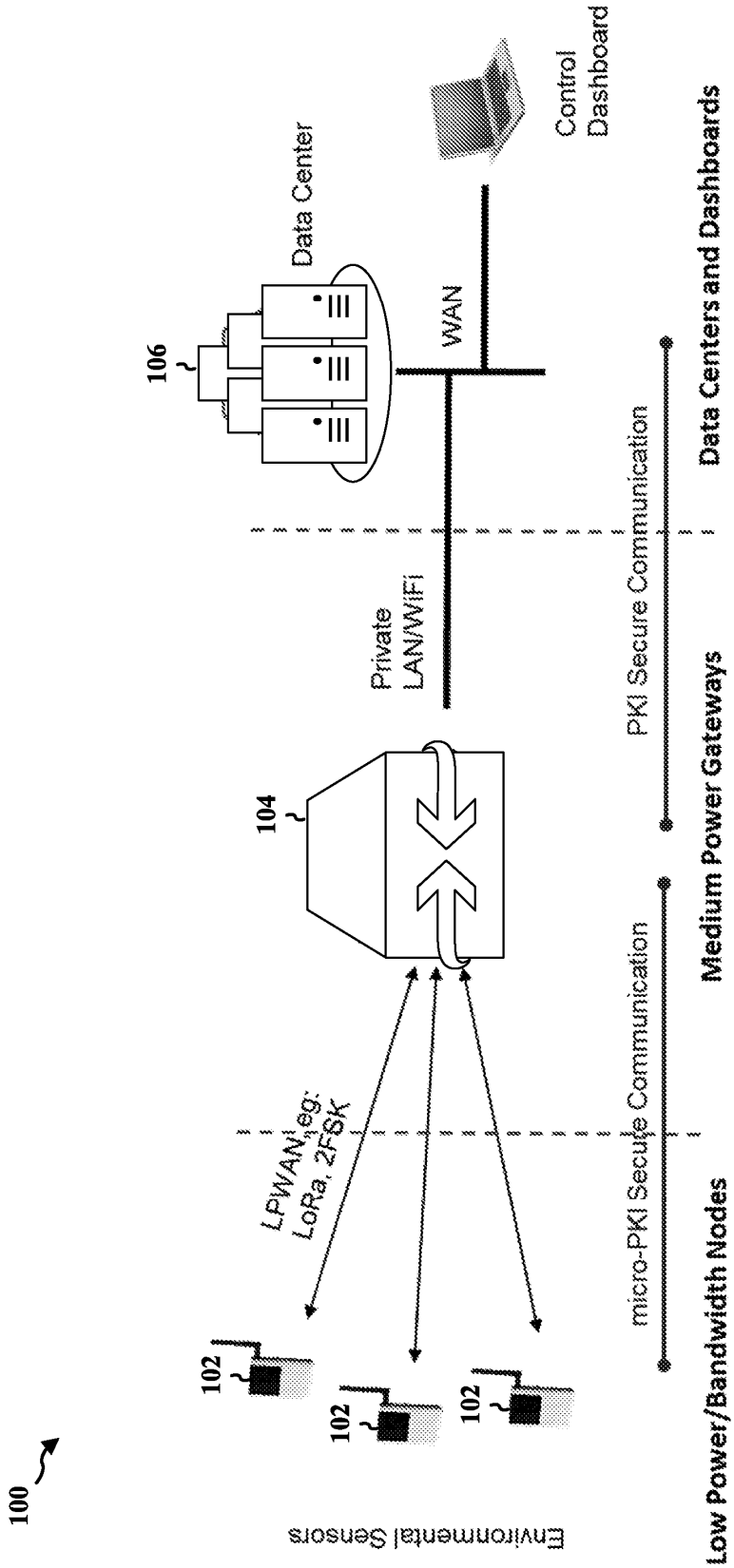
100
Environmental Sensors
102
102
102
LPWAN, eg: LoRa, 2FSK
104
106
Data Center
WAN
Private LAN/WiFi
Control Dashboard
micro-PKI Secure Communication
PKI Secure Communication
Low Power/Bandwidth Nodes
Medium Power Gateways
Data Centers and Dashboards

FIG. 1

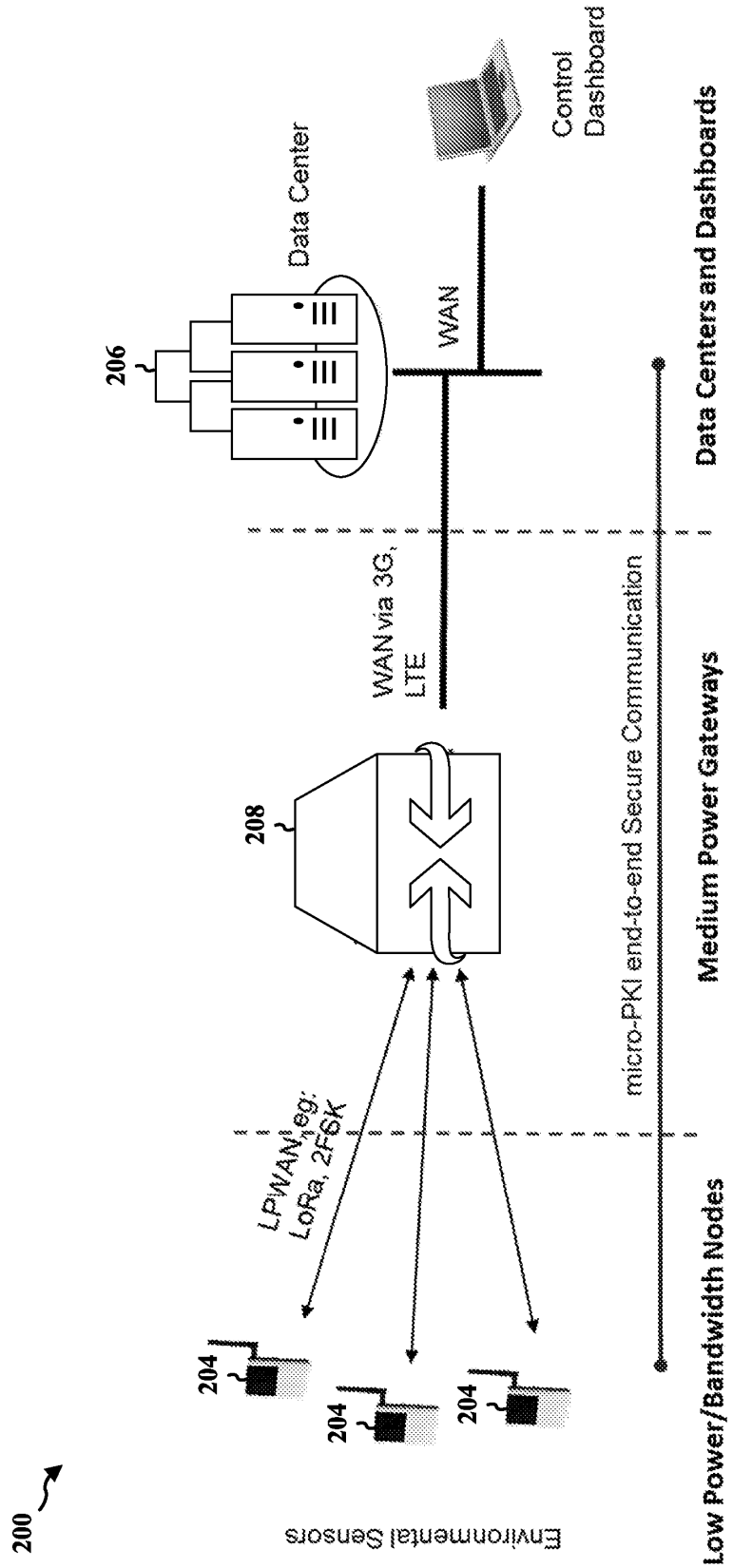
200
Environmental Sensors
204
204
204
LPWAN, eg: LoRa, 2FSK
208
WAN via 3G, LTE
206
Data Center
WAN
Control Dashboard
micro-PKI end-to-end Secure Communication
Low Power/Bandwidth Nodes
Medium Power Gateways
Data Centers and Dashboards

FIG. 2

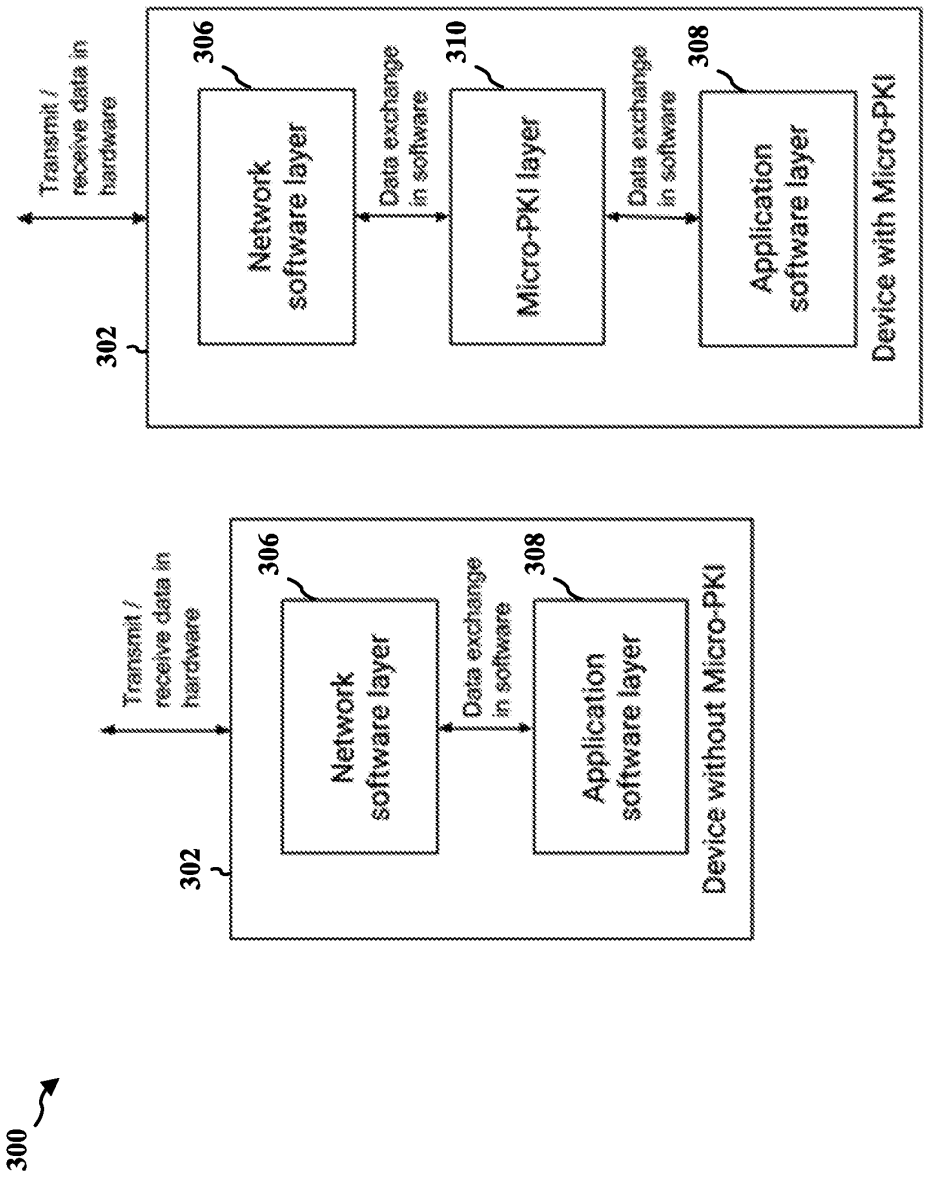
300
302
Transmit / receive data in hardware
306
Network software layer
Data exchange in software
308
Application software layer
Device without Micro-PKI
302
Transmit / receive data in hardware
306
Network software layer
Data exchange in software
310
Micro-PKI layer
Data exchange in software
308
Application software layer
Device with Micro-PKI

FIG. 3

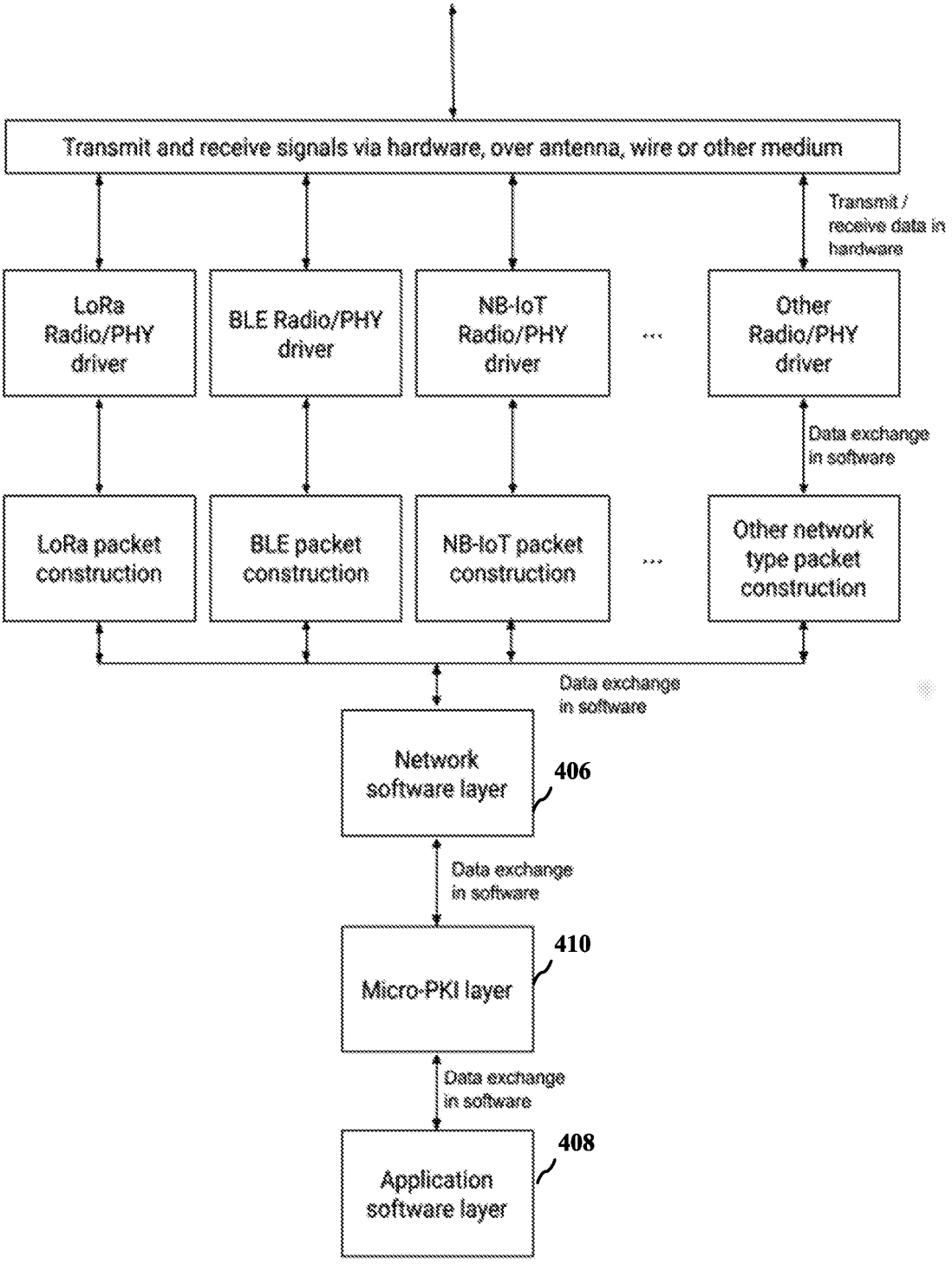
Transmit and receive signals via hardware, over antenna, wire or other medium
Transmit / receive data in hardware
LoRa Radio/PHY driver
BLE Radio/PHY driver
NB-IoT Radio/PHY driver
...
Other Radio/PHY driver
Data exchange in software
LoRa packet construction
BLE packet construction
NB-IoT packet construction
...
Other network type packet construction
Data exchange in software
Network software layer
406
Data exchange in software
Micro-PKI layer
410
Data exchange in software
Application software layer
408

FIG. 4

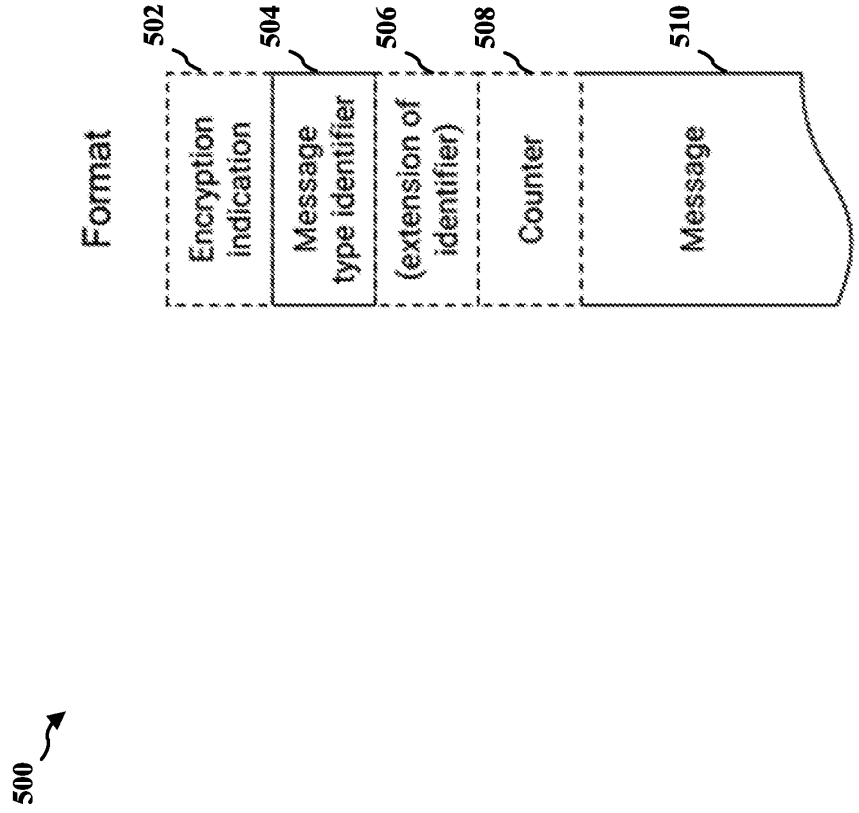
500
Format
502
Encryption indication
504
Message type identifier
506
(extension of identifier)
508
Counter
510
Message

FIG. 5

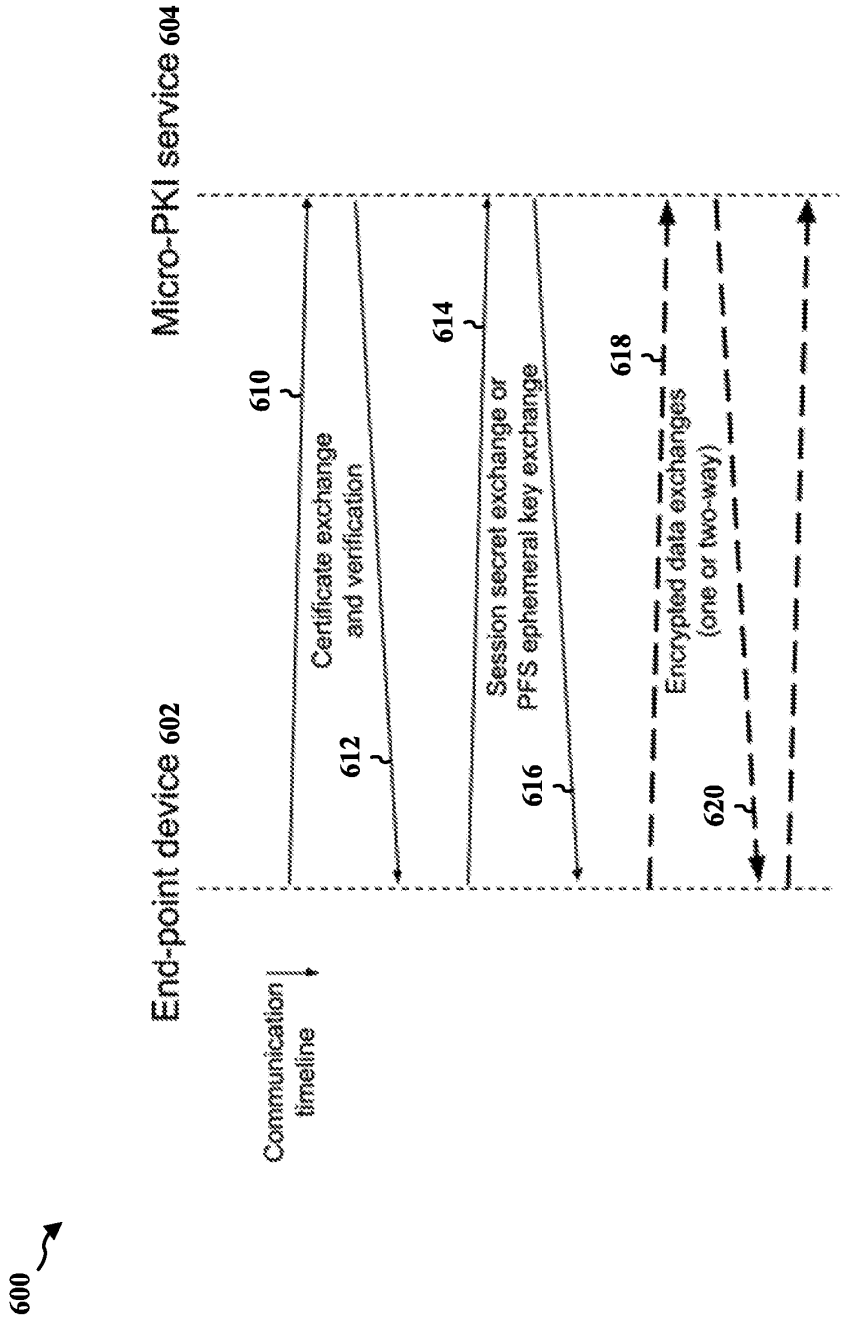
600
End-point device 602
Micro-PKI service 604
Communication timeline
610
Certificate exchange and verification
612
614
Session secret exchange or PFS ephemeral key exchange
616
618
Encrypted data exchanges (one or two-way)
620

FIG. 6

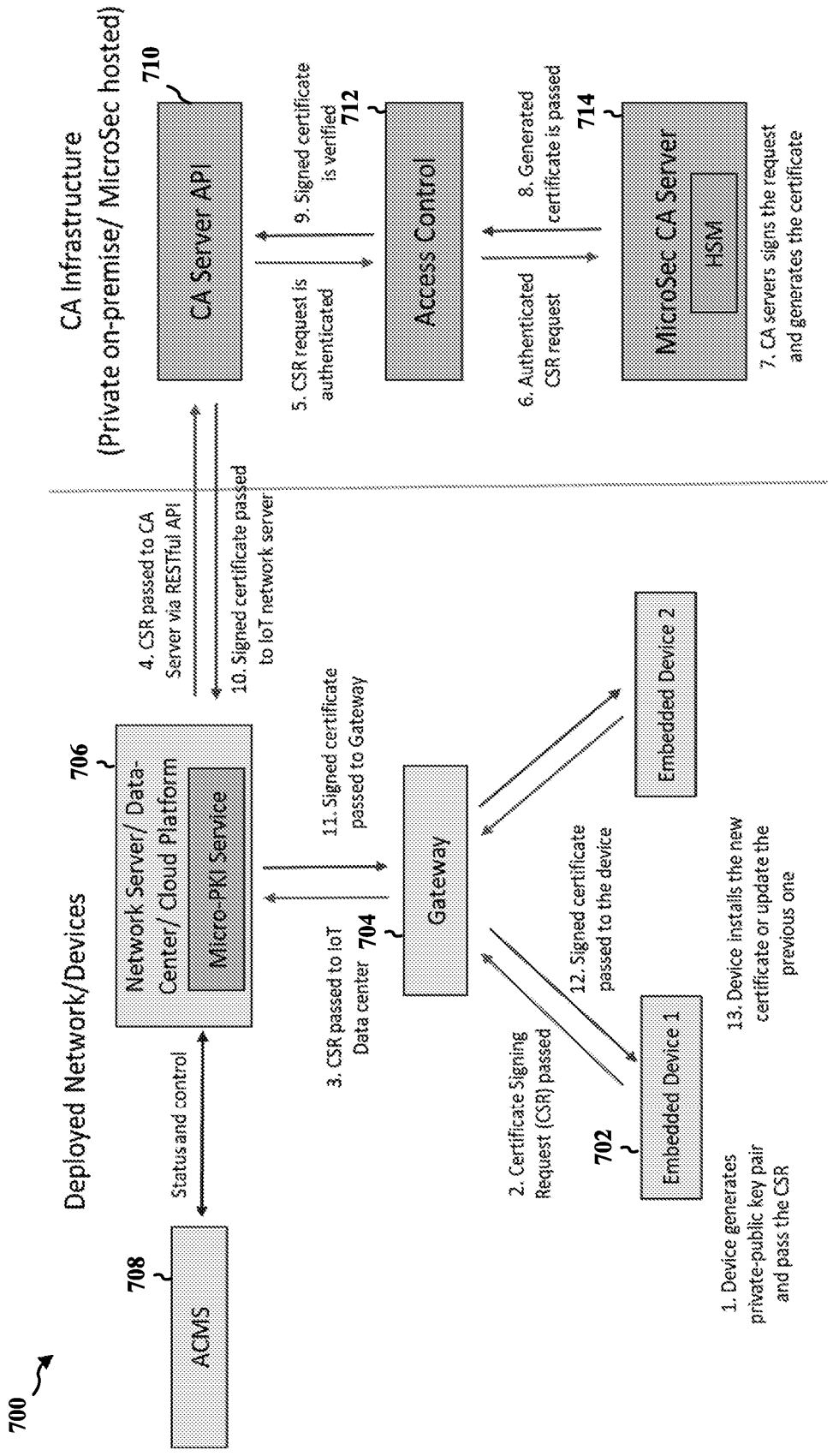
700
Deployed Network/Devices
CA Infrastructure
(Private on-premise/ MicroSec hosted)
708
ACMS
Status and control
Network Server/ Data-Center/ Cloud Platform
706
Micro-PKI Service
4. CSR passed to CA Server via RESTful API
10. Signed certificate passed to IoT network server
CA Server API
710
5. CSR request is authenticated
9. Signed certificate is verified
712
Access Control
6. Authenticated CSR request
8. Generated certificate is passed
714
MicroSec CA Server
HSM
7. CA servers signs the request and generates the certificate
3. CSR passed to IoT Data center
704
11. Signed certificate passed to Gateway
Gateway
2. Certificate Signing Request (CSR) passed
12. Signed certificate passed to the device
Embedded Device 2
702
Embedded Device 1
1. Device generates private-public key pair and pass the CSR
13. Device installs the new certificate or update the previous one

FIG. 7

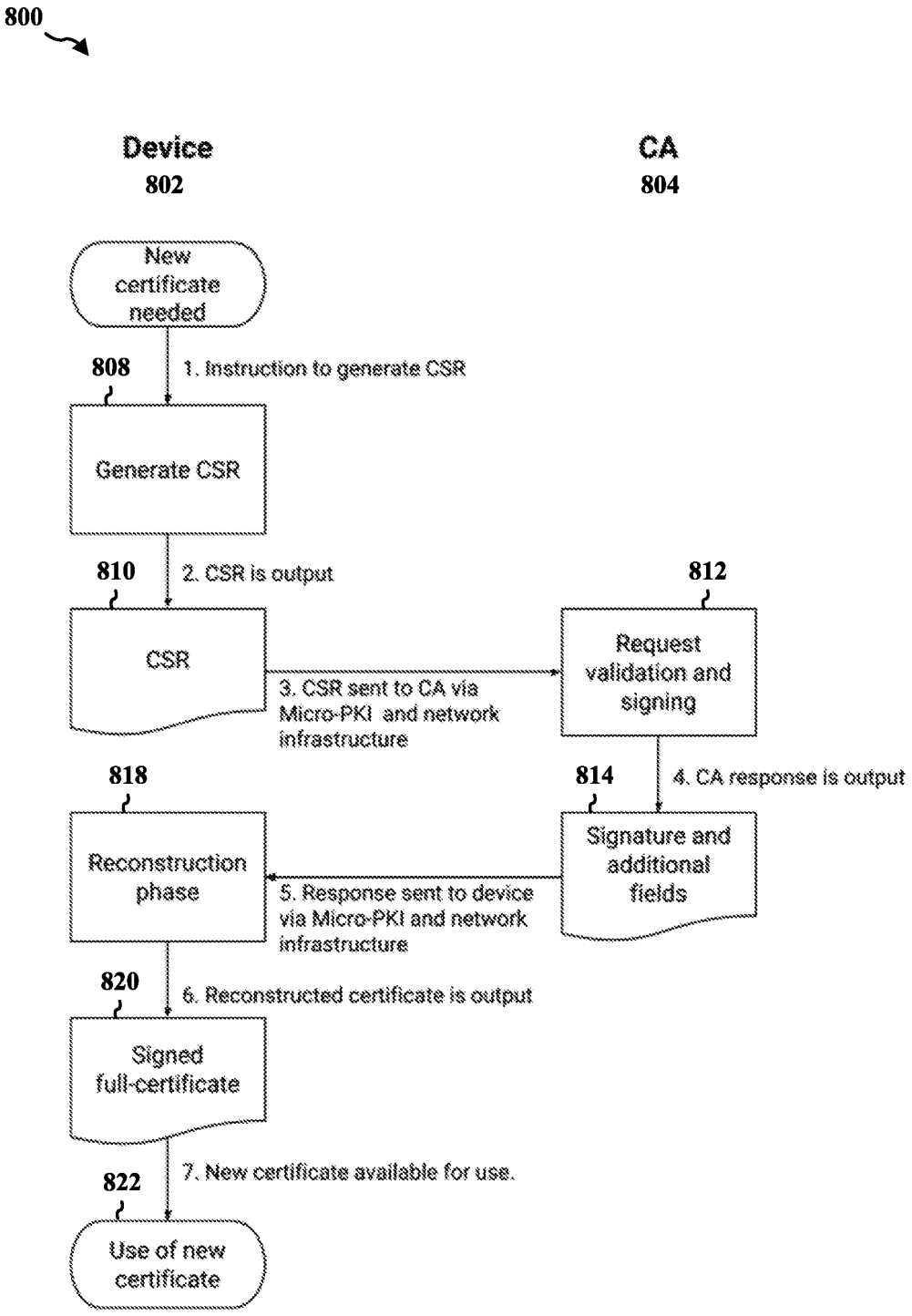
800
Device
802
CA
804
New certificate needed
808
1. Instruction to generate CSR
Generate CSR
810
2. CSR is output
CSR
812
Request validation and signing
3. CSR sent to CA via Micro-PKI and network infrastructure
818
814
4. CA response is output
Reconstruction phase
Signature and additional fields
5. Response sent to device via Micro-PKI and network infrastructure
820
6. Reconstructed certificate is output
Signed full-certificate
822
7. New certificate available for use.
Use of new certificate

FIG. 8

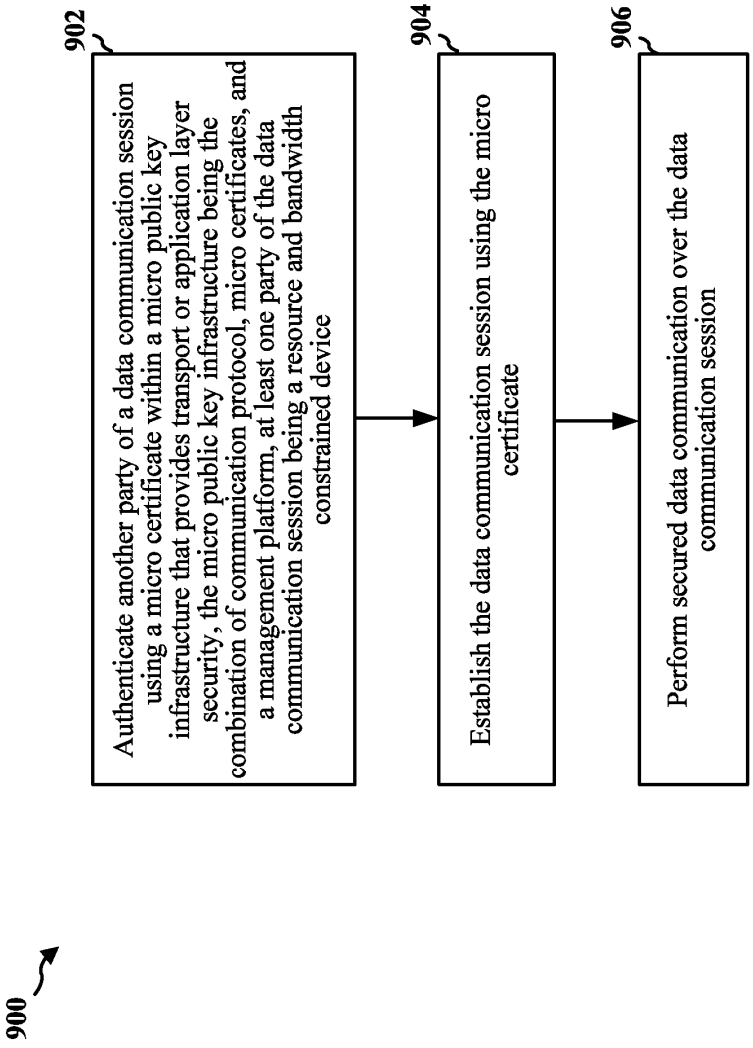
900
902
Authenticate another party of a data communication session using a micro certificate within a micro public key infrastructure that provides transport or application layer security, the micro public key infrastructure being the combination of communication protocol, micro certificates, and a management platform, at least one party of the data communication session being a resource and bandwidth constrained device
904
Establish the data communication session using the micro certificate
906
Perform secured data communication over the data communication session

FIG. 9

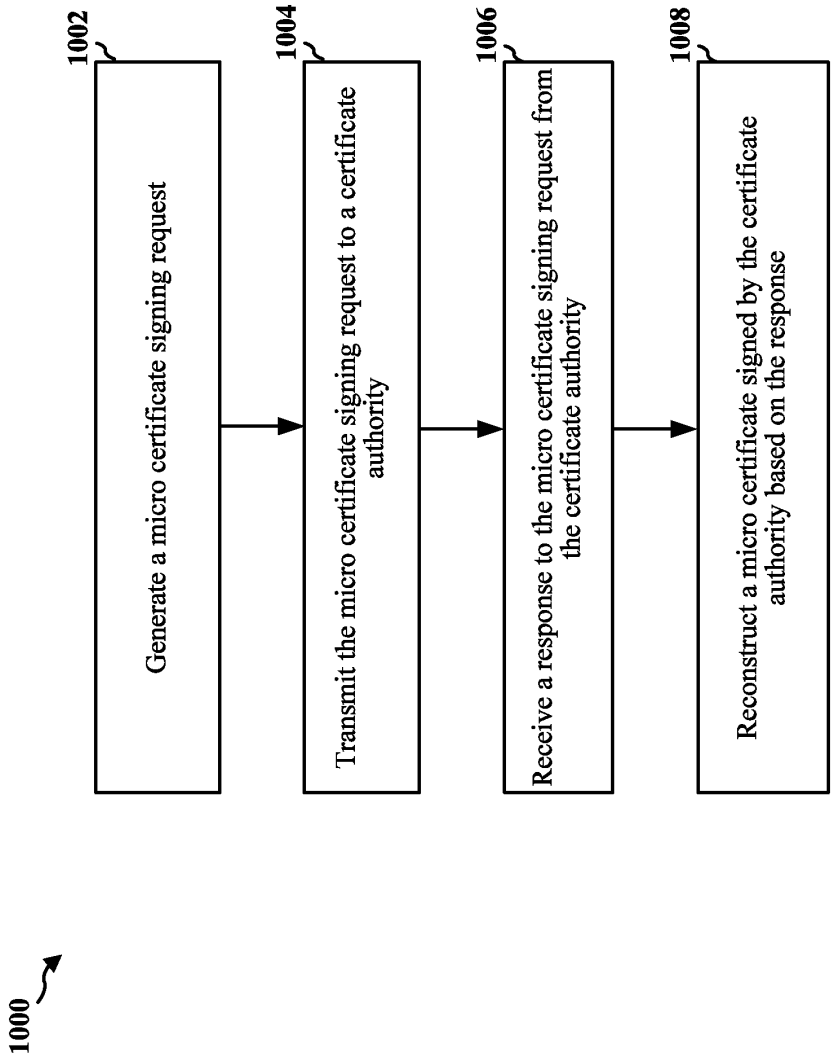
1000
1002
Generate a micro certificate signing request
1004
Transmit the micro certificate signing request to a certificate authority
1006
Receive a response to the micro certificate signing request from the certificate authority
1008
Reconstruct a micro certificate signed by the certificate authority based on the response

FIG. 10

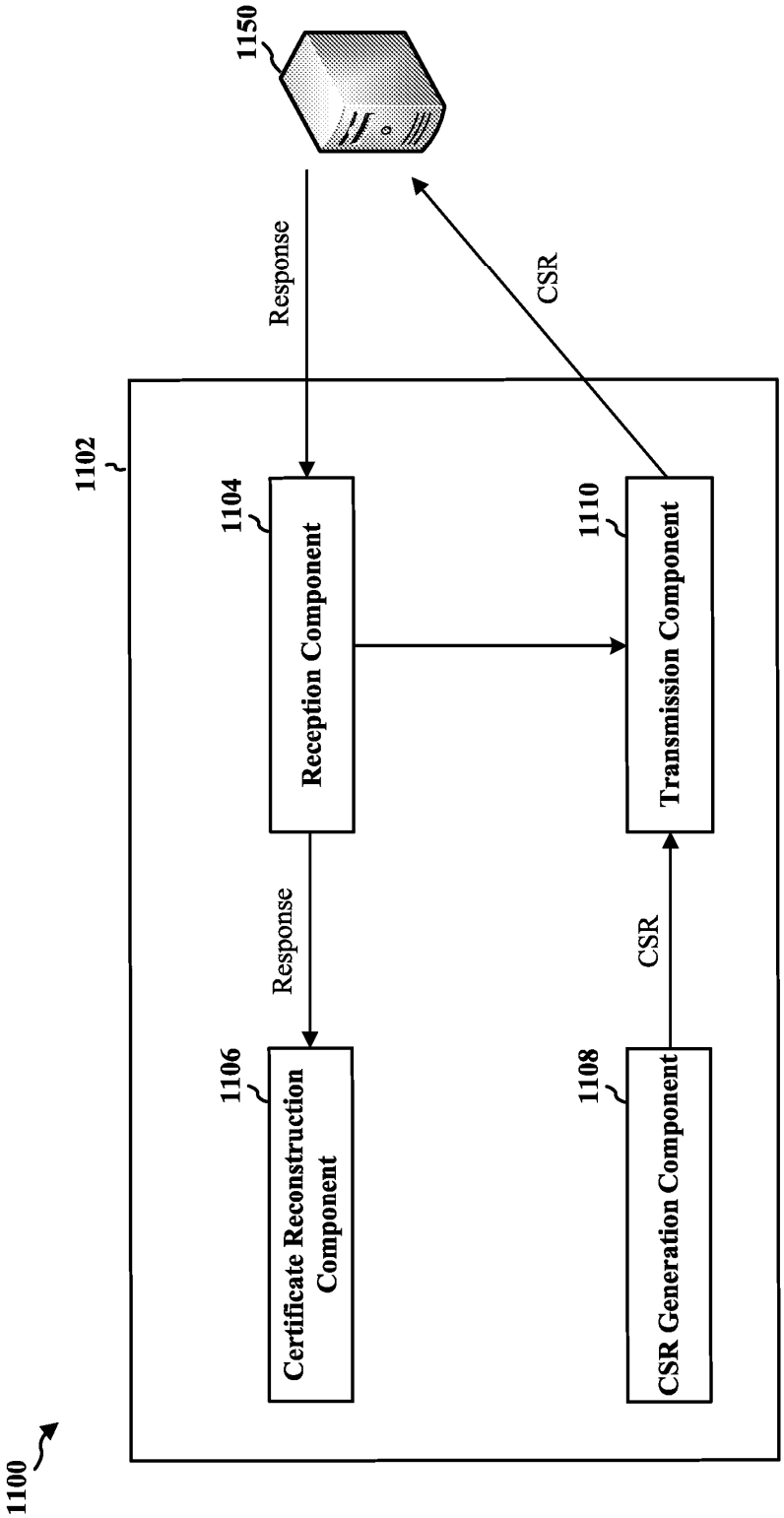
1150
Response
CSR
1102
1104
Reception Component
1110
Transmission Component
Response
CSR
1106
Certificate Reconstruction Component
1108
CSR Generation Component
1100

FIG. 11

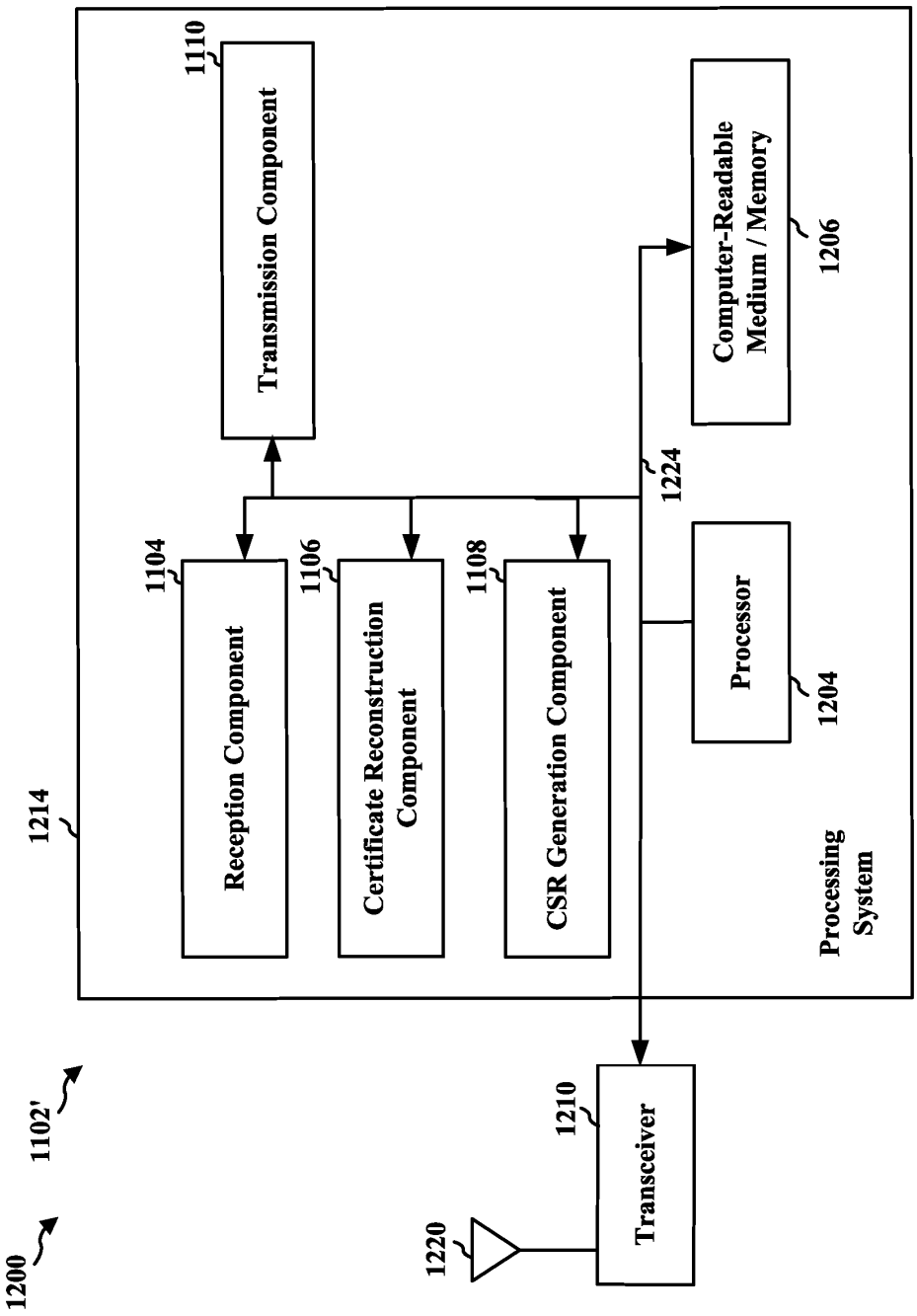
1200
1102'
1214
1110
Transmission Component
1104
Reception Component
1106
Certificate Reconstruction Component
1108
CSR Generation Component
1224
Computer-Readable Medium / Memory
1206
Processor
1204
Processing System
1210
Transceiver
1220

FIG. 12

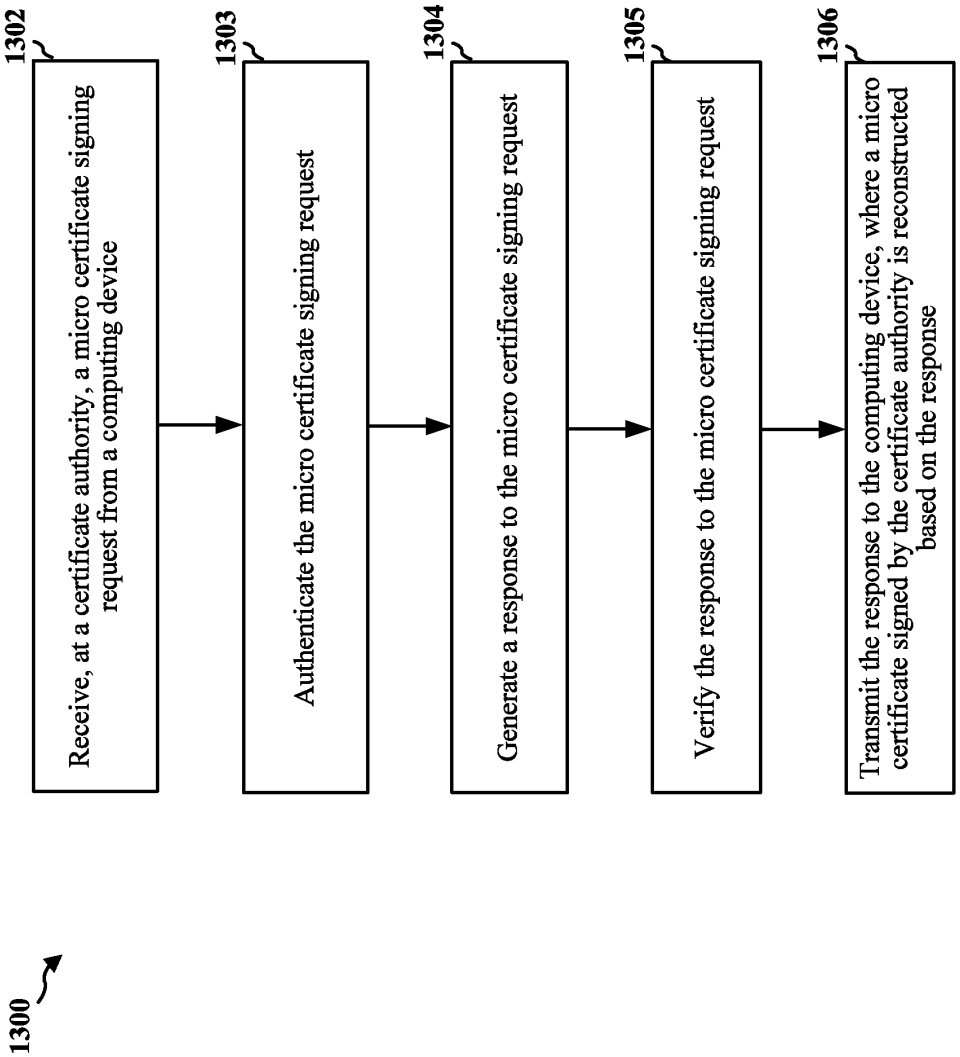
1300
1302
Receive, at a certificate authority, a micro certificate signing request from a computing device
1303
Authenticate the micro certificate signing request
1304
Generate a response to the micro certificate signing request
1305
Verify the response to the micro certificate signing request
1306
Transmit the response to the computing device, where a micro certificate signed by the certificate authority is reconstructed based on the response

FIG. 13

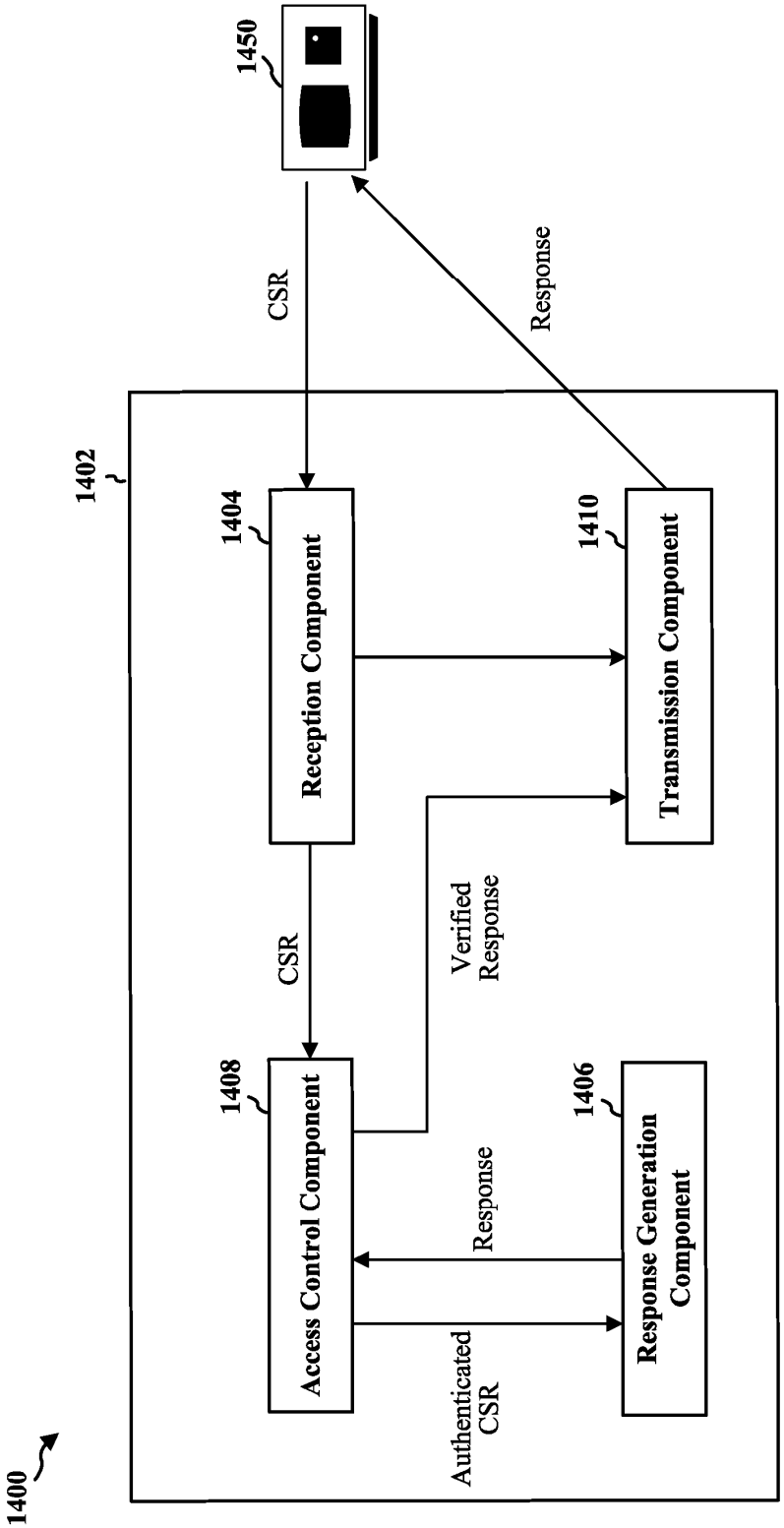
1450
CSR
Response
1402
1404
Reception Component
1410
Transmission Component
CSR
Verified Response
1408
Access Control Component
1406
Response Generation Component
Response
Authenticated CSR
1400

FIG. 14

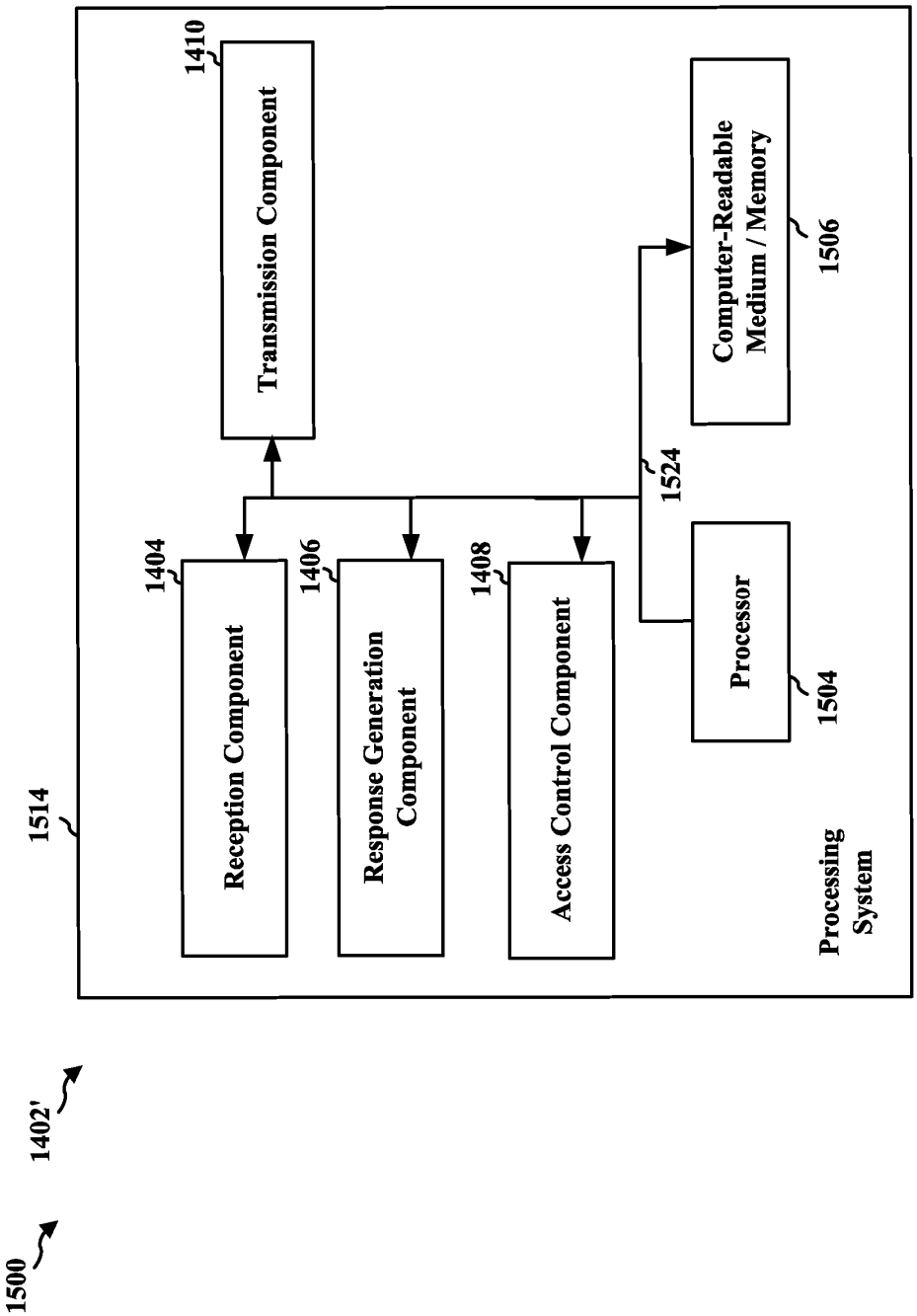
1500
1402'
1514
Processing System
Reception Component
1404
Response Generation Component
1406
Access Control Component
1408
Transmission Component
1410
Processor
1504
Computer-Readable Medium / Memory
1506
1524

FIG. 15