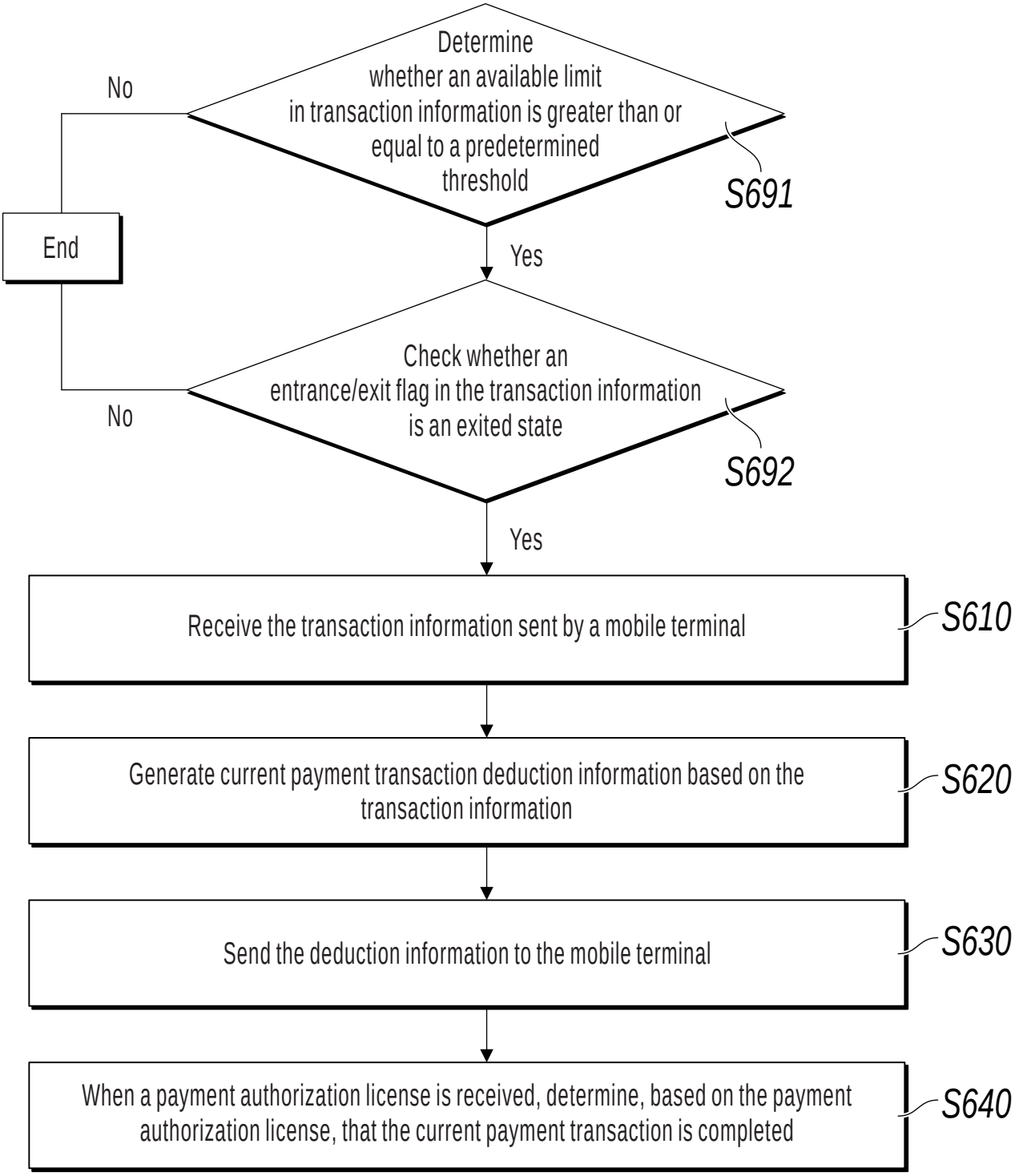

Determine whether an available limit in transaction information is greater than or equal to a predetermined threshold
S691
No
End
Yes
Check whether an entrance/exit flag in the transaction information is an exited state
S692
No
Yes
Receive the transaction information sent by a mobile terminal
S610
Generate current payment transaction deduction information based on the transaction information
S620
Send the deduction information to the mobile terminal
S630
When a payment authorization license is received, determine, based on the payment authorization license, that the current payment transaction is completed
S640

FIG. 9

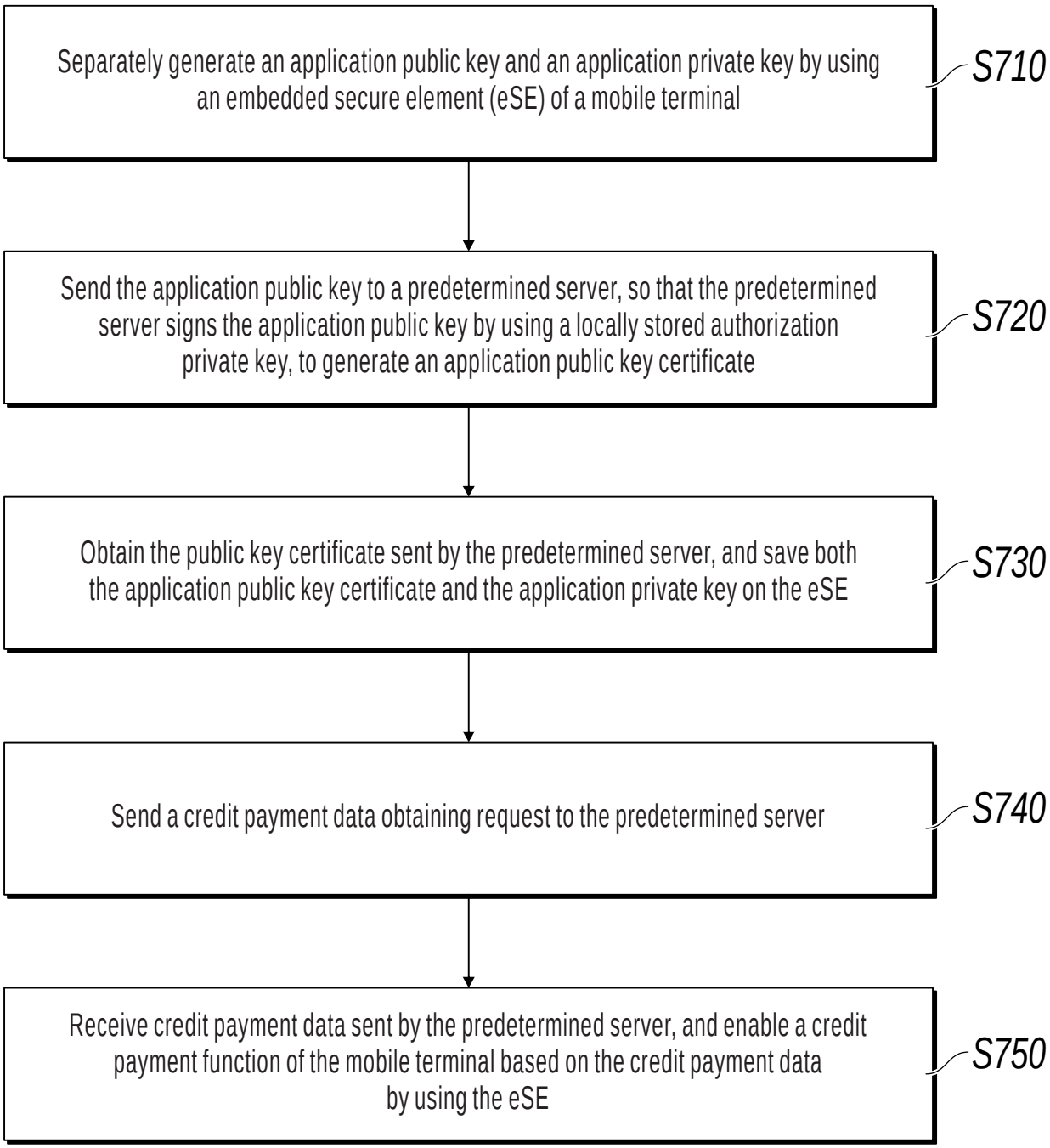

Separately generate an application public key and an application private key by using an embedded secure element (eSE) of a mobile terminal
S710
Send the application public key to a predetermined server, so that the predetermined server signs the application public key by using a locally stored authorization private key, to generate an application public key certificate
S720
Obtain the public key certificate sent by the predetermined server, and save both the application public key certificate and the application private key on the eSE
S730
Send a credit payment data obtaining request to the predetermined server
S740
Receive credit payment data sent by the predetermined server, and enable a credit payment function of the mobile terminal based on the credit payment data by using the eSE
S750

FIG. 10

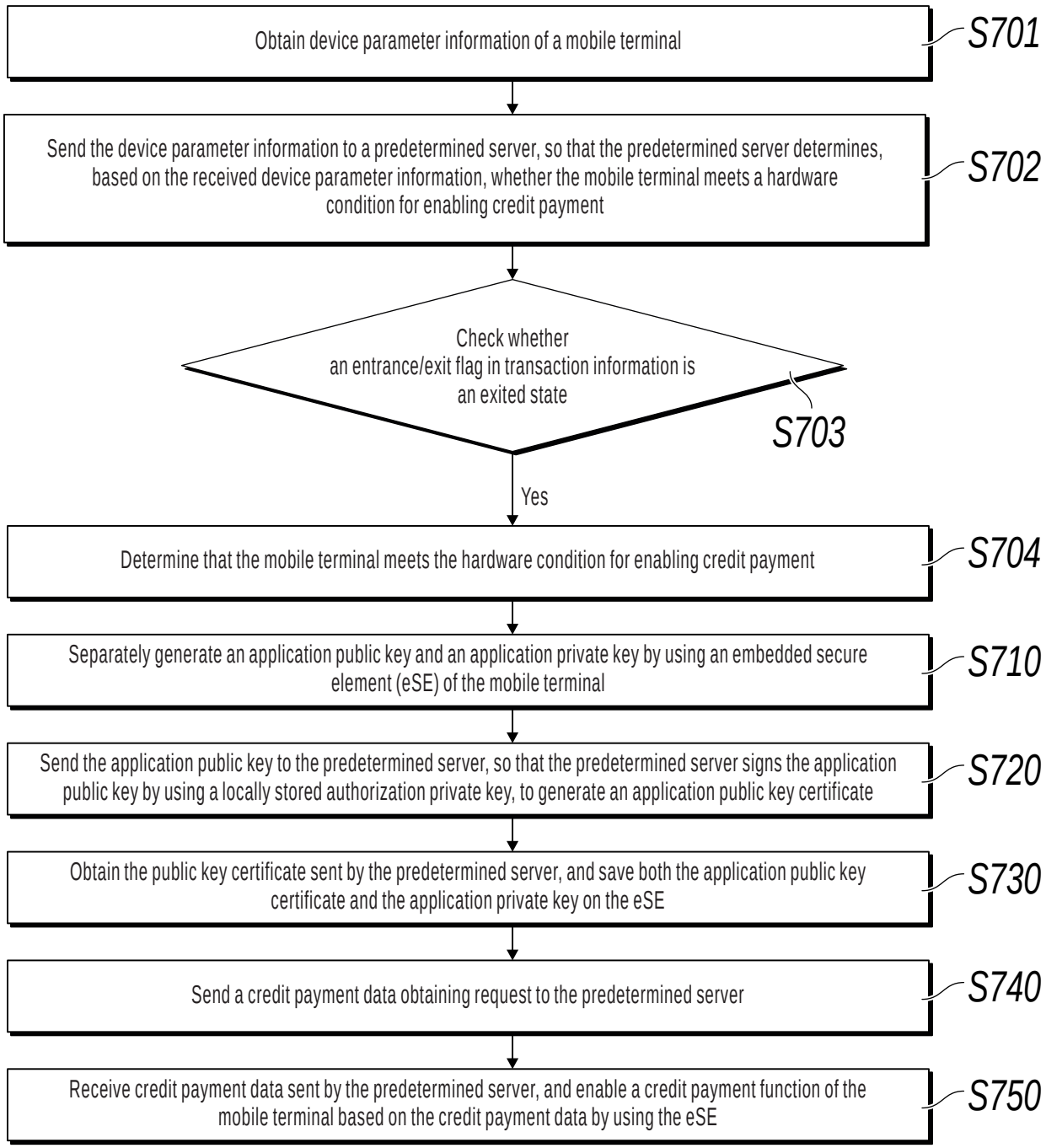

Obtain device parameter information of a mobile terminal
S701
Send the device parameter information to a predetermined server, so that the predetermined server determines, based on the received device parameter information, whether the mobile terminal meets a hardware condition for enabling credit payment
S702
Check whether an entrance/exit flag in transaction information is an exited state
S703
Yes
Determine that the mobile terminal meets the hardware condition for enabling credit payment
S704
Separately generate an application public key and an application private key by using an embedded secure element (eSE) of the mobile terminal
S710
Send the application public key to the predetermined server, so that the predetermined server signs the application public key by using a locally stored authorization private key, to generate an application public key certificate
S720
Obtain the public key certificate sent by the predetermined server, and save both the application public key certificate and the application private key on the eSE
S730
Send a credit payment data obtaining request to the predetermined server
S740
Receive credit payment data sent by the predetermined server, and enable a credit payment function of the mobile terminal based on the credit payment data by using the eSE
S750

FIG. 11

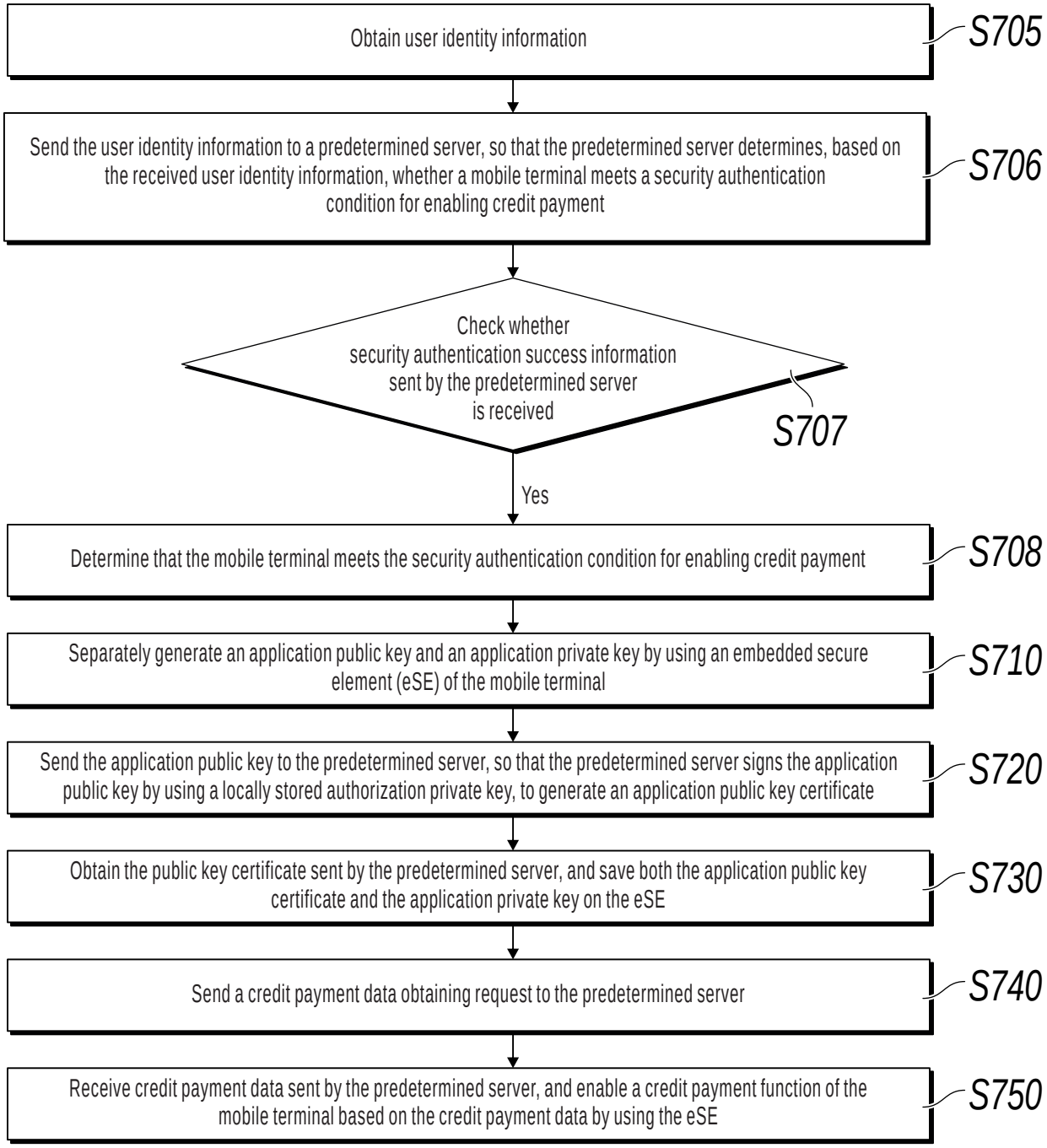

Obtain user identity information
S705
Send the user identity information to a predetermined server, so that the predetermined server determines, based on the received user identity information, whether a mobile terminal meets a security authentication condition for enabling credit payment
S706
Check whether security authentication success information sent by the predetermined server is received
S707
Yes
Determine that the mobile terminal meets the security authentication condition for enabling credit payment
S708
Separately generate an application public key and an application private key by using an embedded secure element (eSE) of the mobile terminal
S710
Send the application public key to the predetermined server, so that the predetermined server signs the application public key by using a locally stored authorization private key, to generate an application public key certificate
S720
Obtain the public key certificate sent by the predetermined server, and save both the application public key certificate and the application private key on the eSE
S730
Send a credit payment data obtaining request to the predetermined server
S740
Receive credit payment data sent by the predetermined server, and enable a credit payment function of the mobile terminal based on the credit payment data by using the eSE
S750

FIG. 12

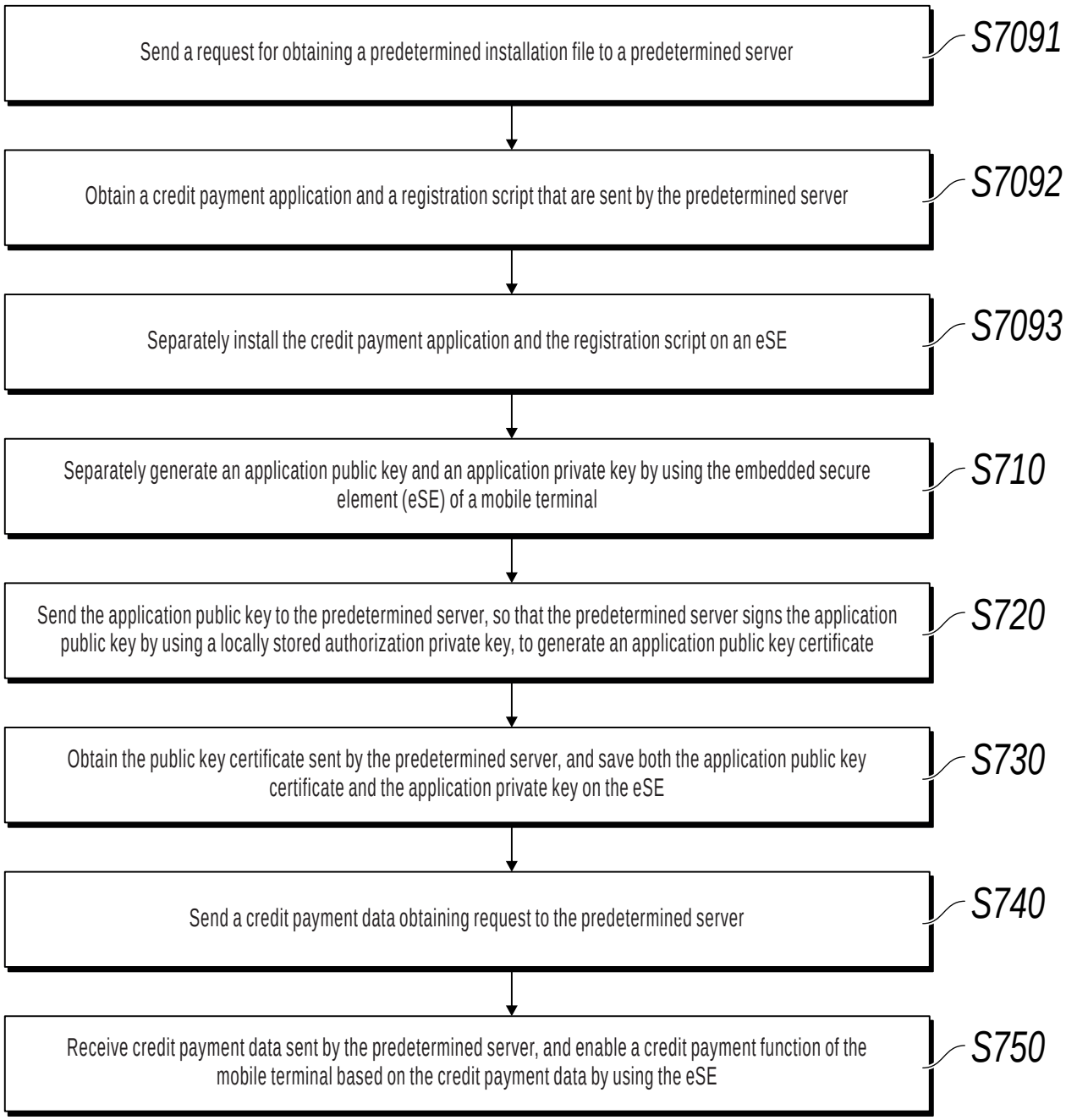

Send a request for obtaining a predetermined installation file to a predetermined server
S7091
Obtain a credit payment application and a registration script that are sent by the predetermined server
S7092
Separately install the credit payment application and the registration script on an eSE
S7093
Separately generate an application public key and an application private key by using the embedded secure element (eSE) of a mobile terminal
S710
Send the application public key to the predetermined server, so that the predetermined server signs the application public key by using a locally stored authorization private key, to generate an application public key certificate
S720
Obtain the public key certificate sent by the predetermined server, and save both the application public key certificate and the application private key on the eSE
S730
Send a credit payment data obtaining request to the predetermined server
S740
Receive credit payment data sent by the predetermined server, and enable a credit payment function of the mobile terminal based on the credit payment data by using the eSE
S750

FIG. 13

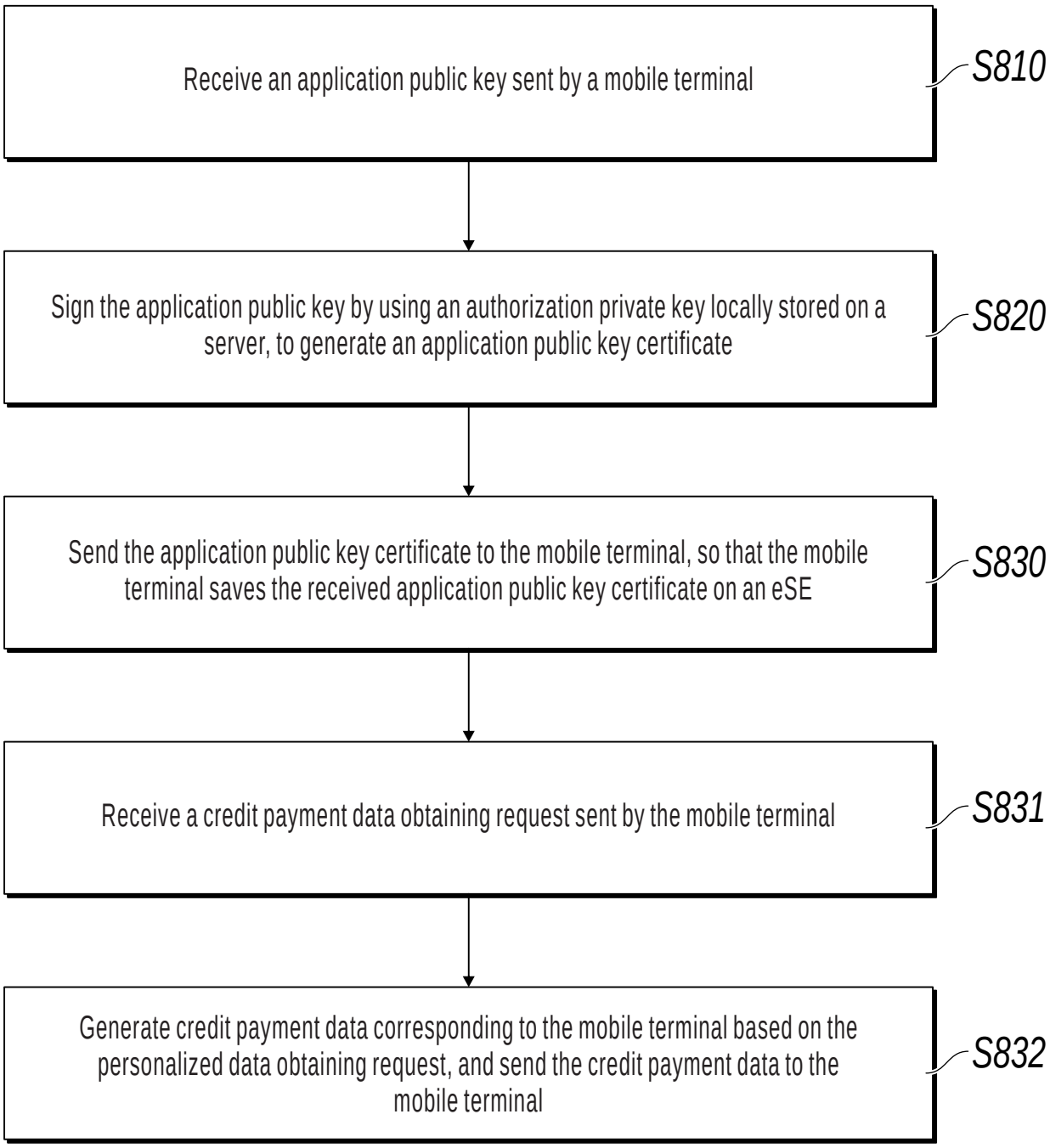

Receive an application public key sent by a mobile terminal
S810
Sign the application public key by using an authorization private key locally stored on a server, to generate an application public key certificate
S820
Send the application public key certificate to the mobile terminal, so that the mobile terminal saves the received application public key certificate on an eSE
S830
Receive a credit payment data obtaining request sent by the mobile terminal
S831
Generate credit payment data corresponding to the mobile terminal based on the personalized data obtaining request, and send the credit payment data to the mobile terminal
S832

FIG. 14

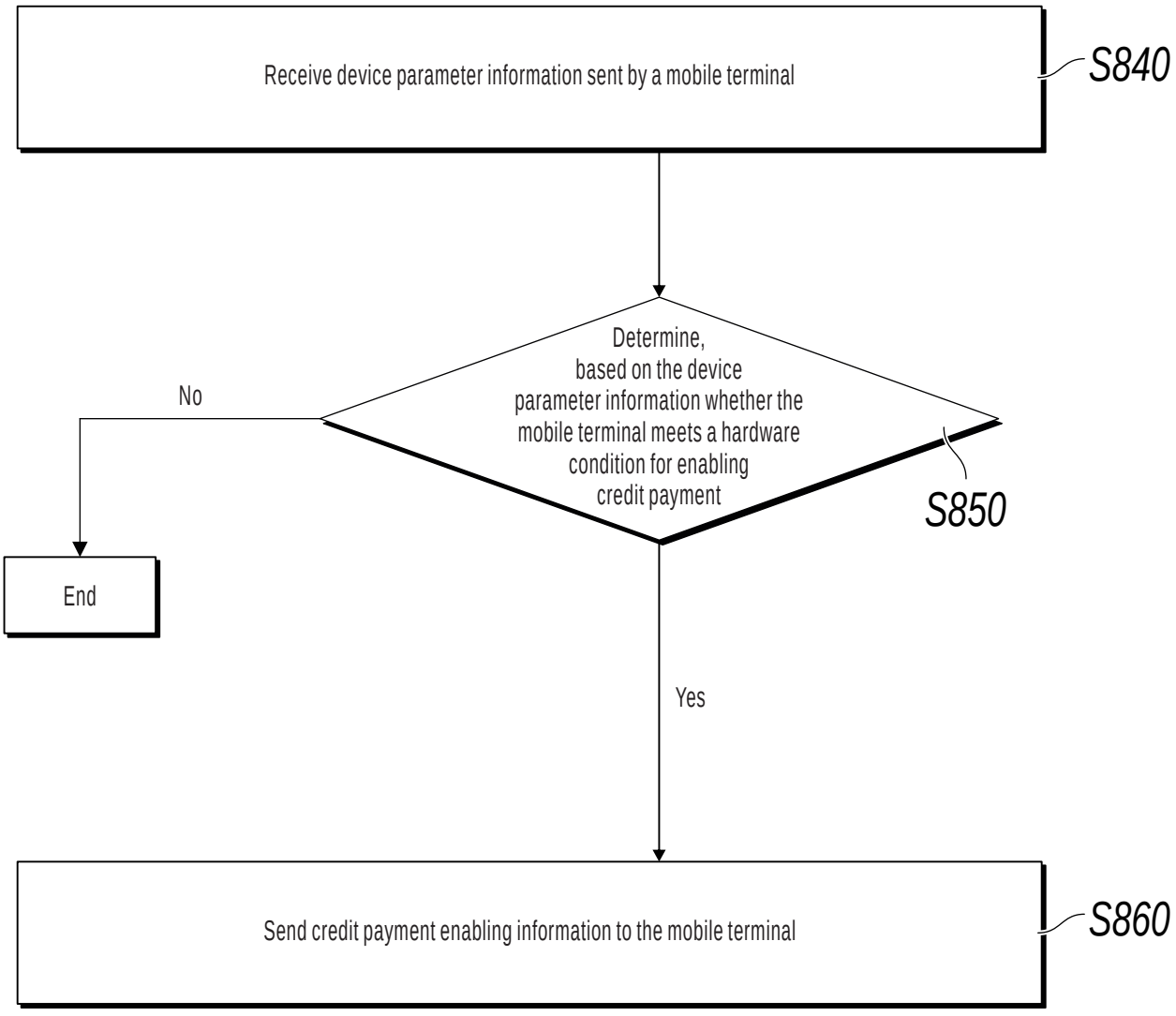

Receive device parameter information sent by a mobile terminal
S840
Determine, based on the device parameter information whether the mobile terminal meets a hardware condition for enabling credit payment
S850
No
End
Yes
Send credit payment enabling information to the mobile terminal
S860

FIG. 15

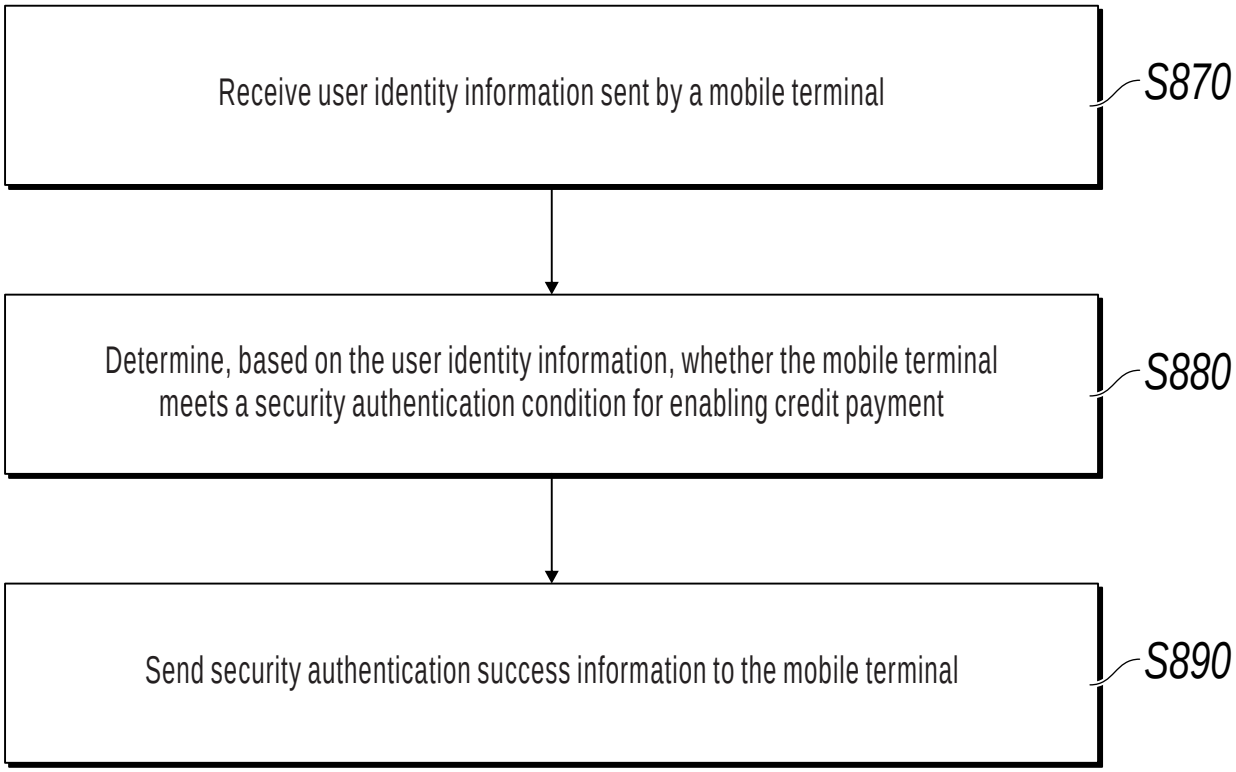

Receive user identity information sent by a mobile terminal
S870
Determine, based on the user identity information, whether the mobile terminal meets a security authentication condition for enabling credit payment
S880
Send security authentication success information to the mobile terminal
S890

FIG. 16

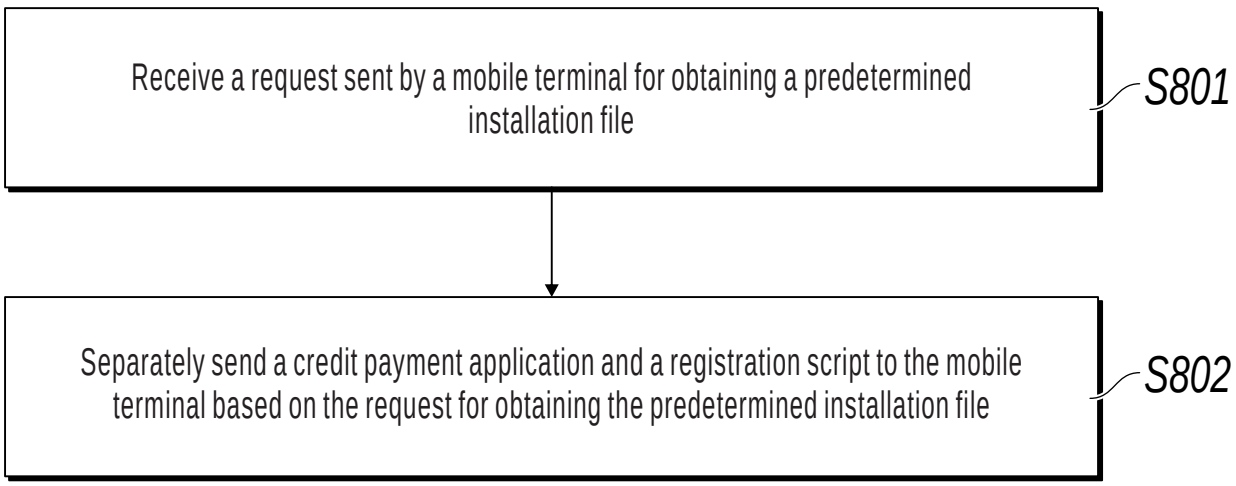

Receive a request sent by a mobile terminal for obtaining a predetermined installation file
S801
Separately send a credit payment application and a registration script to the mobile terminal based on the request for obtaining the predetermined installation file
S802

FIG. 17

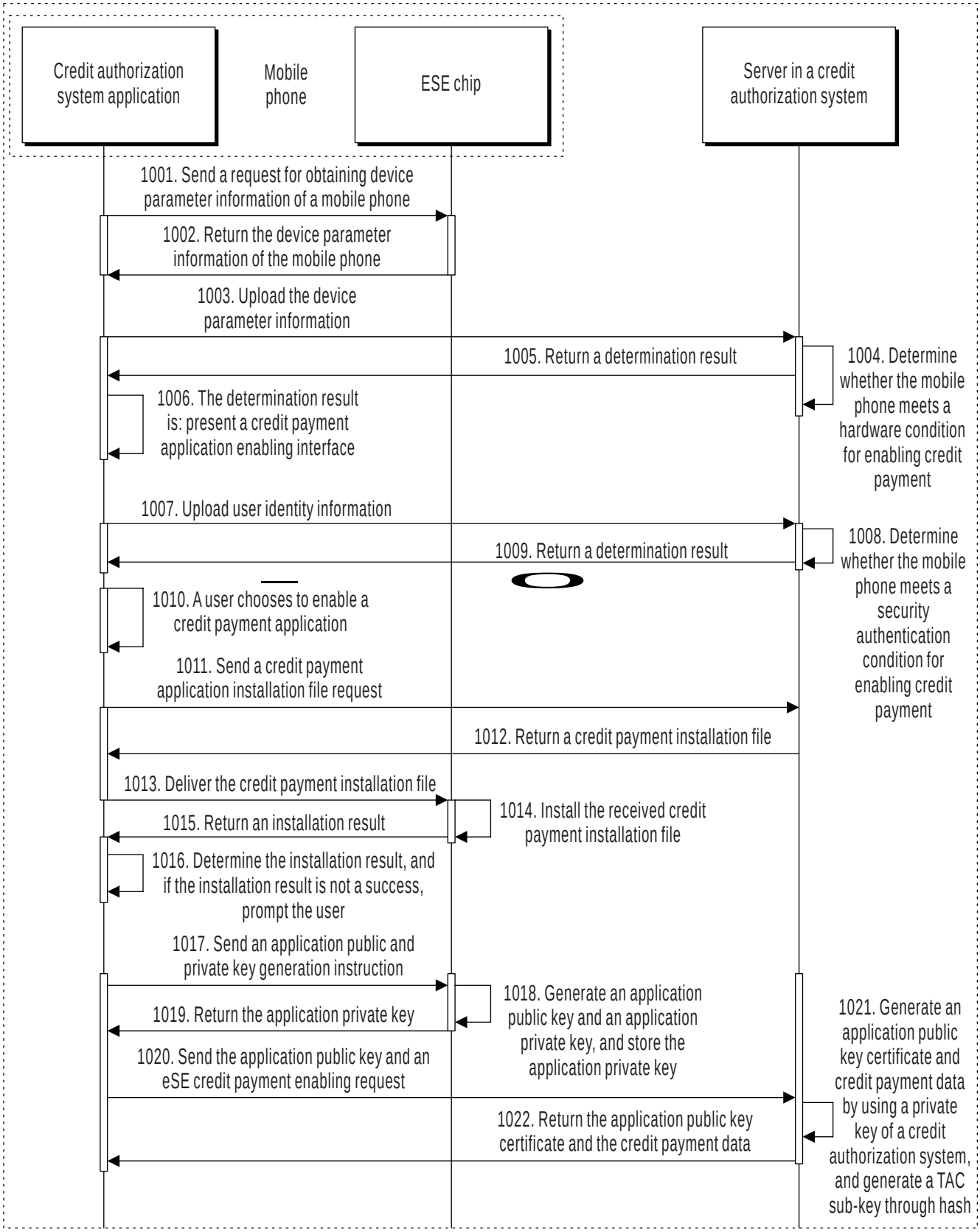

Credit authorization system application
Mobile phone
ESE chip
Server in a credit authorization system
1001. Send a request for obtaining device parameter information of a mobile phone
1002. Return the device parameter information of the mobile phone
1003. Upload the device parameter information
1005. Return a determination result
1004. Determine whether the mobile phone meets a hardware condition for enabling credit payment
1006. The determination result is: present a credit payment application enabling interface
1007. Upload user identity information
1009. Return a determination result
1008. Determine whether the mobile phone meets a security authentication condition for enabling credit payment
1010. A user chooses to enable a credit payment application
1011. Send a credit payment application installation file request
1012. Return a credit payment installation file
1013. Deliver the credit payment installation file
1014. Install the received credit payment installation file
1015. Return an installation result
1016. Determine the installation result, and if the installation result is not a success, prompt the user
1017. Send an application public and private key generation instruction
1018. Generate an application public key and an application private key, and store the application private key
1019. Return the application private key
1020. Send the application public key and an eSE credit payment enabling request
1021. Generate an application public key certificate and credit payment data by using a private key of a credit authorization system, and generate a TAC sub-key through hash
1022. Return the application public key certificate and the credit payment data

FIG. 18A

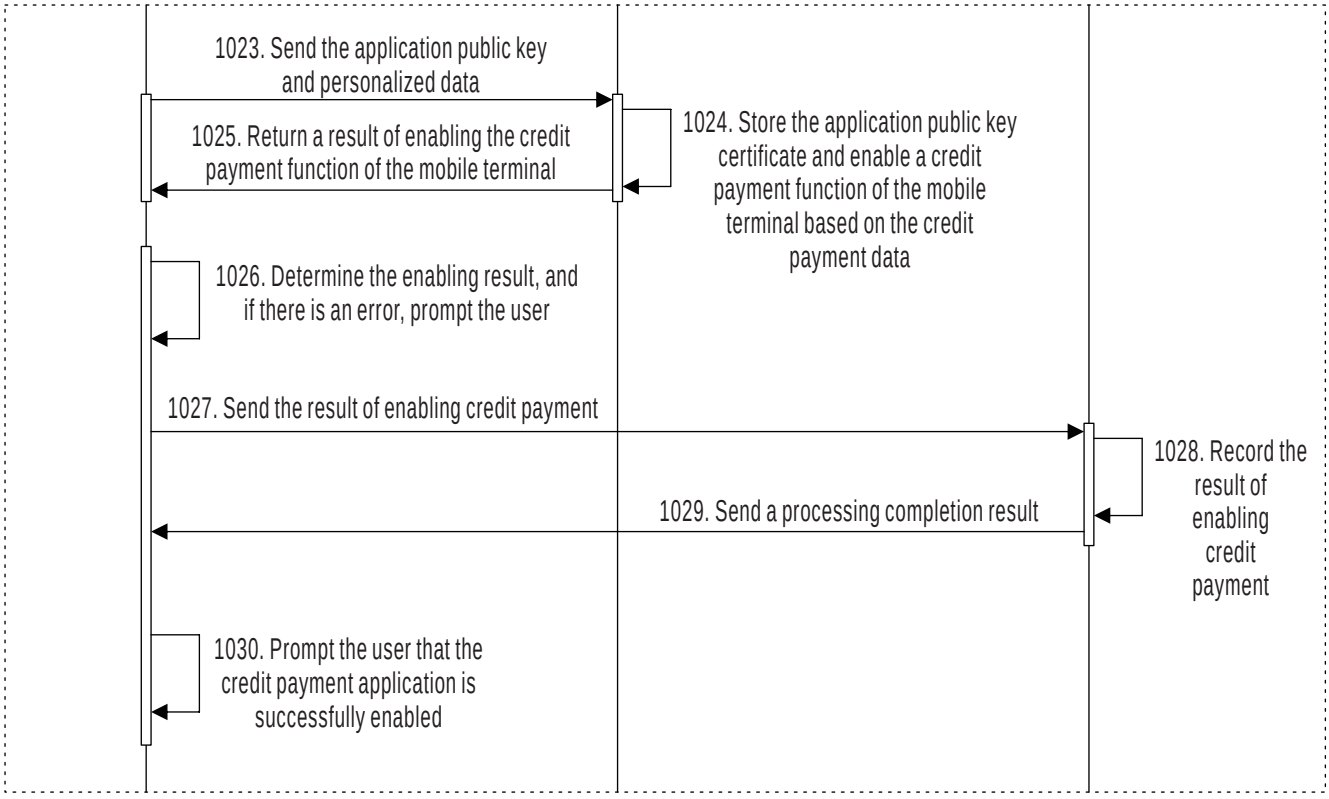

1023. Send the application public key and personalized data
1025. Return a result of enabling the credit payment function of the mobile terminal
1024. Store the application public key certificate and enable a credit payment function of the mobile terminal based on the credit payment data
1026. Determine the enabling result, and if there is an error, prompt the user
1027. Send the result of enabling credit payment
1028. Record the result of enabling credit payment
1029. Send a processing completion result
1030. Prompt the user that the credit payment application is successfully enabled

FIG. 18B

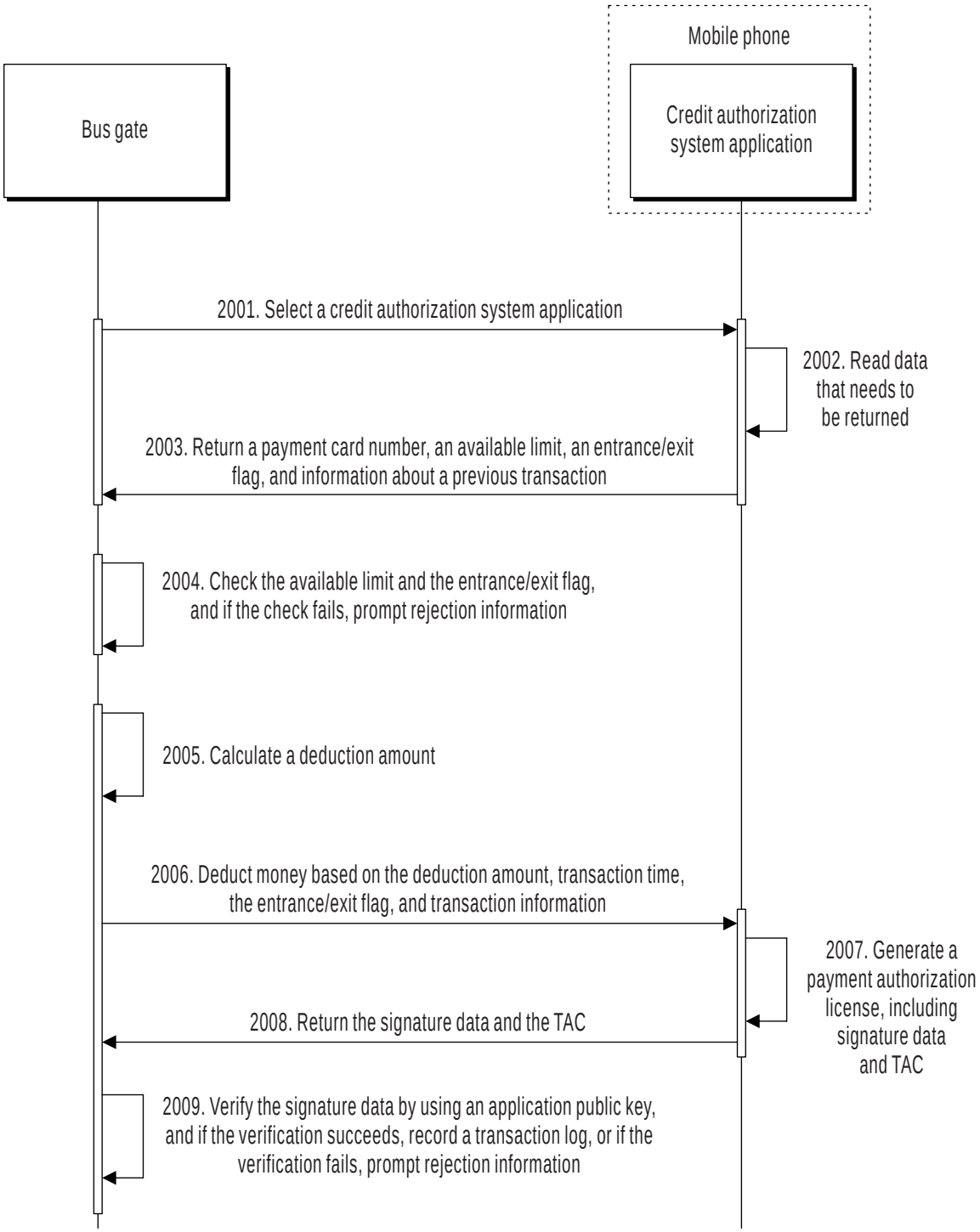

Mobile phone
Bus gate
Credit authorization system application
2001. Select a credit authorization system application
2002. Read data that needs to be returned
2003. Return a payment card number, an available limit, an entrance/exit flag, and information about a previous transaction
2004. Check the available limit and the entrance/exit flag, and if the check fails, prompt rejection information
2005. Calculate a deduction amount
2006. Deduct money based on the deduction amount, transaction time, the entrance/exit flag, and transaction information
2007. Generate a payment authorization license, including signature data and TAC
2008. Return the signature data and the TAC
2009. Verify the signature data by using an application public key, and if the verification succeeds, record a transaction log, or if the verification fails, prompt rejection information

FIG. 19

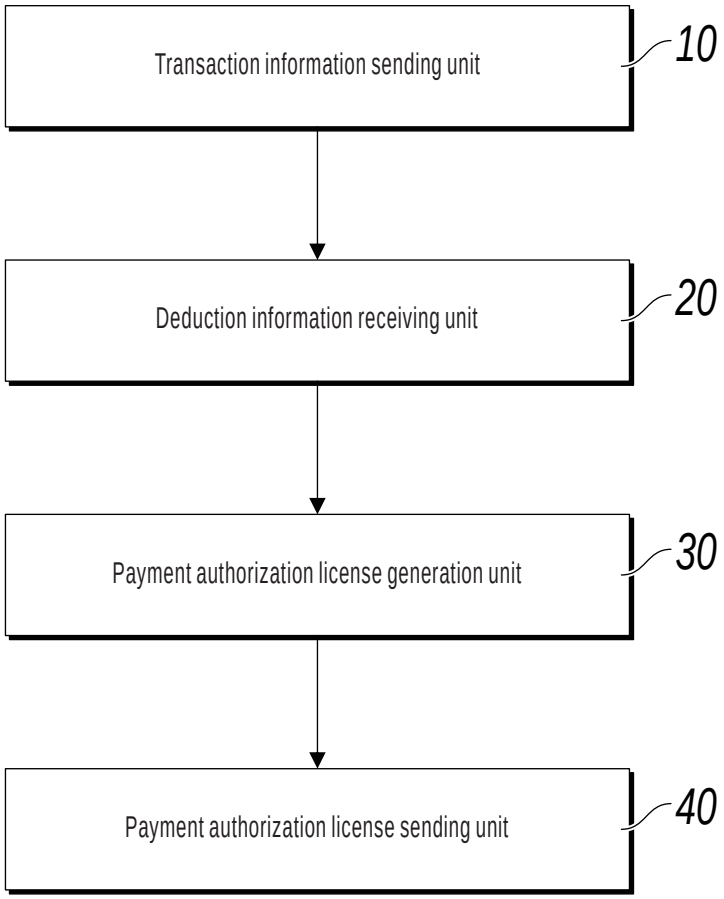

Transaction information sending unit
10
Deduction information receiving unit
20
Payment authorization license generation unit
30
Payment authorization license sending unit
40

FIG. 20

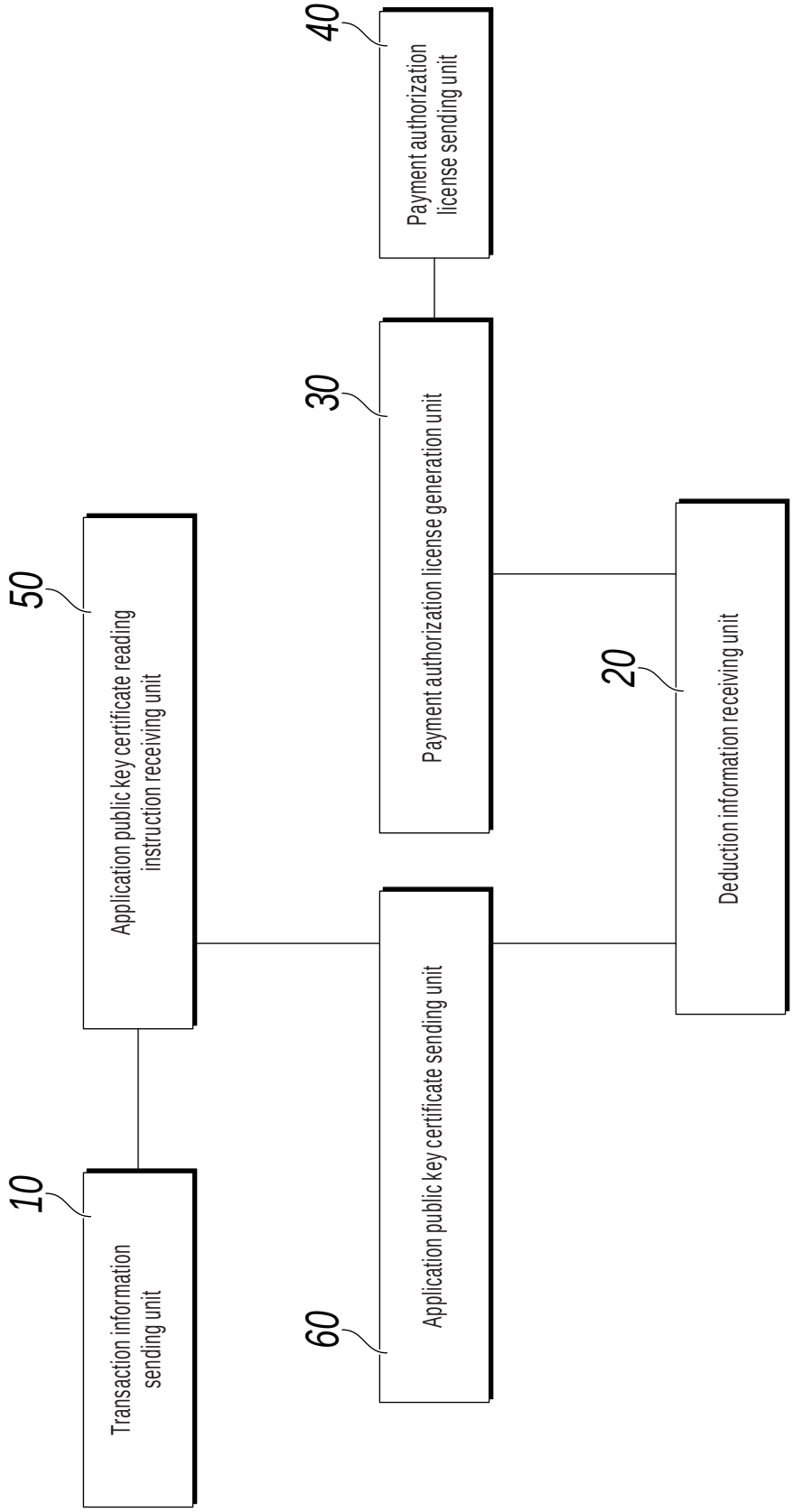

10
Transaction information sending unit
50
Application public key certificate reading instruction receiving unit
60
Application public key certificate sending unit
30
Payment authorization license generation unit
40
Payment authorization license sending unit
20
Deduction information receiving unit

FIG. 21

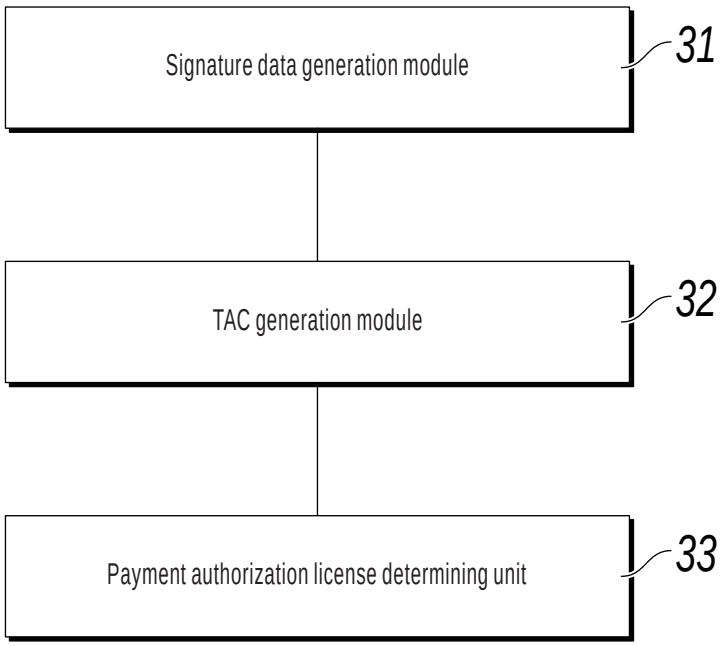

Signature data generation module
31
TAC generation module
32
Payment authorization license determining unit
33

FIG. 22

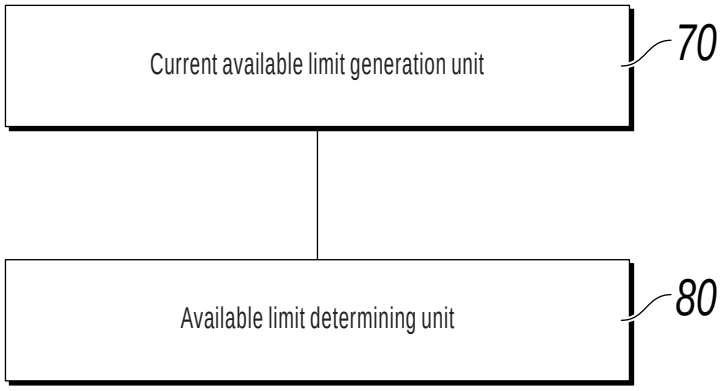

Current available limit generation unit
70
Available limit determining unit
80

FIG. 23

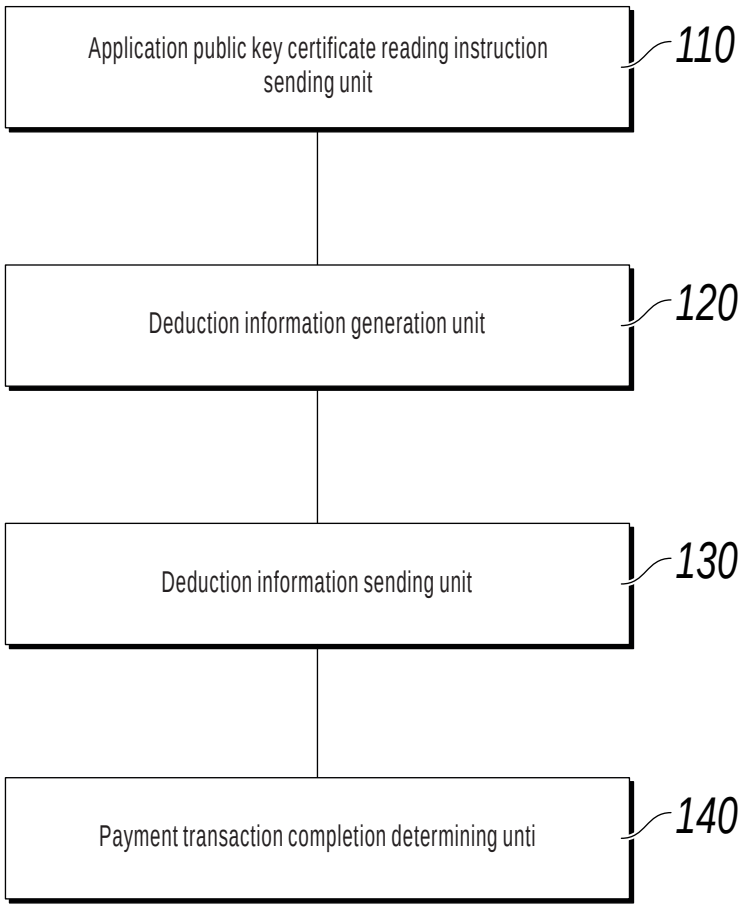

Application public key certificate reading instruction sending unit
110
Deduction information generation unit
120
Deduction information sending unit
130
Payment transaction completion determining unti
140

FIG. 24

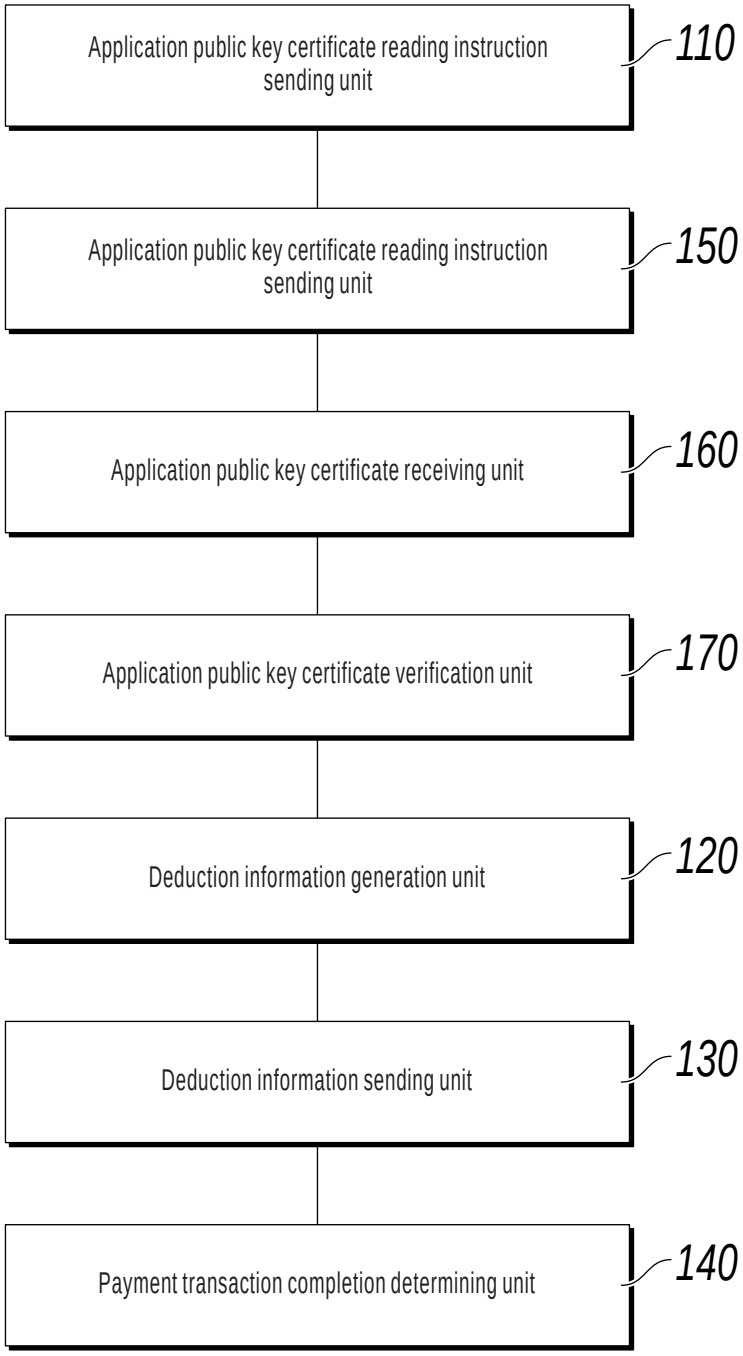

Application public key certificate reading instruction sending unit
110
Application public key certificate reading instruction sending unit
150
Application public key certificate receiving unit
160
Application public key certificate verification unit
170
Deduction information generation unit
120
Deduction information sending unit
130
Payment transaction completion determining unit
140

FIG. 25

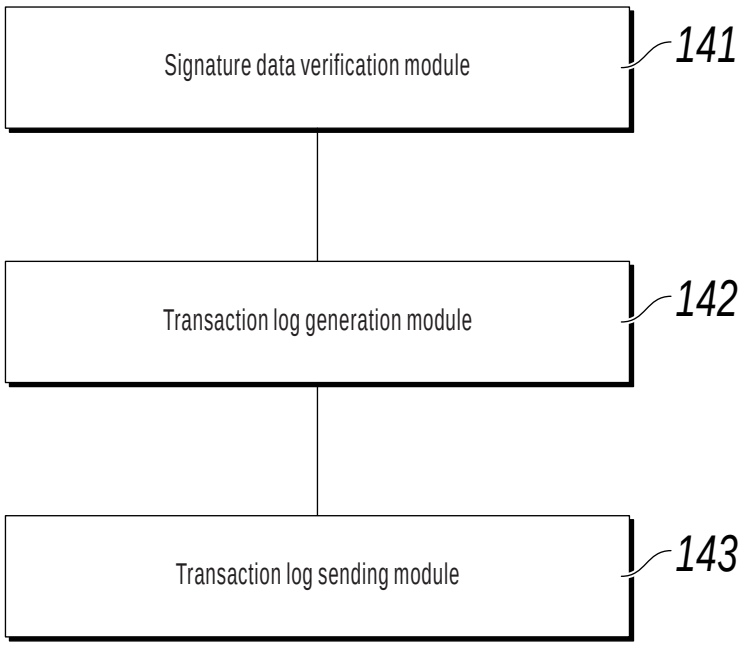

Signature data verification module
141
Transaction log generation module
142
Transaction log sending module
143

FIG. 26

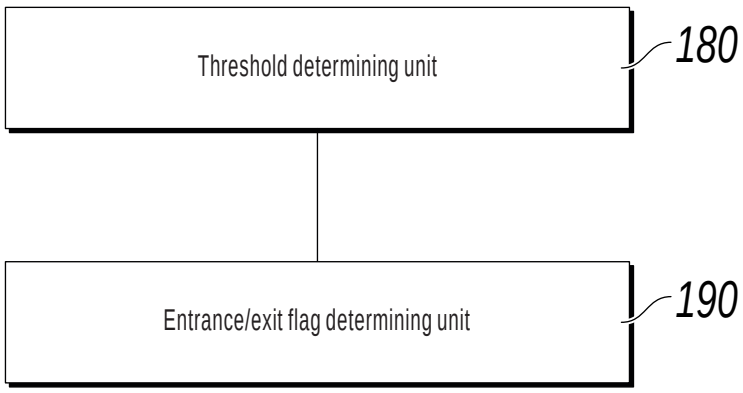

Threshold determining unit
180
Entrance/exit flag determining unit
190

FIG. 27

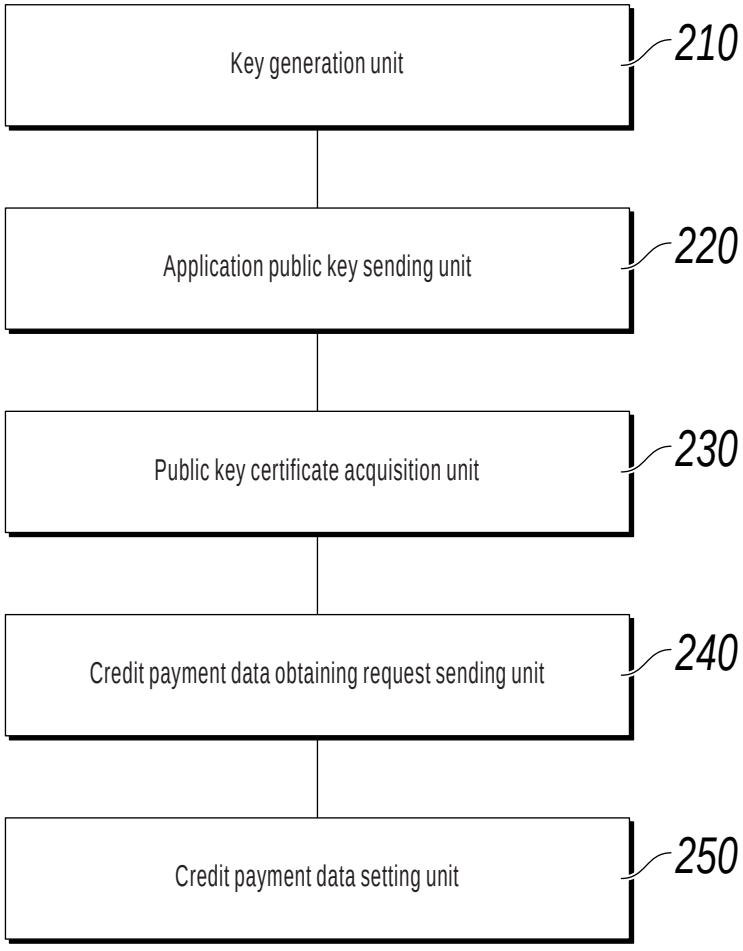

Key generation unit
210
Application public key sending unit
220
Public key certificate acquisition unit
230
Credit payment data obtaining request sending unit
240
Credit payment data setting unit
250

FIG. 28

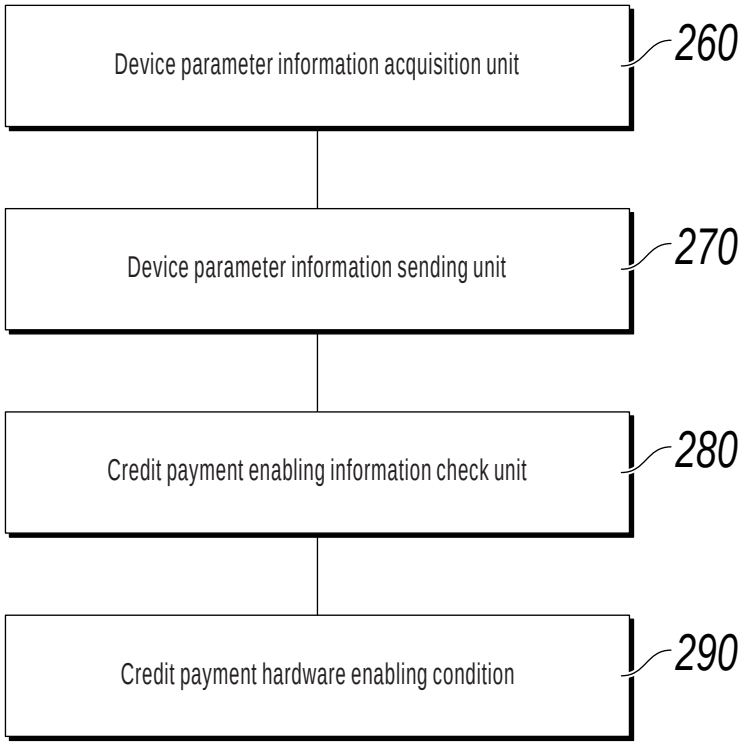

Device parameter information acquisition unit
260
Device parameter information sending unit
270
Credit payment enabling information check unit
280
Credit payment hardware enabling condition
290

FIG. 29

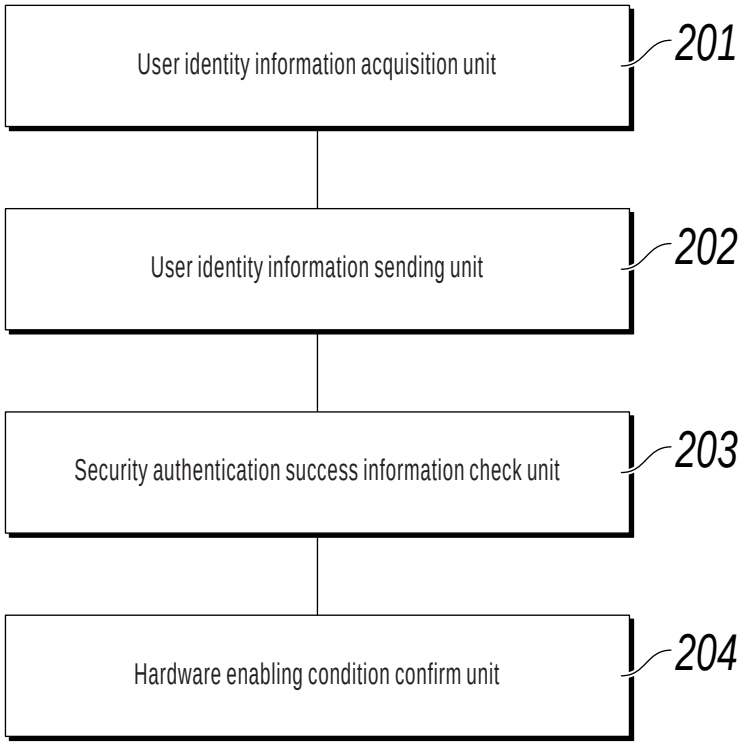

User identity information acquisition unit
201
User identity information sending unit
202
Security authentication success information check unit
203
Hardware enabling condition confirm unit
204

FIG. 30

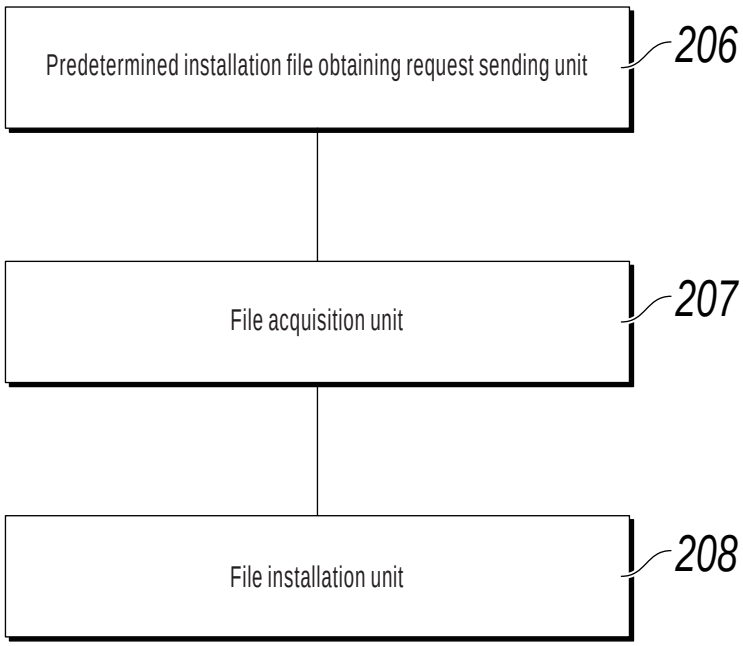

Predetermined installation file obtaining request sending unit
206
File acquisition unit
207
File installation unit
208

FIG. 31

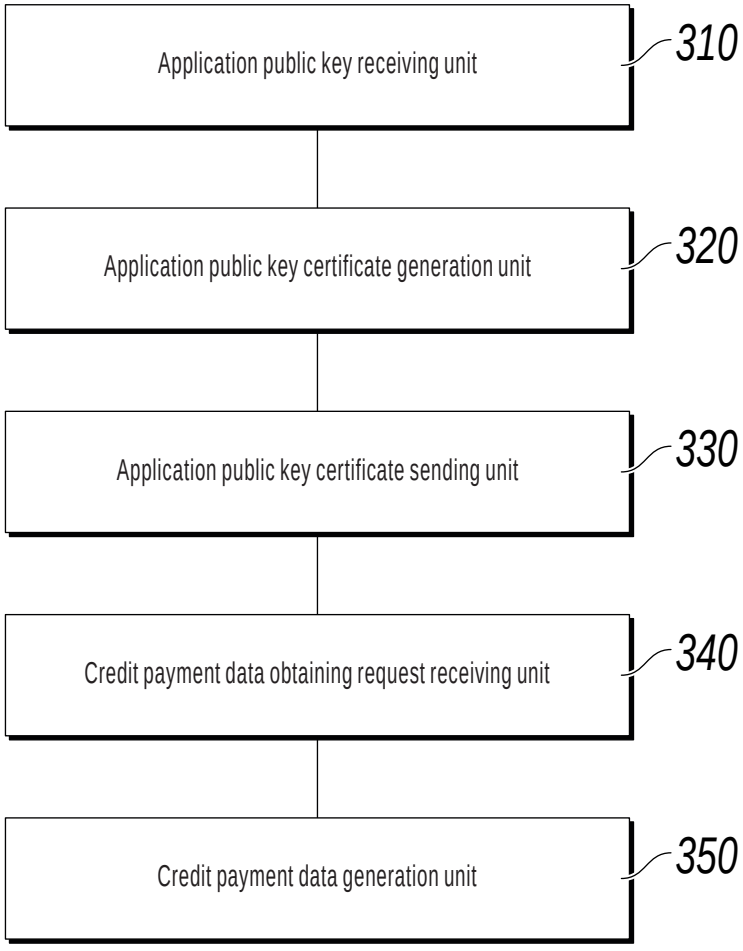

Application public key receiving unit
310
Application public key certificate generation unit
320
Application public key certificate sending unit
330
Credit payment data obtaining request receiving unit
340
Credit payment data generation unit
350

FIG. 32

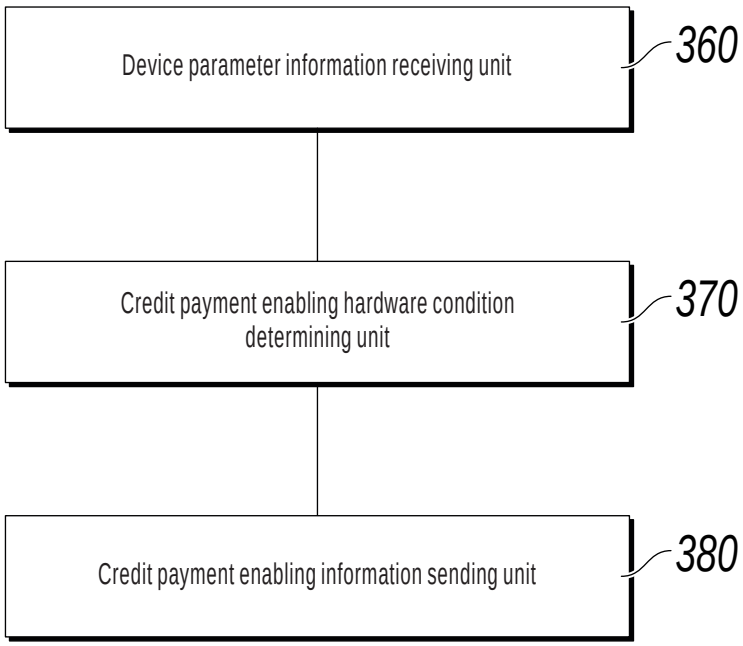

Device parameter information receiving unit
360
Credit payment enabling hardware condition determining unit
370
Credit payment enabling information sending unit
380

FIG. 33

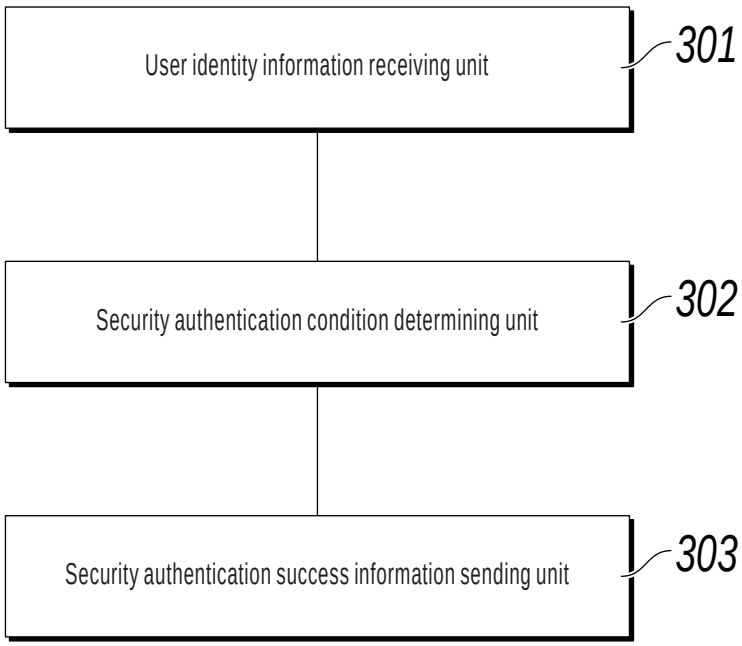

User identity information receiving unit
301
Security authentication condition determining unit
302
Security authentication success information sending unit
303

FIG. 34

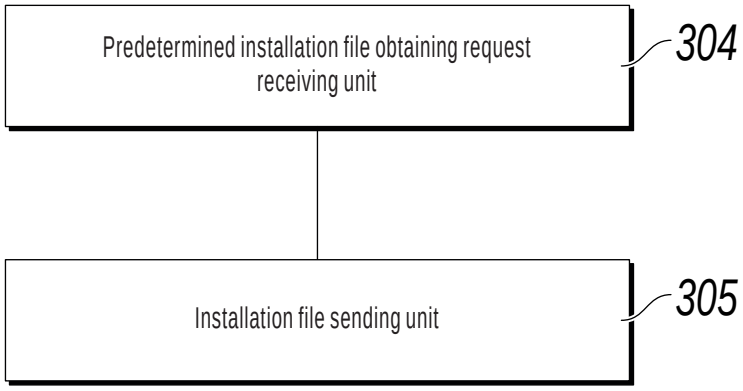

Predetermined installation file obtaining request receiving unit
304
Installation file sending unit
305

FIG. 35