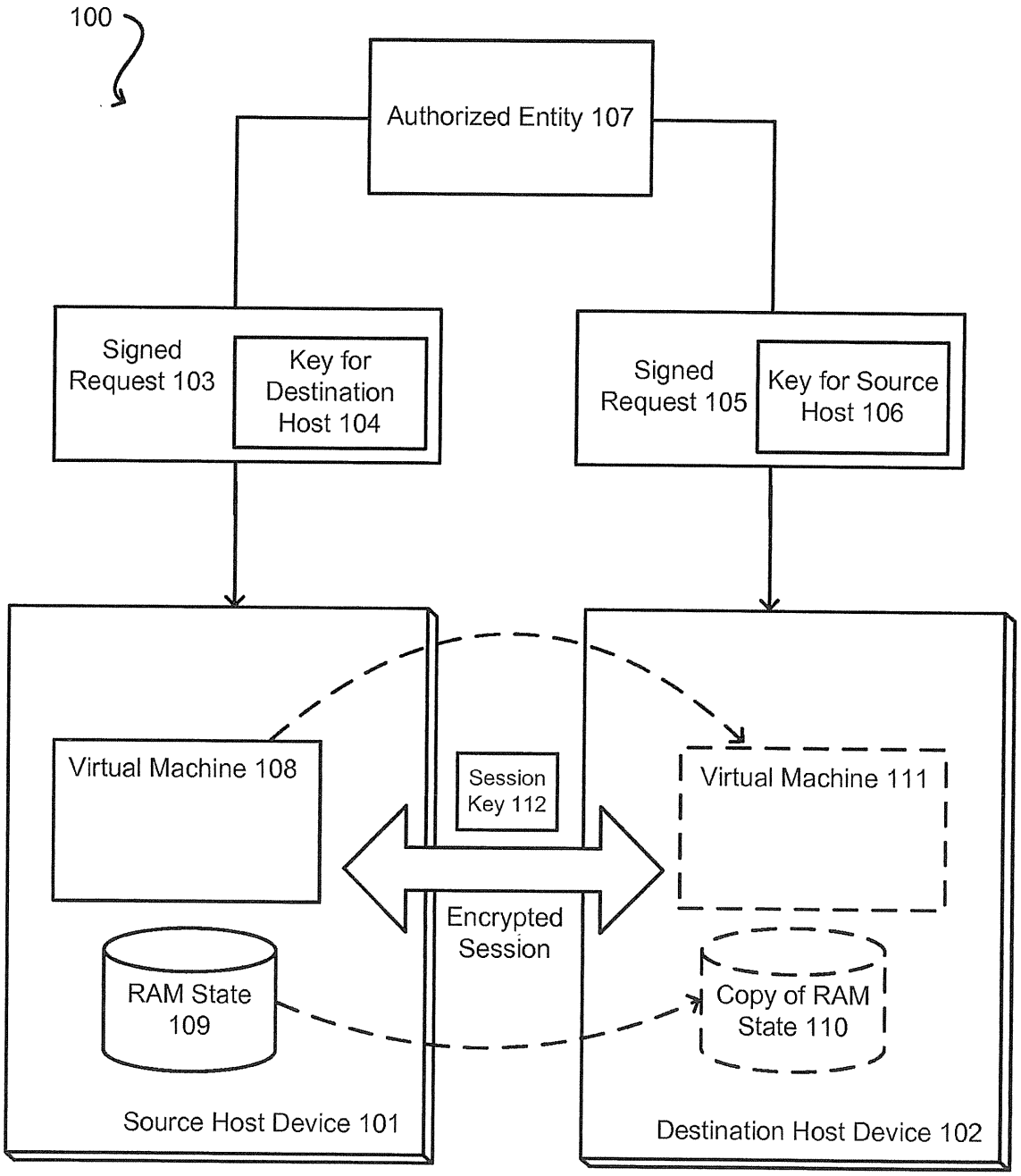
100
Authorized Entity 107
Signed Request 103
Key for Destination Host 104
Signed Request 105
Key for Source Host 106
Virtual Machine 108
Session Key 112
Virtual Machine 111
Encrypted Session
RAM State 109
Copy of RAM State 110
Source Host Device 101
Destination Host Device 102

FIGURE 1A

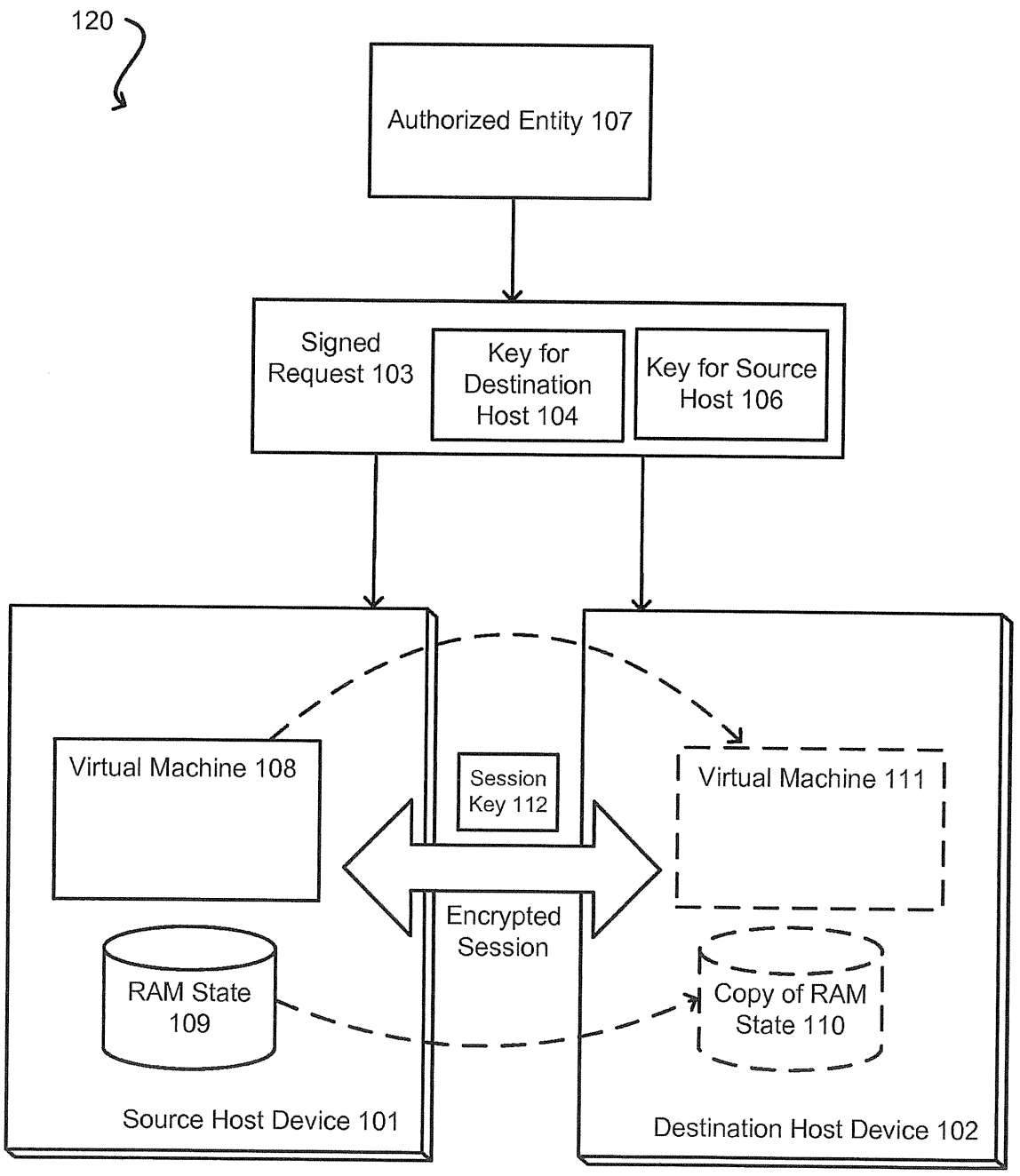
120
Authorized Entity 107
Signed Request 103
Key for Destination Host 104
Key for Source Host 106
Virtual Machine 108
Session Key 112
Virtual Machine 111
Encrypted Session
RAM State 109
Copy of RAM State 110
Source Host Device 101
Destination Host Device 102

FIGURE 1B

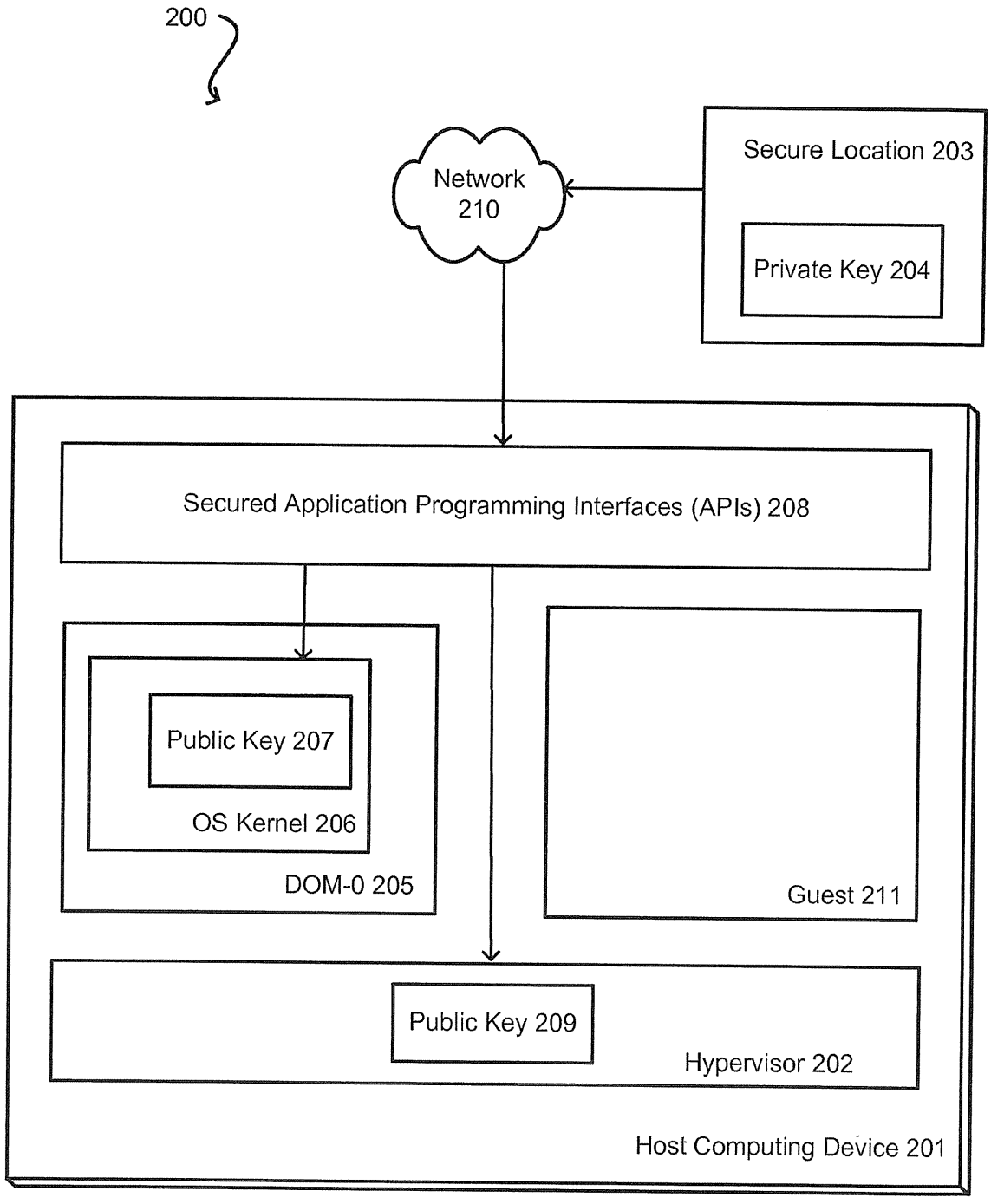
200
Network
210
Secure Location 203
Private Key 204
Secured Application Programming Interfaces (APIs) 208
Public Key 207
OS Kernel 206
DOM-0 205
Guest 211
Public Key 209
Hypervisor 202
Host Computing Device 201

FIGURE 2

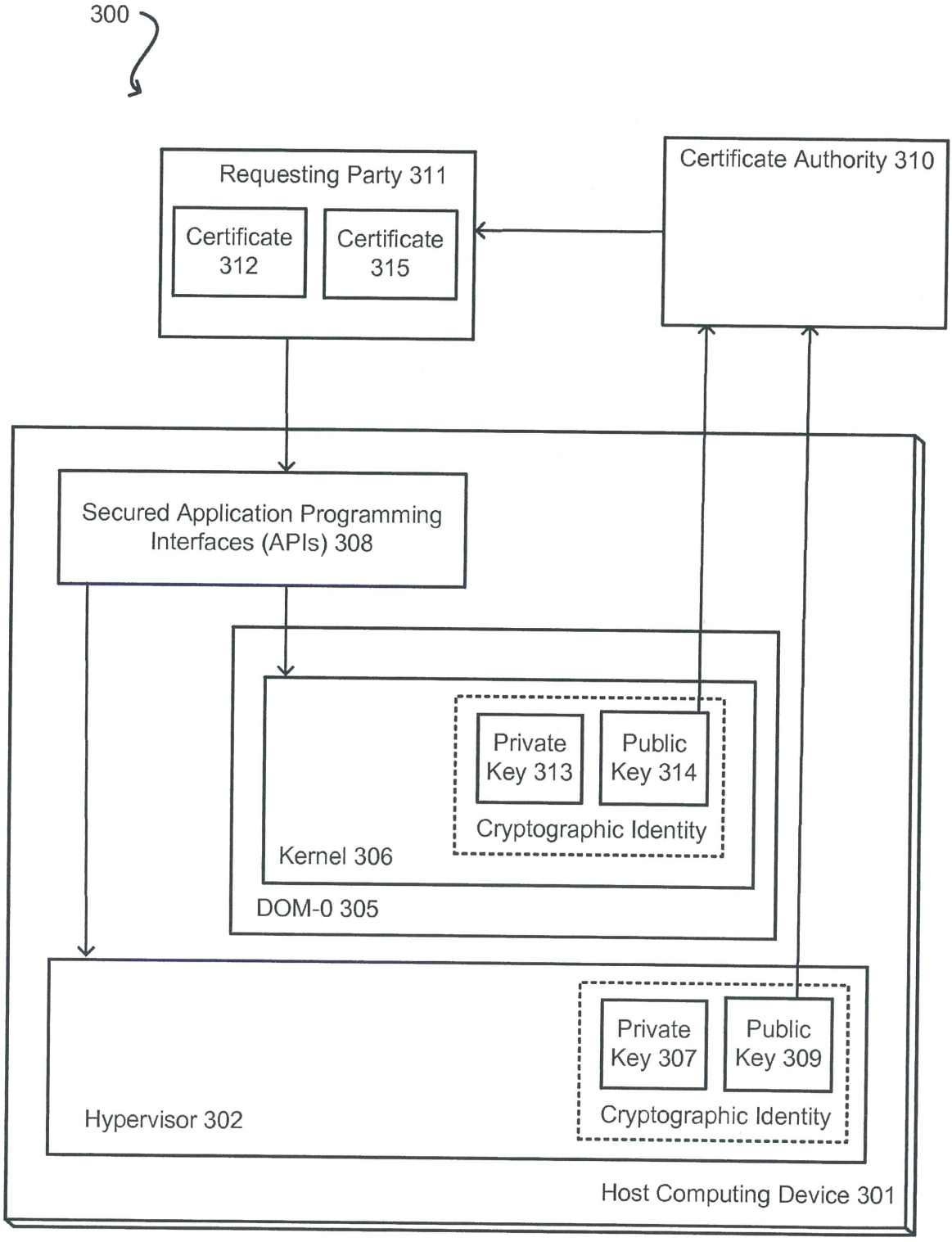
300
Requesting Party 311
Certificate 312
Certificate 315
Certificate Authority 310
Secured Application Programming Interfaces (APIs) 308
Private Key 313
Public Key 314
Cryptographic Identity
Kernel 306
DOM-0 305
Private Key 307
Public Key 309
Cryptographic Identity
Hypervisor 302
Host Computing Device 301

FIGURE 3

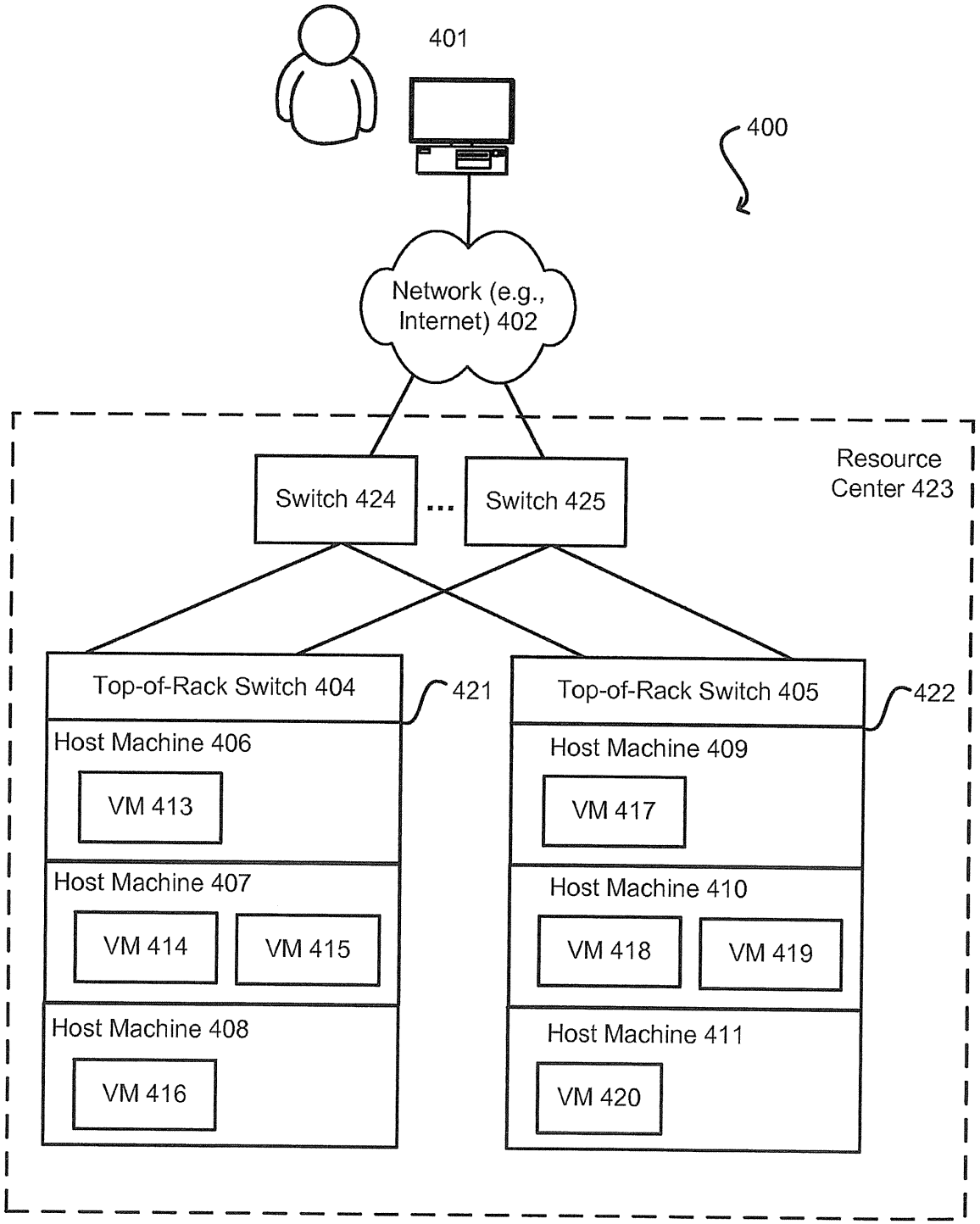
401
400
Network (e.g., Internet) 402
Switch 424
...
Switch 425
Resource Center 423
Top-of-Rack Switch 404
421
Top-of-Rack Switch 405
422
Host Machine 406
VM 413
Host Machine 407
VM 414
VM 415
Host Machine 408
VM 416
Host Machine 409
VM 417
Host Machine 410
VM 418
VM 419
Host Machine 411
VM 420

FIGURE 4

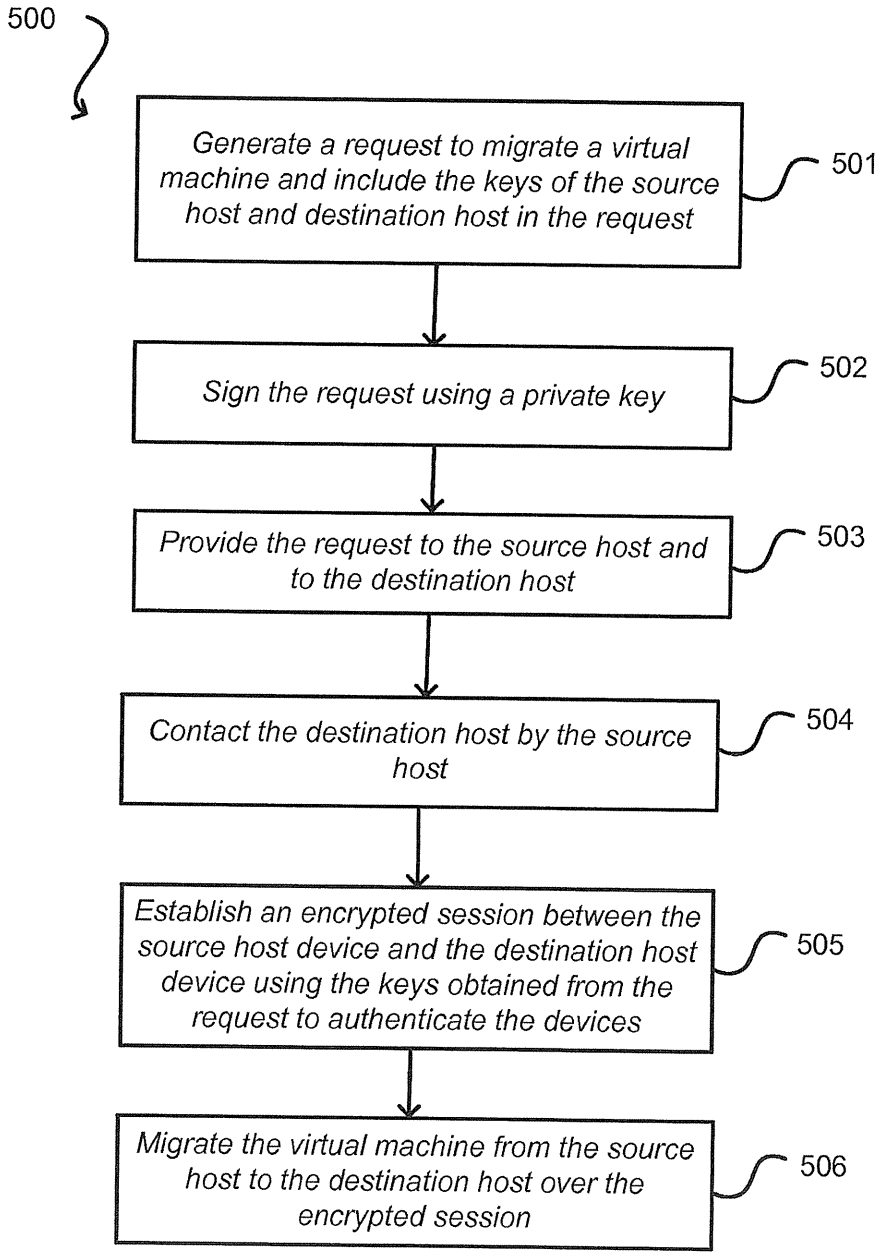
500
Generate a request to migrate a virtual machine and include the keys of the source host and destination host in the request
501
Sign the request using a private key
502
Provide the request to the source host and to the destination host
503
Contact the destination host by the source host
504
Establish an encrypted session between the source host device and the destination host device using the keys obtained from the request to authenticate the devices
505
Migrate the virtual machine from the source host to the destination host over the encrypted session
506

FIGURE 5

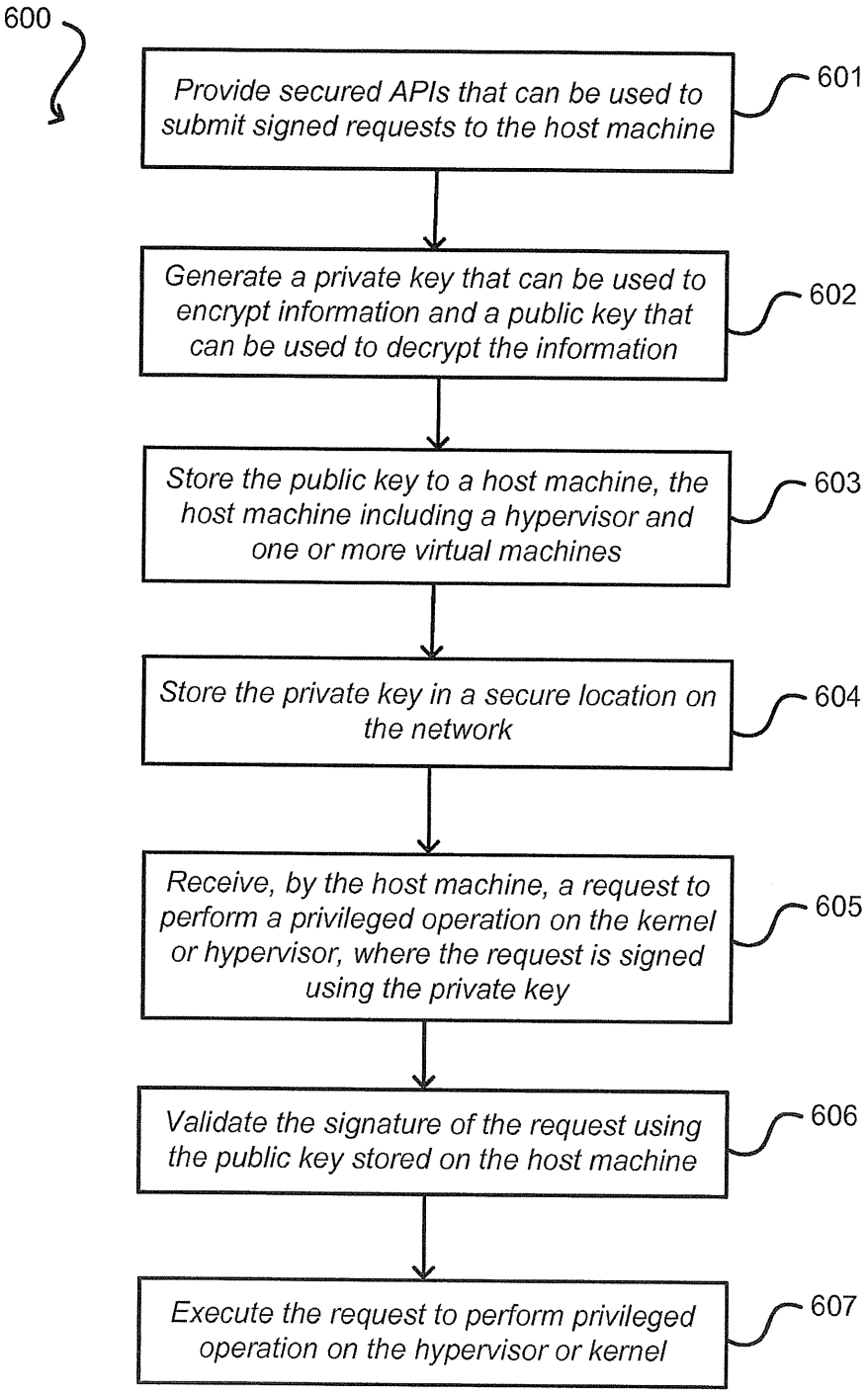
600
Provide secured APIs that can be used to submit signed requests to the host machine
601
Generate a private key that can be used to encrypt information and a public key that can be used to decrypt the information
602
Store the public key to a host machine, the host machine including a hypervisor and one or more virtual machines
603
Store the private key in a secure location on the network
604
Receive, by the host machine, a request to perform a privileged operation on the kernel or hypervisor, where the request is signed using the private key
605
Validate the signature of the request using the public key stored on the host machine
606
Execute the request to perform privileged operation on the hypervisor or kernel
607

FIGURE 6

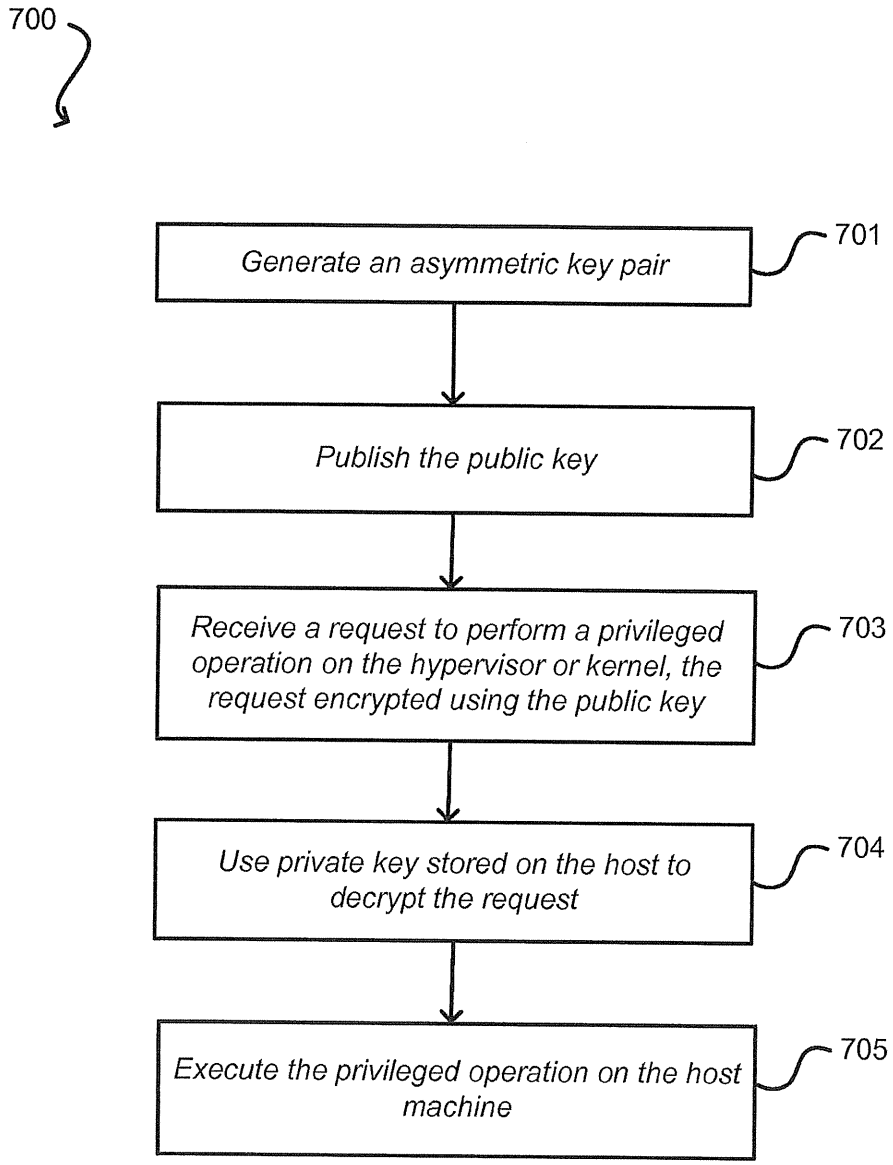
700
Generate an asymmetric key pair
701
Publish the public key
702
Receive a request to perform a privileged operation on the hypervisor or kernel, the request encrypted using the public key
703
Use private key stored on the host to decrypt the request
704
Execute the privileged operation on the host machine
705

FIGURE 7

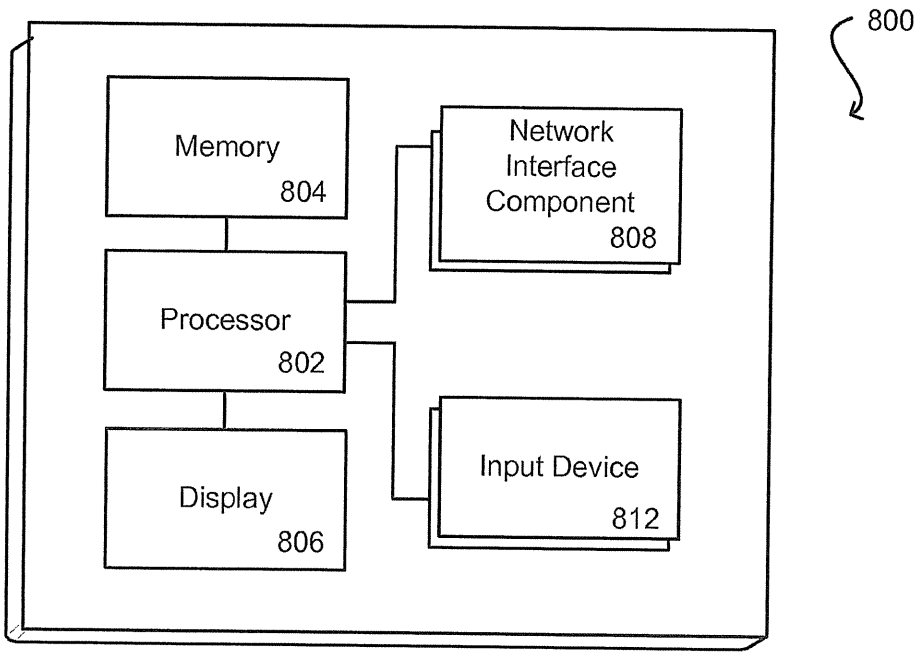
800
Memory
804
Network
Interface
Component
808
Processor
802
Input Device
812
Display
806

FIGURE 8

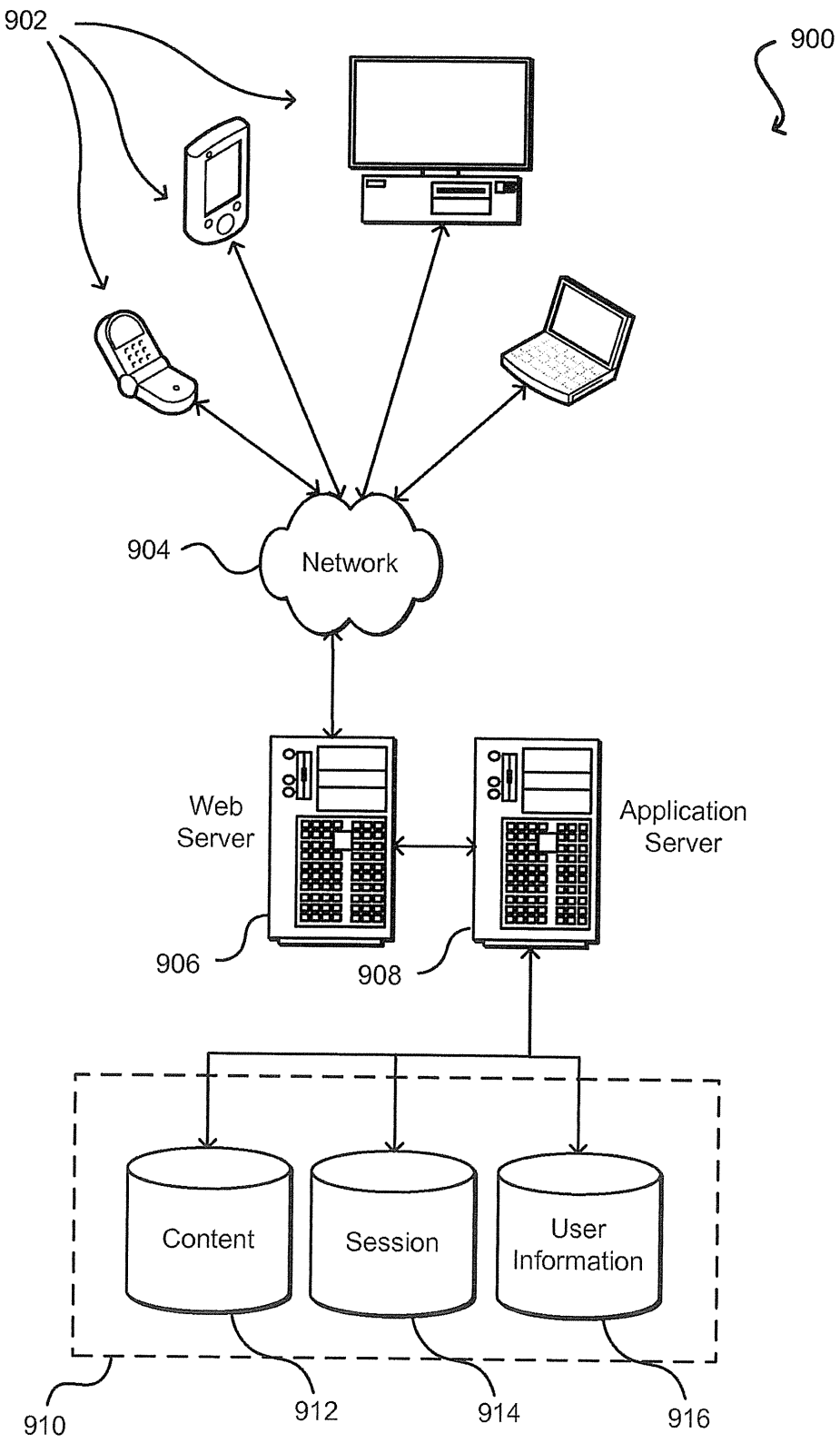
902
900
904
Network
Web
Server
Application
Server
906
908
Content
Session
User
Information
910
912
914
916

FIGURE 9