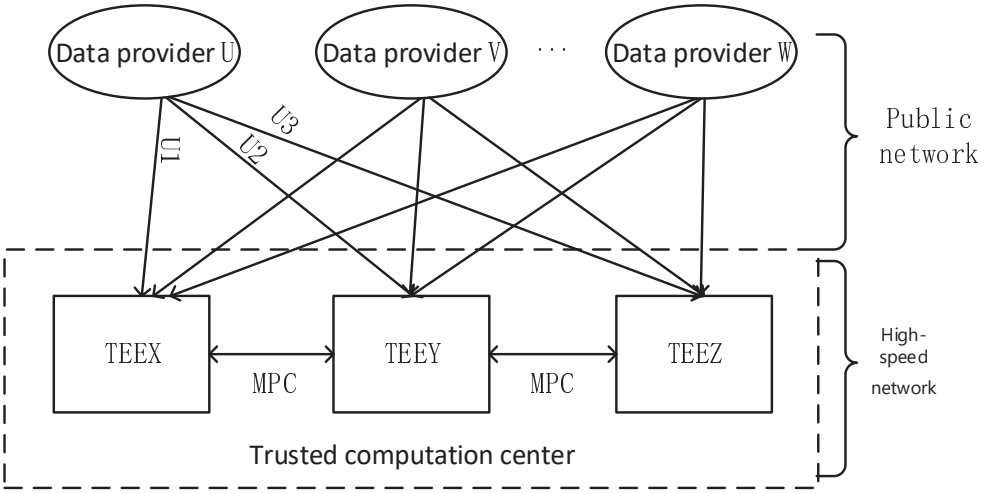
Data provider U
Data provider V
Data provider W
U1
U2
U3
Public network
TEEX
MPC
TEEY
MPC
TEEZ
High-speed network
Trusted computation center

FIG. 1

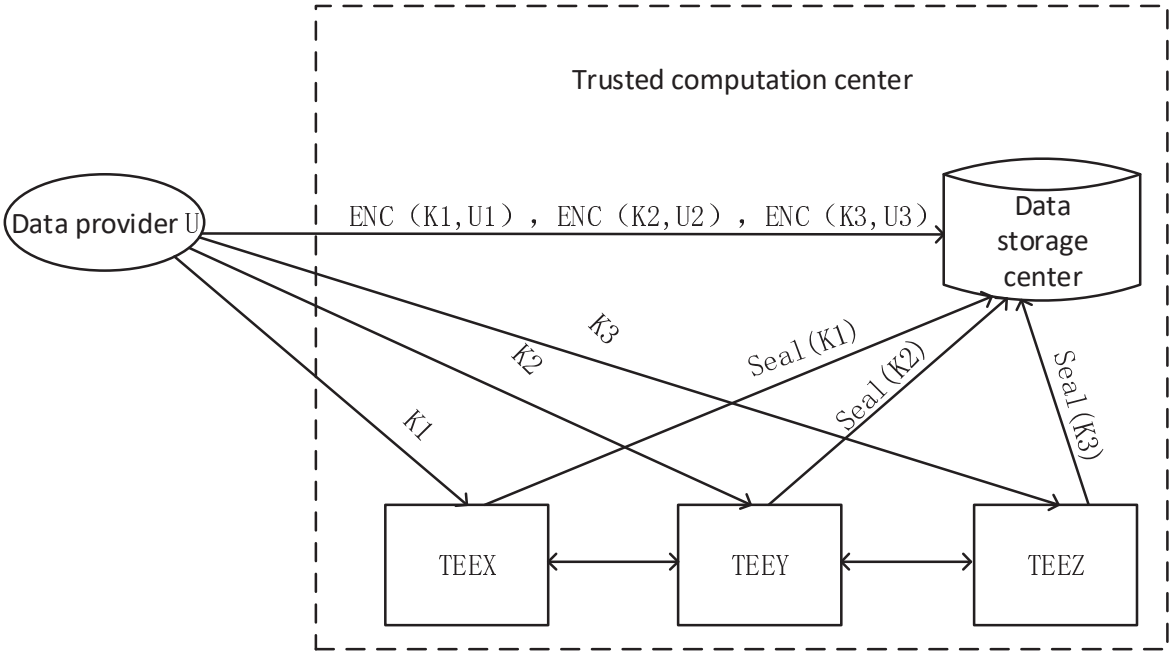
Trusted computation center
Data provider U
ENC（K1,U1），ENC（K2,U2），ENC（K3,U3）
Data storage center
K3
K2
K1
Seal(K1)
Seal(K2)
Seal(K3)
TEEX
TEEY
TEEZ

FIG. 2

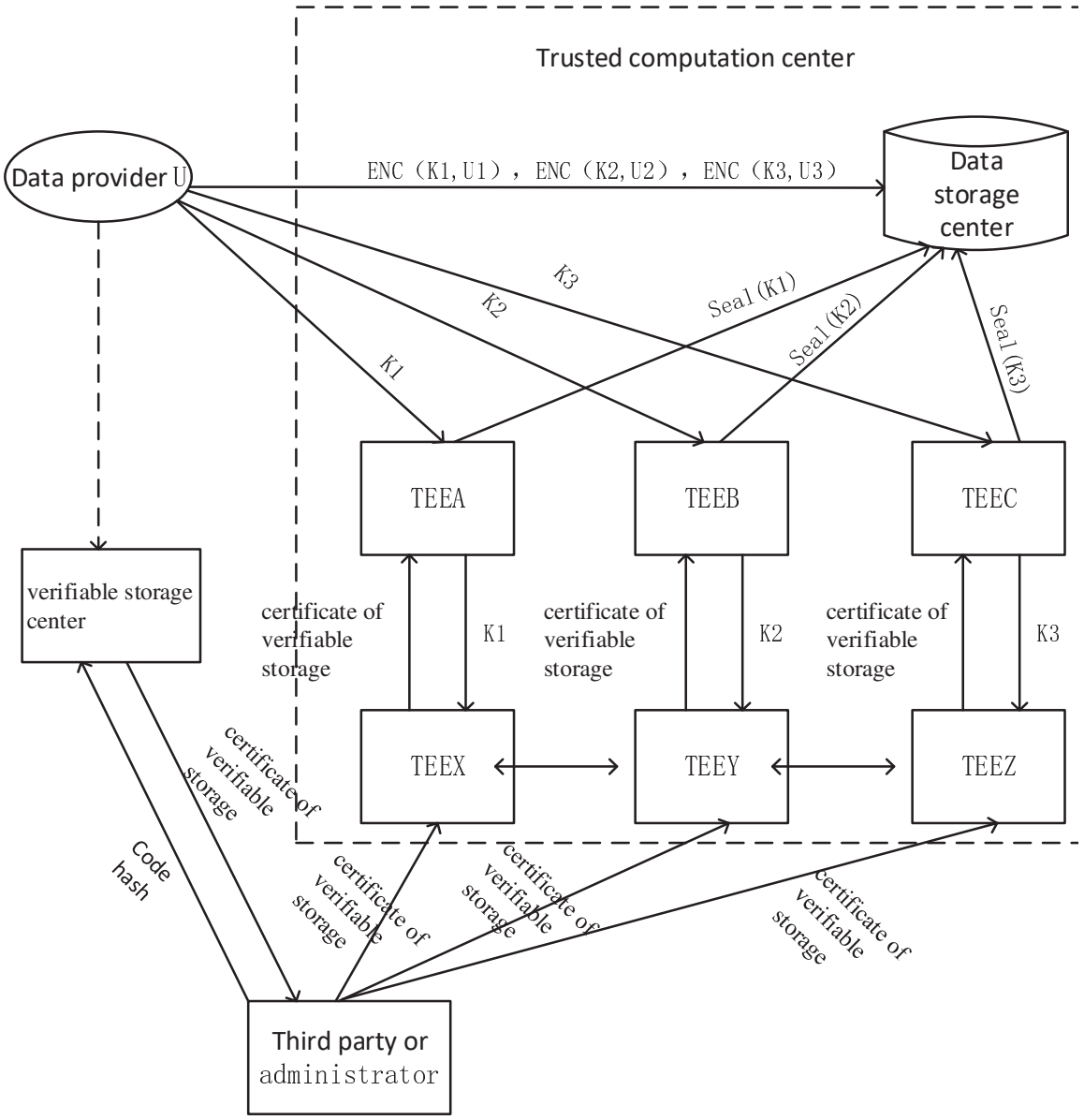
Trusted computation center
Data provider U
ENC（K1,U1），ENC（K2,U2），ENC（K3,U3）
Data storage center
K3
K2
K1
Seal(K1)
Seal(K2)
Seal(K3)
TEEA
TEEB
TEEC
verifiable storage center
certificate of verifiable storage
K1
certificate of verifiable storage
K2
certificate of verifiable storage
K3
TEEX
TEEY
TEEZ
Code hash
certificate of verifiable storage
certificate of verifiable storage
certificate of verifiable storage
certificate of verifiable storage
Third party or administrator

FIG. 3

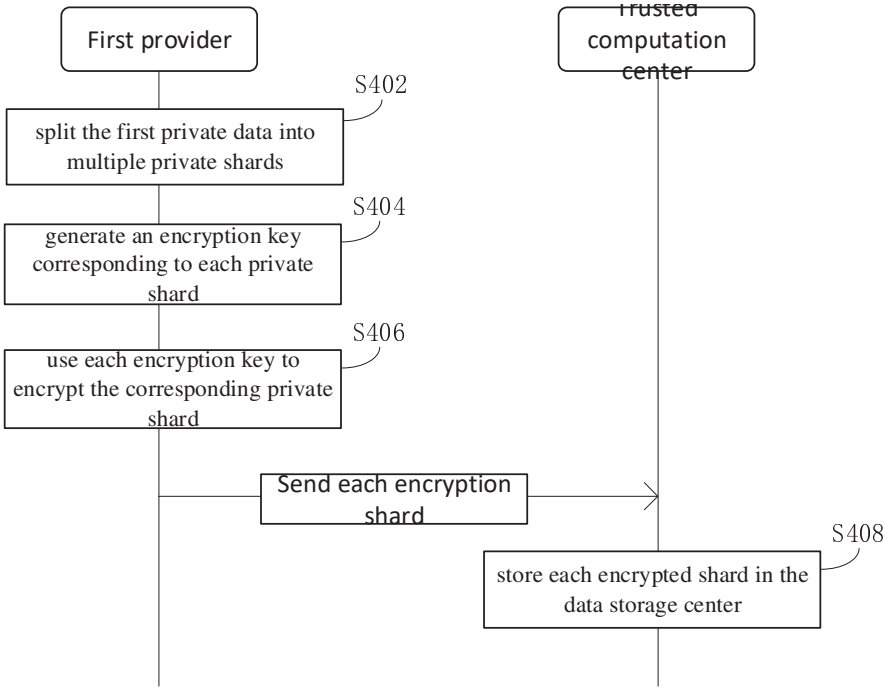
First provider
Trusted computation center
S402
split the first private data into multiple private shards
S404
generate an encryption key corresponding to each private shard
S406
use each encryption key to encrypt the corresponding private shard
Send each encryption shard
S408
store each encrypted shard in the data storage center

FIG.4

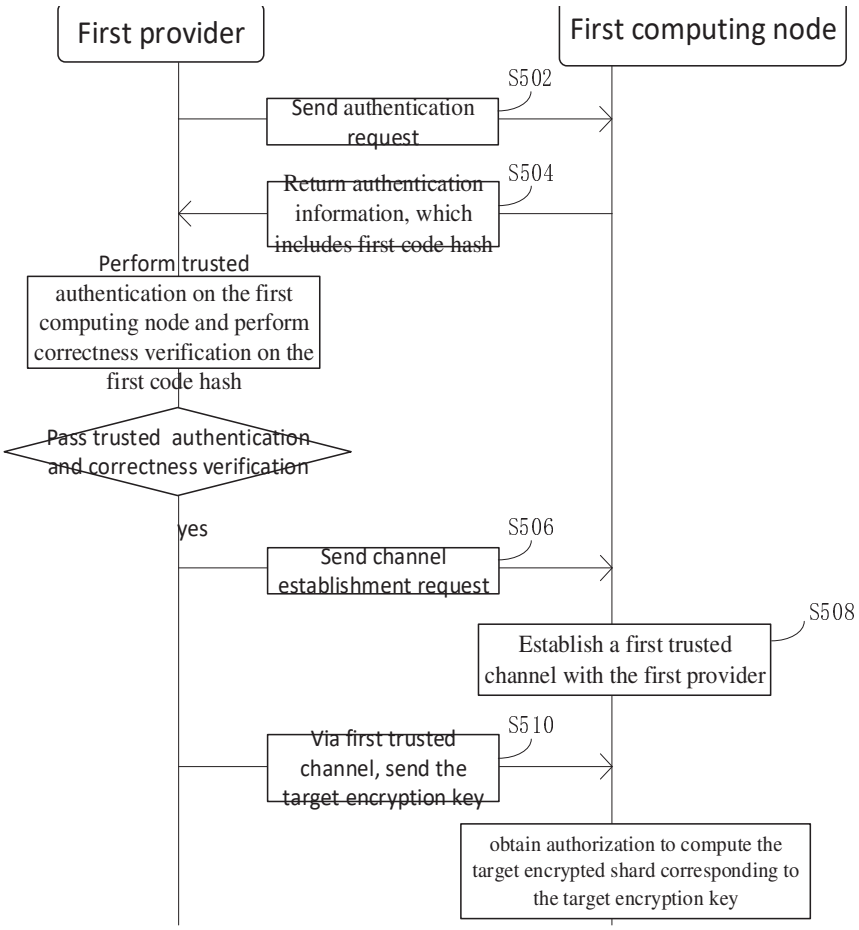
First provider
First computing node
S502
Send authentication request
S504
Return authentication information, which includes first code hash
Perform trusted authentication on the first computing node and perform correctness verification on the first code hash
Pass trusted authentication and correctness verification
yes
S506
Send channel establishment request
S508
Establish a first trusted channel with the first provider
S510
Via first trusted channel, send the target encryption key
obtain authorization to compute the target encrypted shard corresponding to the target encryption key

FIG.5

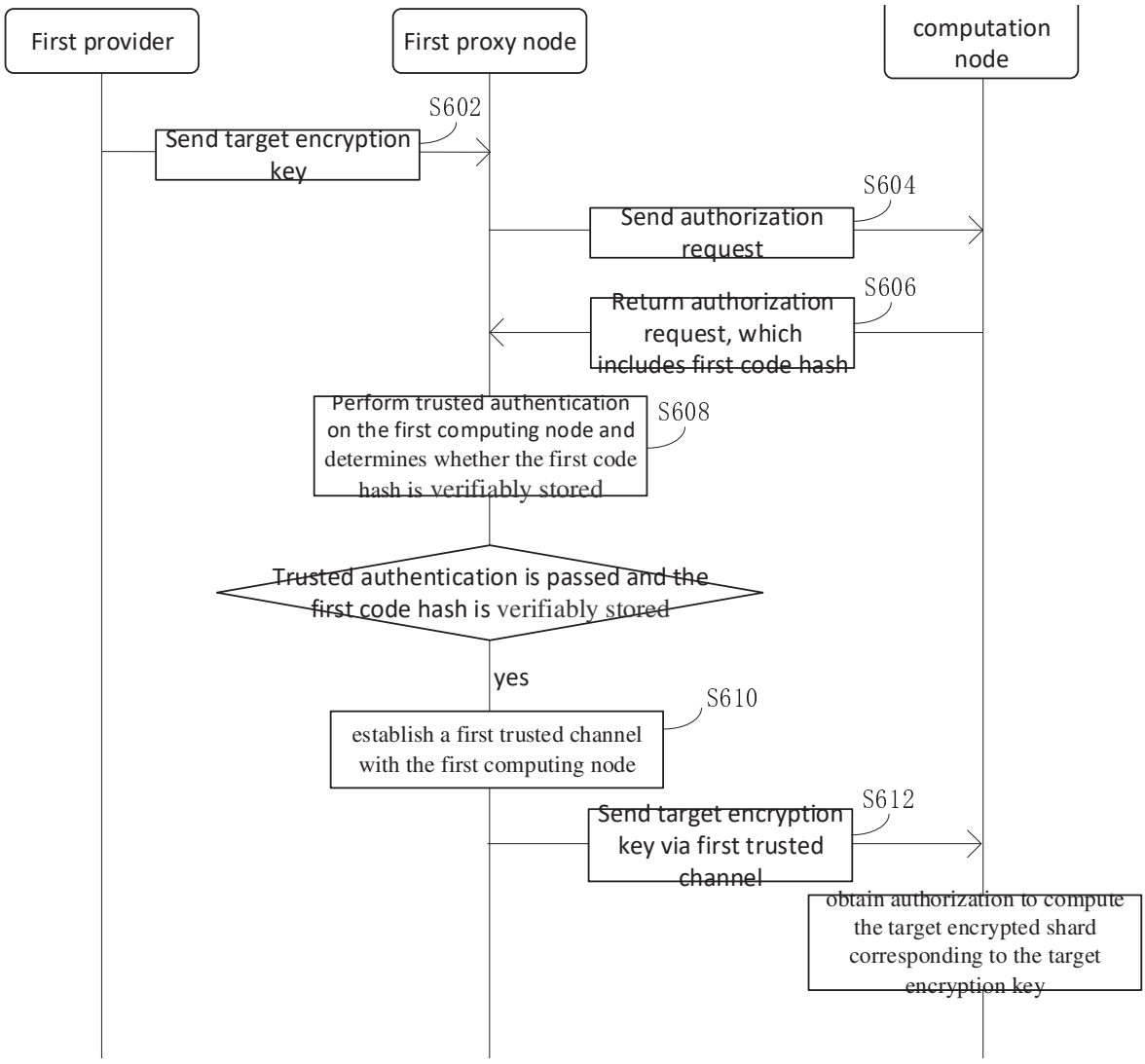
First provider
First proxy node
computation node
S602
Send target encryption key
S604
Send authorization request
S606
Return authorization request, which includes first code hash
Perform trusted authentication on the first computing node and determines whether the first code hash is verifiably stored
S608
Trusted authentication is passed and the first code hash is verifiably stored
yes
S610
establish a first trusted channel with the first computing node
S612
Send target encryption key via first trusted channel
obtain authorization to compute the target encrypted shard corresponding to the target encryption key

FIG.6

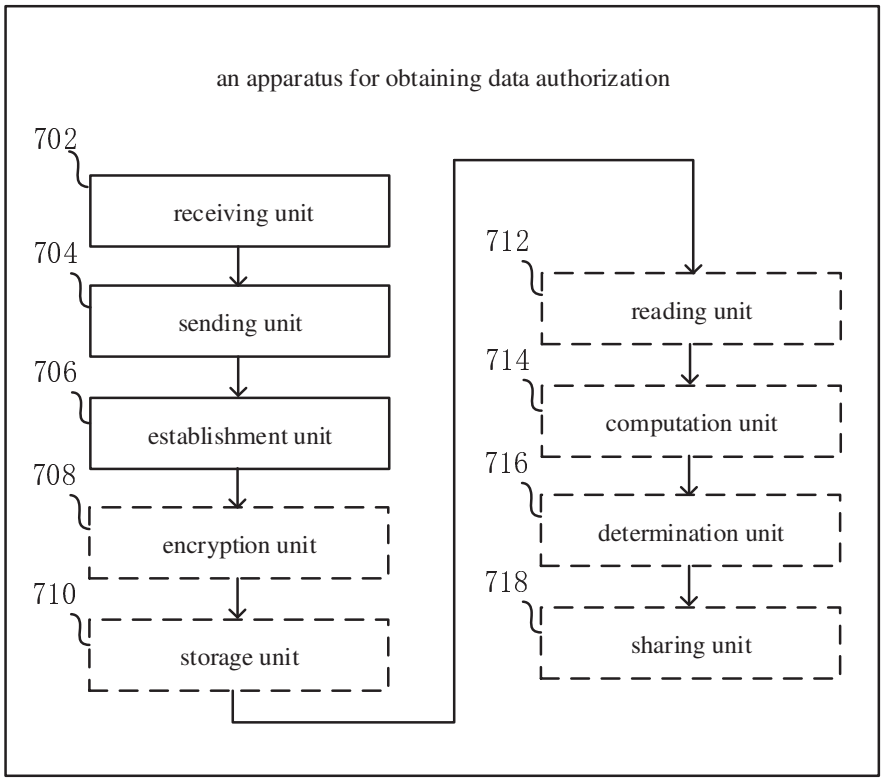
an apparatus for obtaining data authorization
702
receiving unit
704
sending unit
706
establishment unit
708
encryption unit
710
storage unit
712
reading unit
714
computation unit
716
determination unit
718
sharing unit

FIG.7

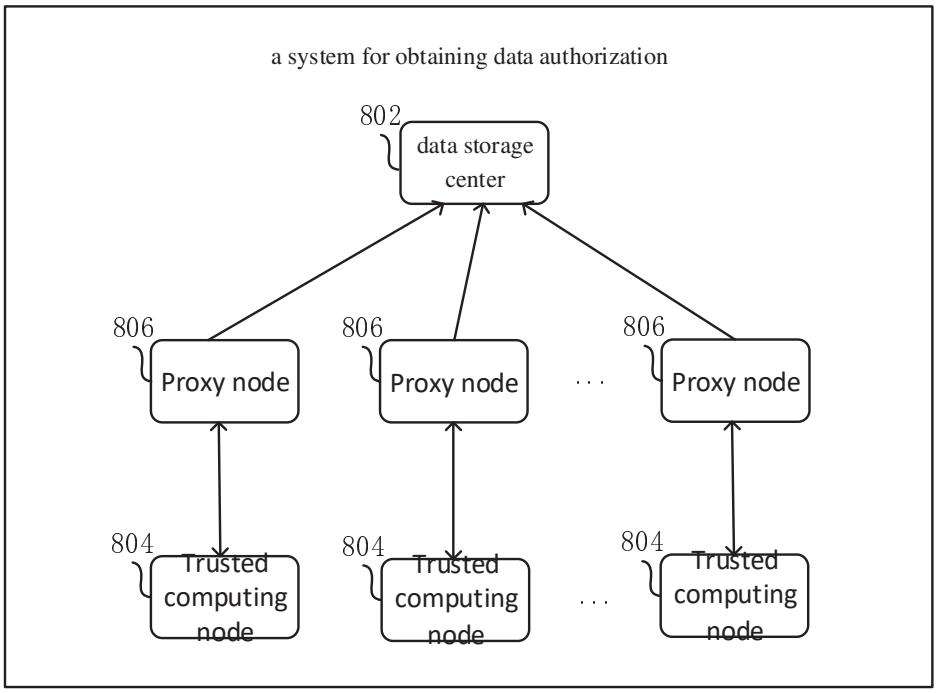
a system for obtaining data authorization
802
data storage center
806
Proxy node
806
Proxy node
806
Proxy node
804
Trusted computing node
804
Trusted computing node
804
Trusted computing node

FIG.8

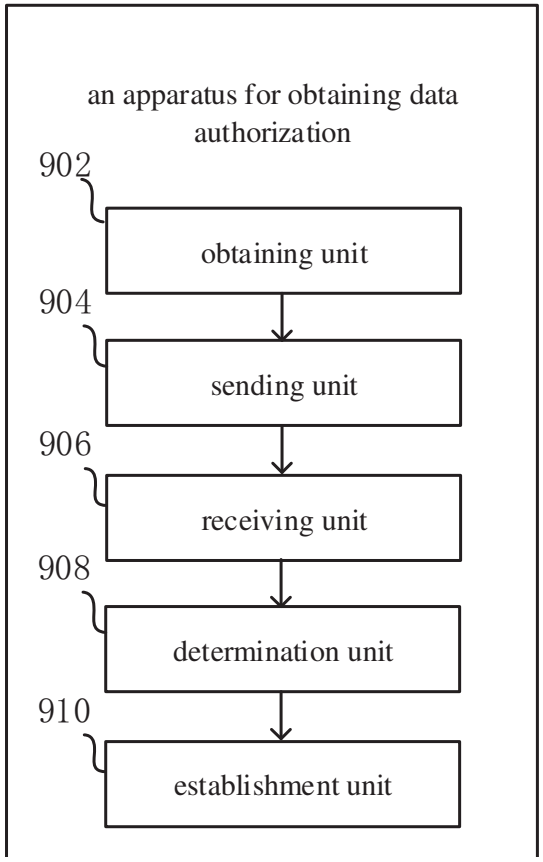
an apparatus for obtaining data authorization
902
obtaining unit
904
sending unit
906
receiving unit
908
determination unit
910
establishment unit

FIG.9