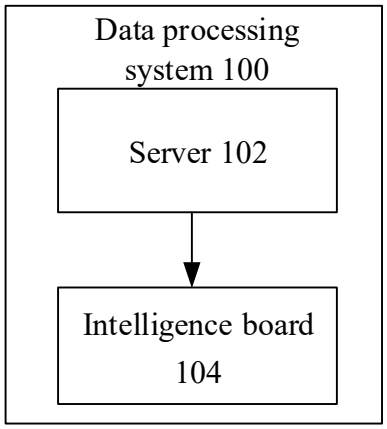

Data processing system 100
Server 102
Intelligence board 104

FIG. 1

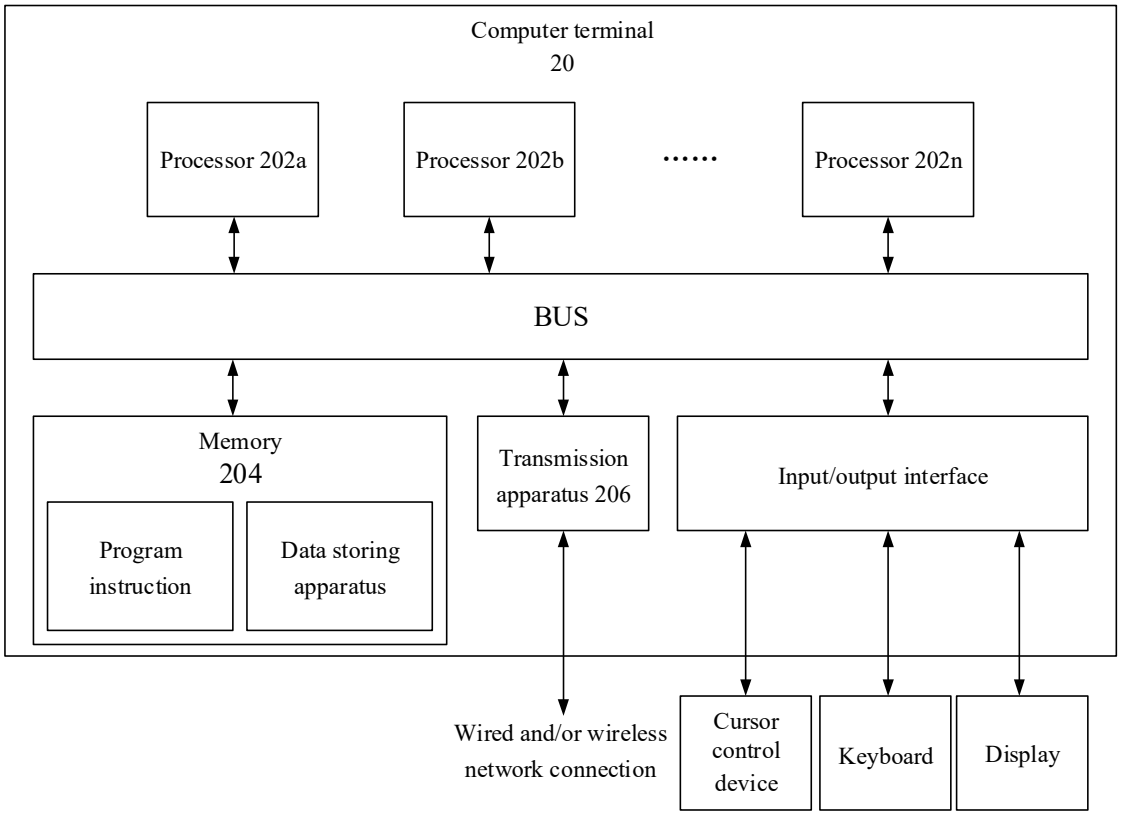

Computer terminal 20
Processor 202a
Processor 202b
.....
Processor 202n
BUS
Memory 204
Program instruction
Data storing apparatus
Transmission apparatus 206
Input/output interface
Wired and/or wireless network connection
Cursor control device
Keyboard
Display

FIG. 2

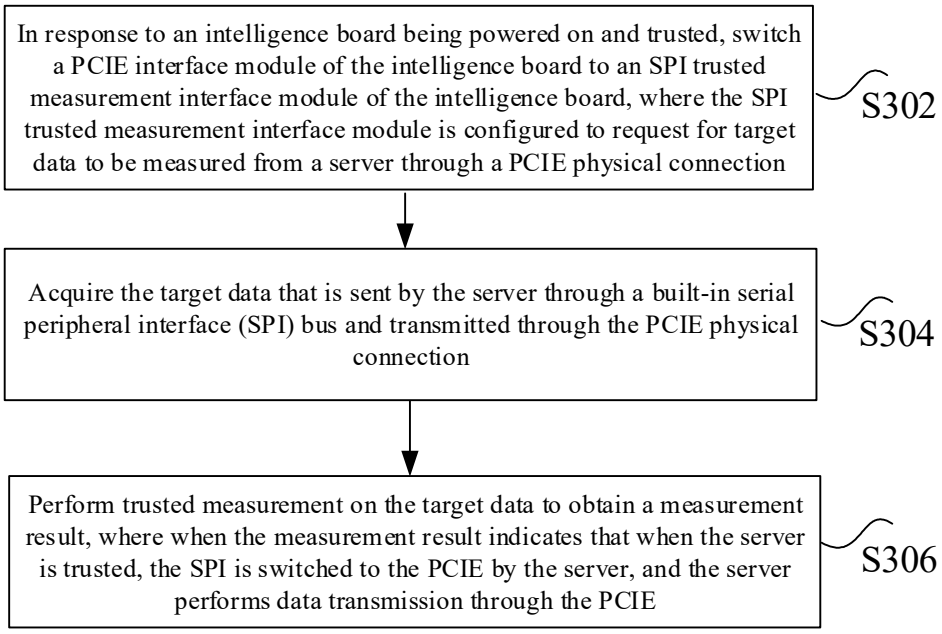

In response to an intelligence board being powered on and trusted, switch a PCIE interface module of the intelligence board to an SPI trusted measurement interface module of the intelligence board, where the SPI trusted measurement interface module is configured to request for target data to be measured from a server through a PCIE physical connection
S302
Acquire the target data that is sent by the server through a built-in serial peripheral interface (SPI) bus and transmitted through the PCIE physical connection
S304
Perform trusted measurement on the target data to obtain a measurement result, where when the measurement result indicates that when the server is trusted, the SPI is switched to the PCIE by the server, and the server performs data transmission through the PCIE
S306

FIG. 3

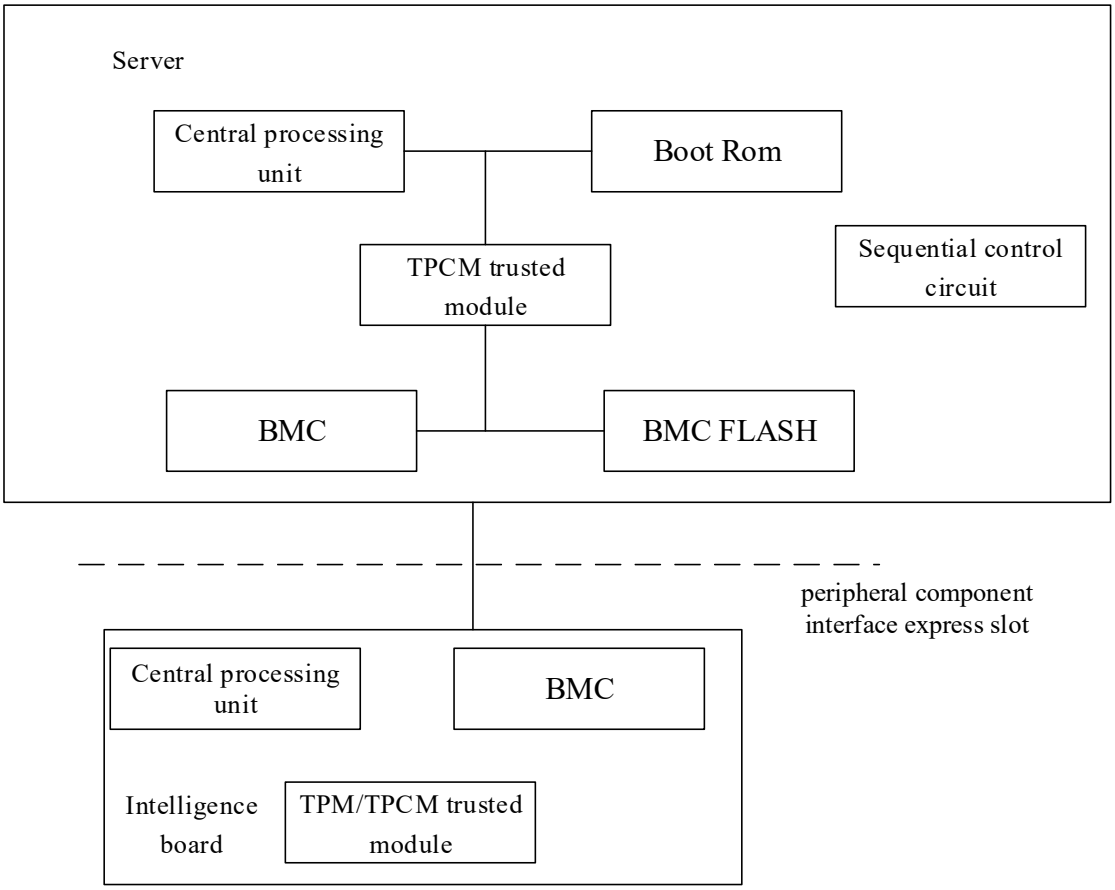

Server
Central processing unit
Boot Rom
TPCM trusted module
Sequential control circuit
BMC
BMC FLASH
peripheral component interface express slot
Central processing unit
BMC
Intelligence board
TPM/TPCM trusted module

FIG. 4

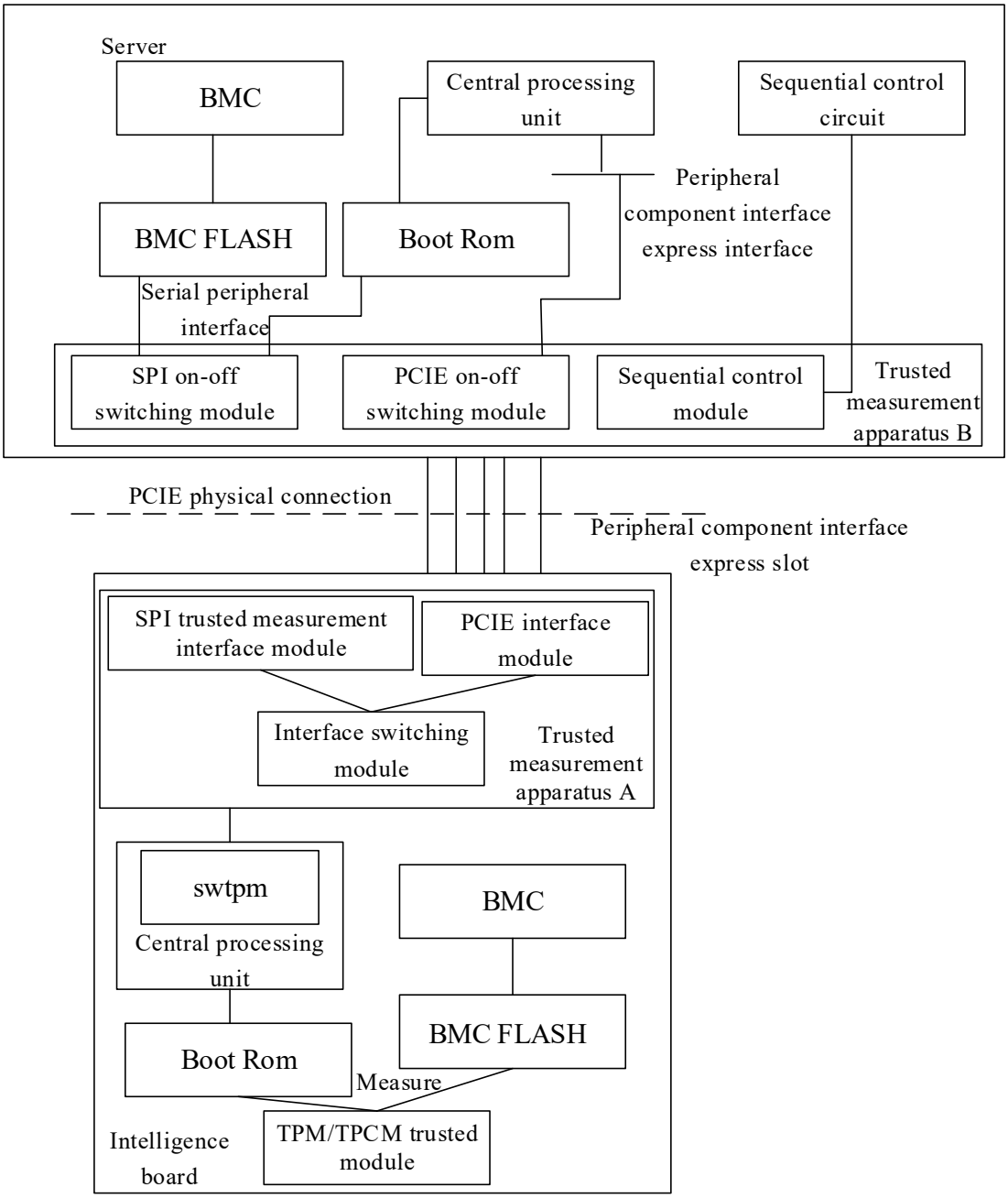

Server
BMC
Central processing unit
Sequential control circuit
Peripheral component interface express interface
BMC FLASH
Boot Rom
Serial peripheral interface
SPI on-off switching module
PCIE on-off switching module
Sequential control module
Trusted measurement apparatus B
PCIE physical connection
Peripheral component interface express slot
SPI trusted measurement interface module
PCIE interface module
Interface switching module
Trusted measurement apparatus A
swtpm
Central processing unit
BMC
BMC FLASH
Boot Rom
Measure
TPM/TPCM trusted module
Intelligence board

FIG. 5

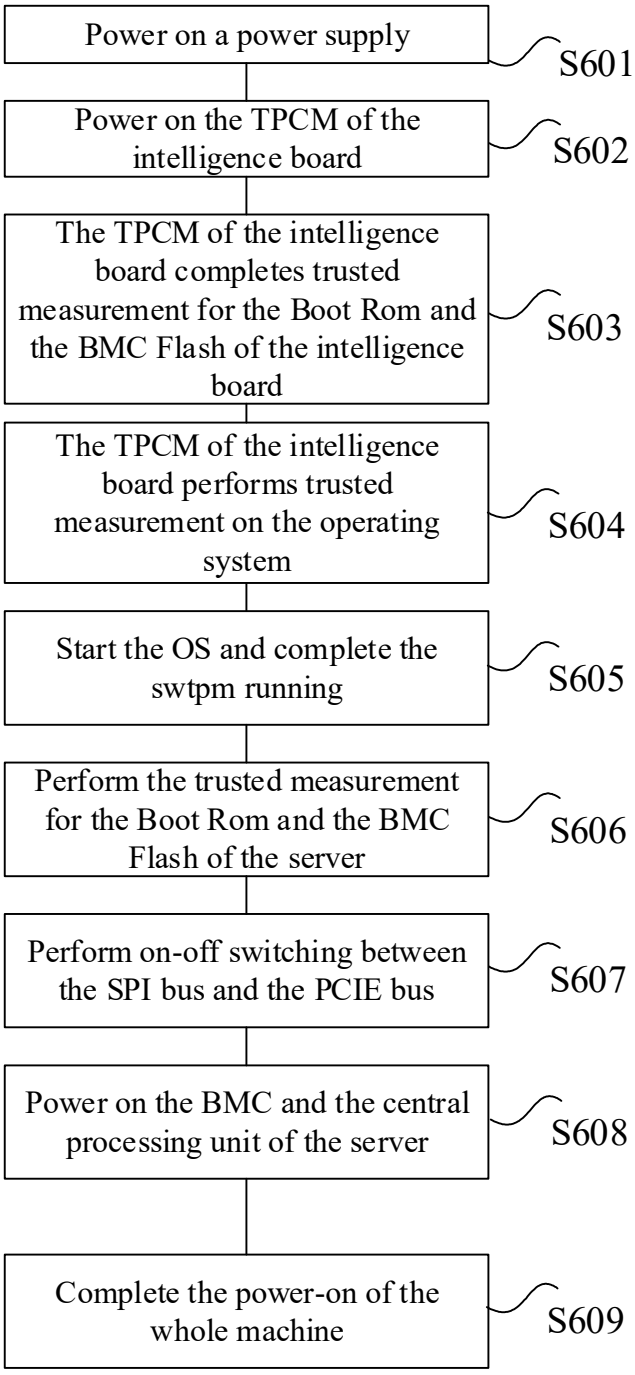

Power on a power supply
S601
Power on the TPCM of the intelligence board
S602
The TPCM of the intelligence board completes trusted measurement for the Boot Rom and the BMC Flash of the intelligence board
S603
The TPCM of the intelligence board performs trusted measurement on the operating system
S604
Start the OS and complete the swtpm running
S605
Perform the trusted measurement for the Boot Rom and the BMC Flash of the server
S606
Perform on-off switching between the SPI bus and the PCIE bus
S607
Power on the BMC and the central processing unit of the server
S608
Complete the power-on of the whole machine
S609

FIG. 6

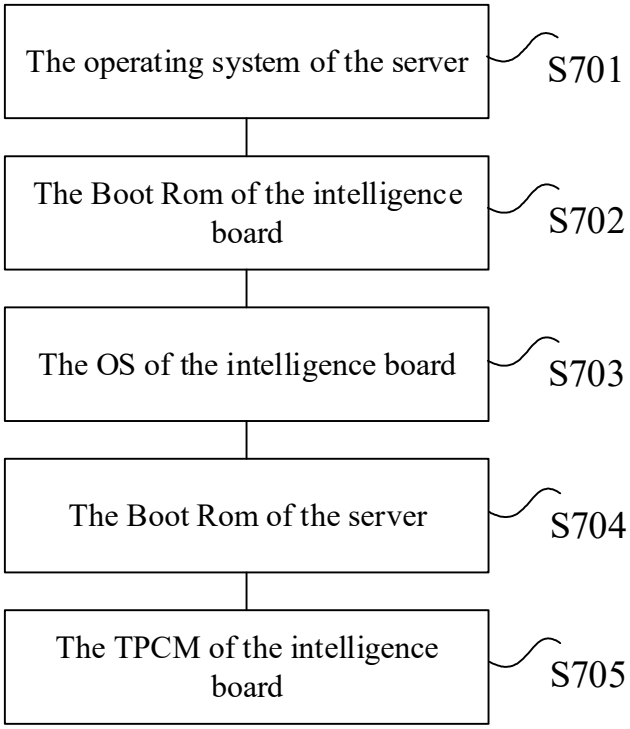

The operating system of the server
S701
The Boot Rom of the intelligence board
S702
The OS of the intelligence board
S703
The Boot Rom of the server
S704
The TPCM of the intelligence board
S705

FIG. 7

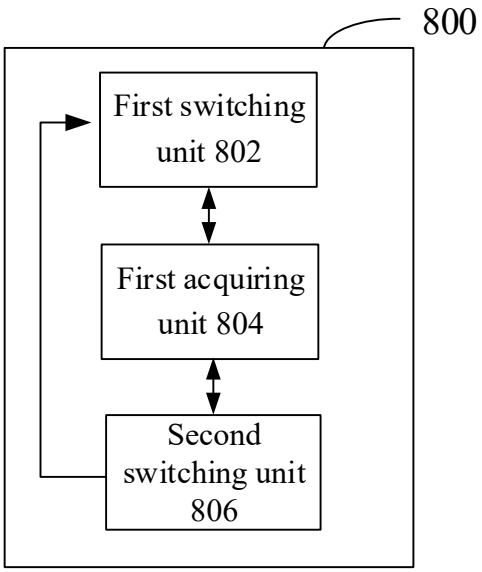

800
First switching unit 802
First acquiring unit 804
Second switching unit 806

FIG. 8

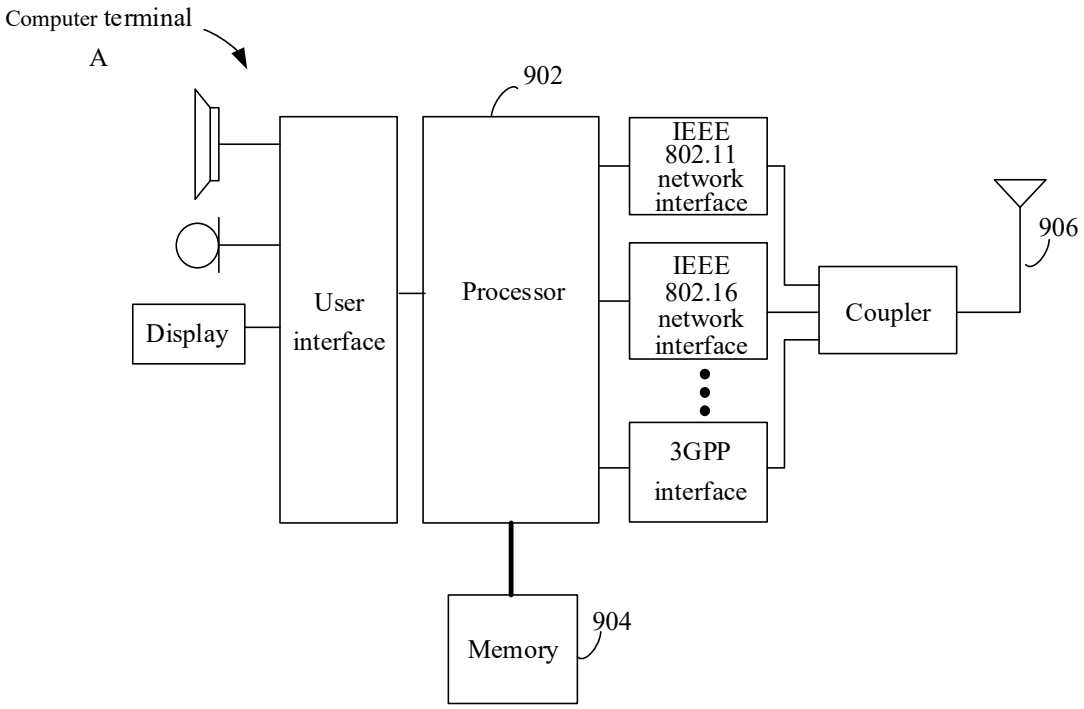

Computer terminal
A
902
IEEE
802.11
network
interface
906
IEEE
802.16
network
interface
Coupler
Processor
User
interface
Display
3GPP
interface
Memory
904

FIG. 9