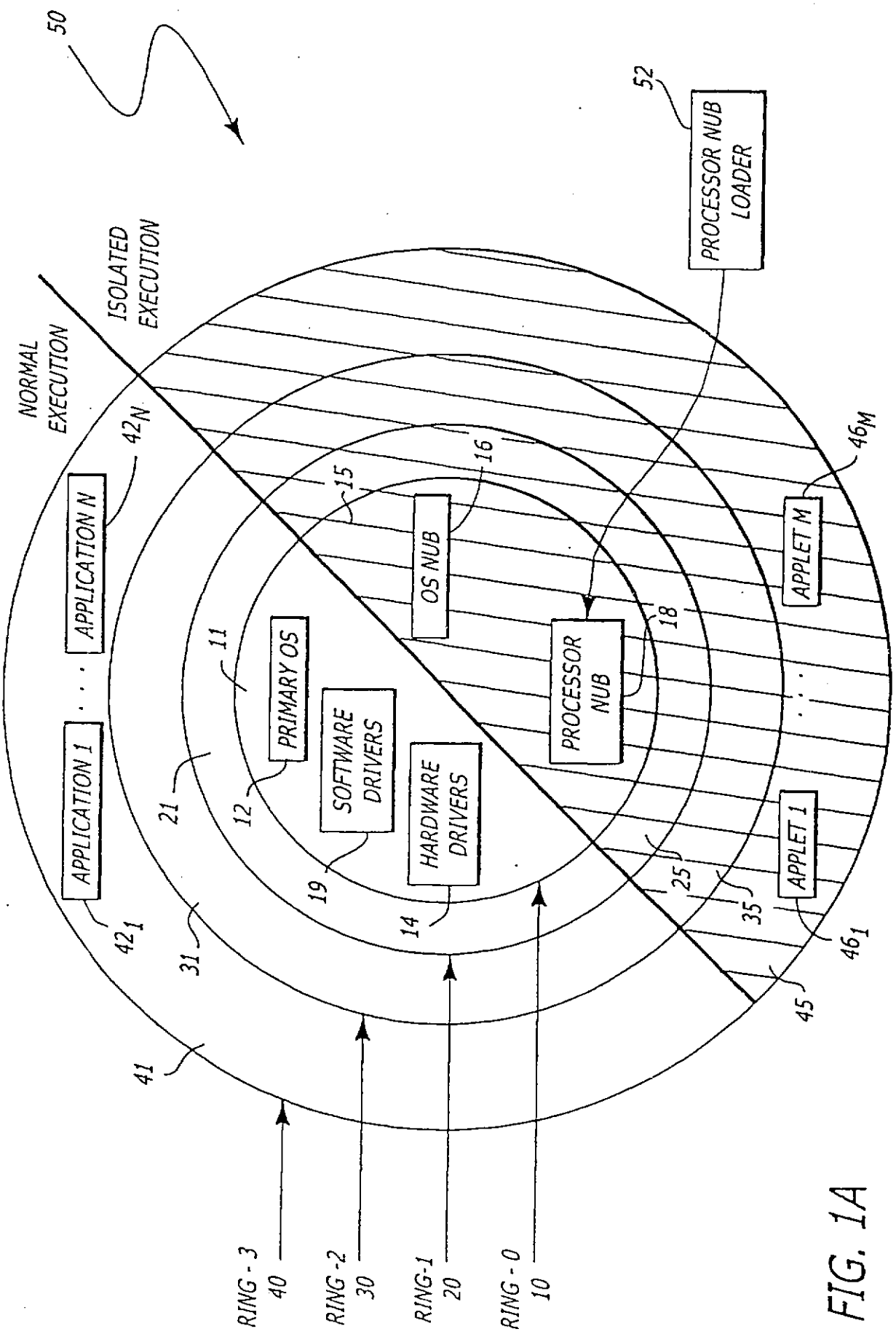

50
52
PROCESSOR NUB LOADER
NORMAL EXECUTION
ISOLATED EXECUTION
APPLICATION N
APPLICATION 1
42N
421
OS NUB
PROCESSOR NUB
APPLET M
APPLET 1
46M
461
PRIMARY OS
SOFTWARE DRIVERS
HARDWARE DRIVERS
15
16
18
11
12
21
19
14
25
35
45
31
41
RING - 3 40
RING -2 30
RING-1 20
RING - 0 10

FIG. 1A

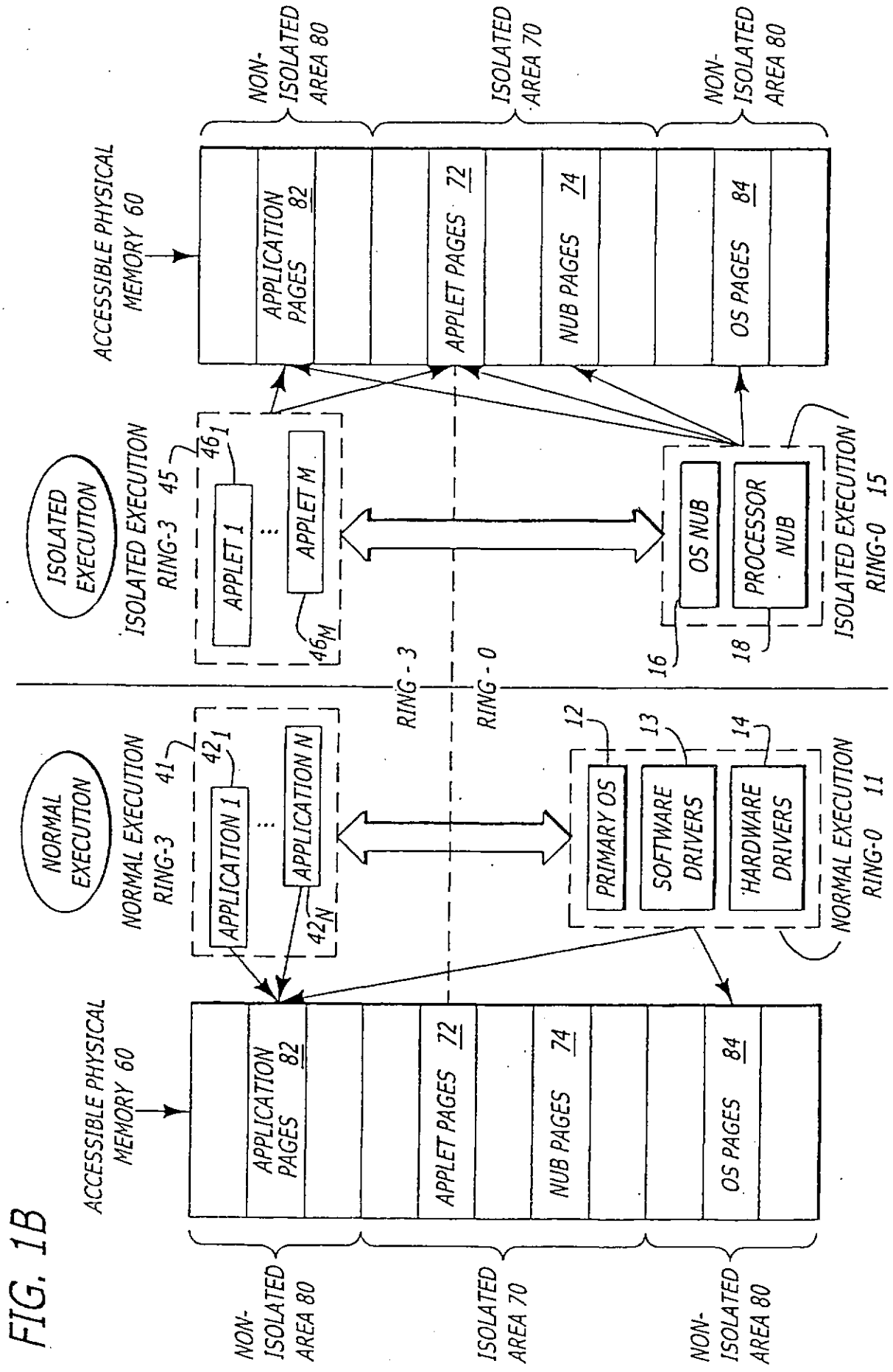
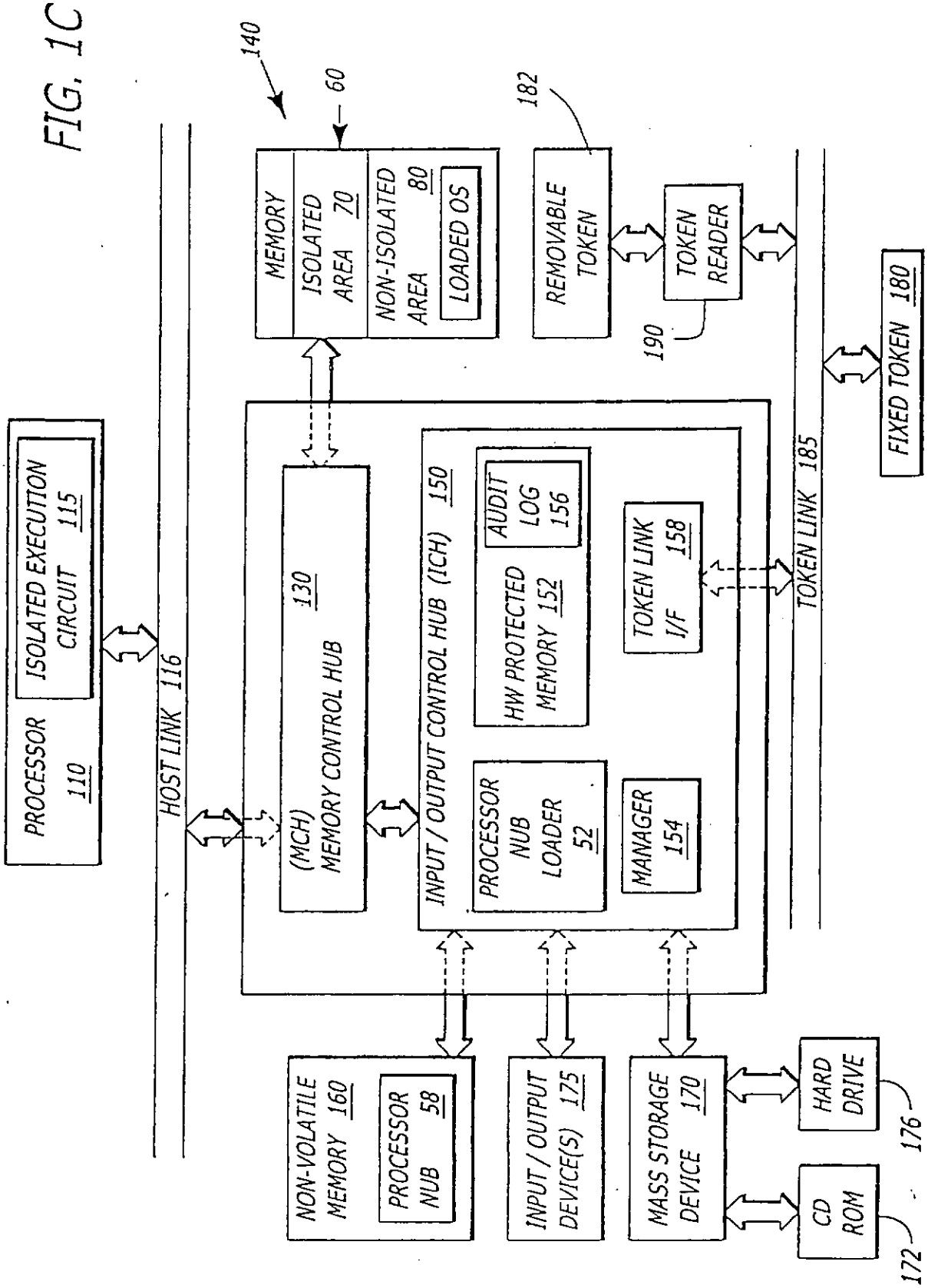

ACCESSIBLE PHYSICAL MEMORY 60
NON-ISOLATED AREA 80
ISOLATED AREA 70
NON-ISOLATED AREA 80
APPLICATION PAGES 82
APPLET PAGES 72
NUB PAGES 74
OS PAGES 84
ISOLATED EXECUTION
ISOLATED EXECUTION RING-3 45
APPLET 1 46 1
APPLET M 46 M
OS NUB 16
PROCESSOR NUB 18
ISOLATED EXECUTION RING-0 15
RING - 3
RING - 0
NORMAL EXECUTION
NORMAL EXECUTION RING-3 41
APPLICATION 1 42 1
APPLICATION N 42 N
PRIMARY OS 12
SOFTWARE DRIVERS 13
HARDWARE DRIVERS 14
NORMAL EXECUTION RING-0 11
ACCESSIBLE PHYSICAL MEMORY 60
APPLICATION PAGES 82
APPLET PAGES 72
NUB PAGES 74
OS PAGES 84
NON-ISOLATED AREA 80
ISOLATED AREA 70
NON-ISOLATED AREA 80

FIG. 1B

FIG. 1C


140
60
182
MEMORY
ISOLATED AREA 70
NON-ISOLATED AREA 80
LOADED OS
REMOVABLE TOKEN
TOKEN READER
190
PROCESSOR 110
ISOLATED EXECUTION CIRCUIT 115
HOST LINK 116
(MCH) MEMORY CONTROL HUB 130
INPUT / OUTPUT CONTROL HUB (ICH) 150
HW PROTECTED MEMORY 152
AUDIT LOG 156
TOKEN LINK I/F 158
PROCESSOR NUB LOADER 52
MANAGER 154
TOKEN LINK 185
FIXED TOKEN 180
NON-VOLATILE MEMORY 160
PROCESSOR NUB 58
INPUT / OUTPUT DEVICE(S) 175
MASS STORAGE DEVICE 170
HARD DRIVE
176
CD ROM
172

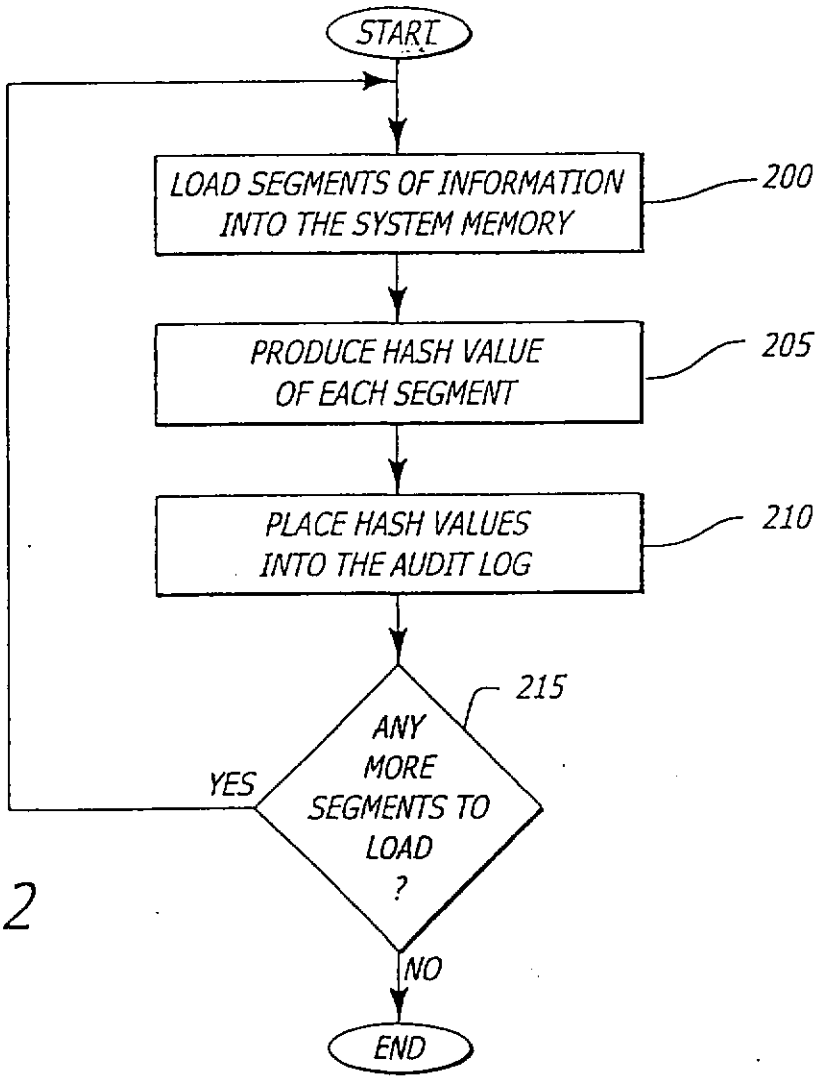

START
LOAD SEGMENTS OF INFORMATION INTO THE SYSTEM MEMORY
200
PRODUCE HASH VALUE OF EACH SEGMENT
205
PLACE HASH VALUES INTO THE AUDIT LOG
210
ANY MORE SEGMENTS TO LOAD ?
215
YES
NO
END

FIG. 2

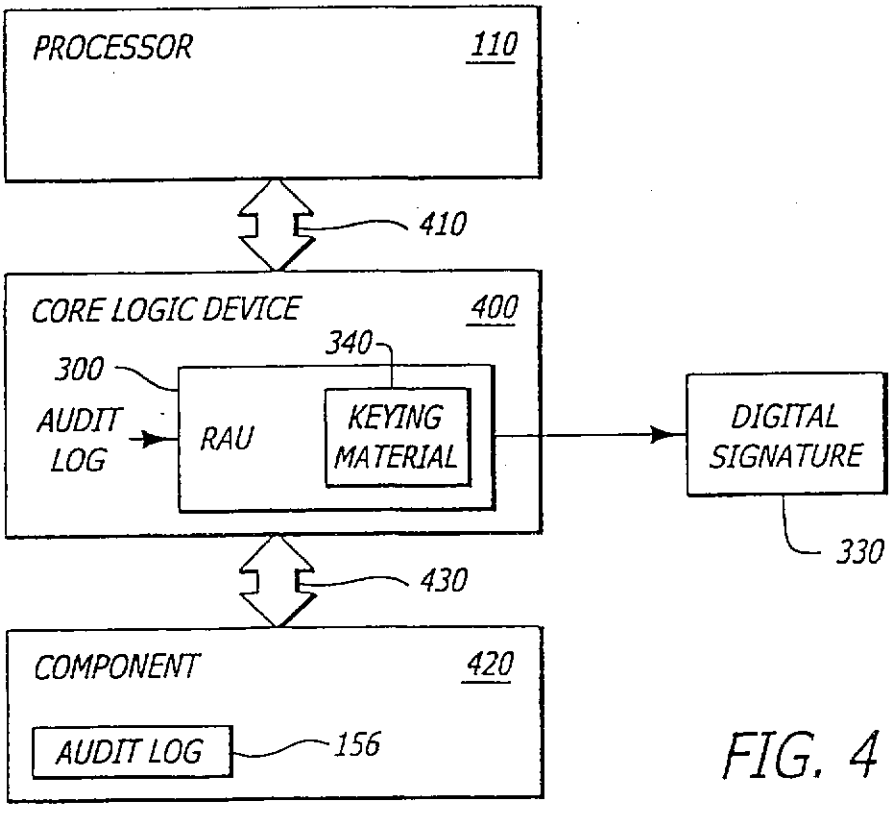
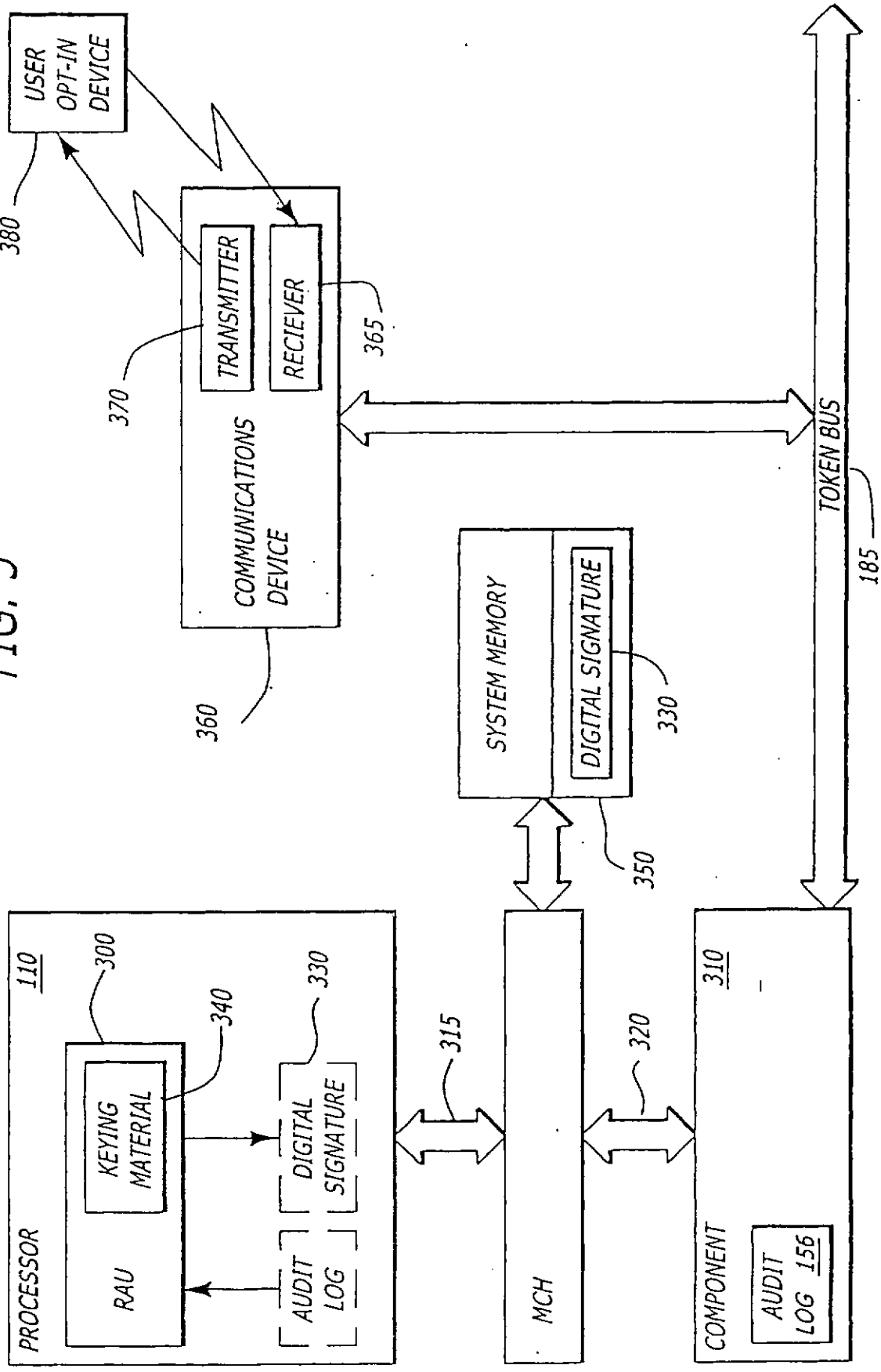

PROCESSOR
110
410
CORE LOGIC DEVICE
400
340
300
AUDIT LOG
RAU
KEYING MATERIAL
DIGITAL SIGNATURE
330
430
COMPONENT
420
AUDIT LOG
156

FIG. 4

FIG. 3


USER OPT-IN DEVICE
380
TRANSMITTER
RECIEVER
365
370
COMMUNICATIONS DEVICE
360
TOKEN BUS
185
SYSTEM MEMORY
DIGITAL SIGNATURE
330
350
PROCESSOR
110
300
340
330
KEYING MATERIAL
RAU
DIGITAL SIGNATURE
AUDIT LOG
315
MCH
320
310
COMPONENT
AUDIT LOG 156

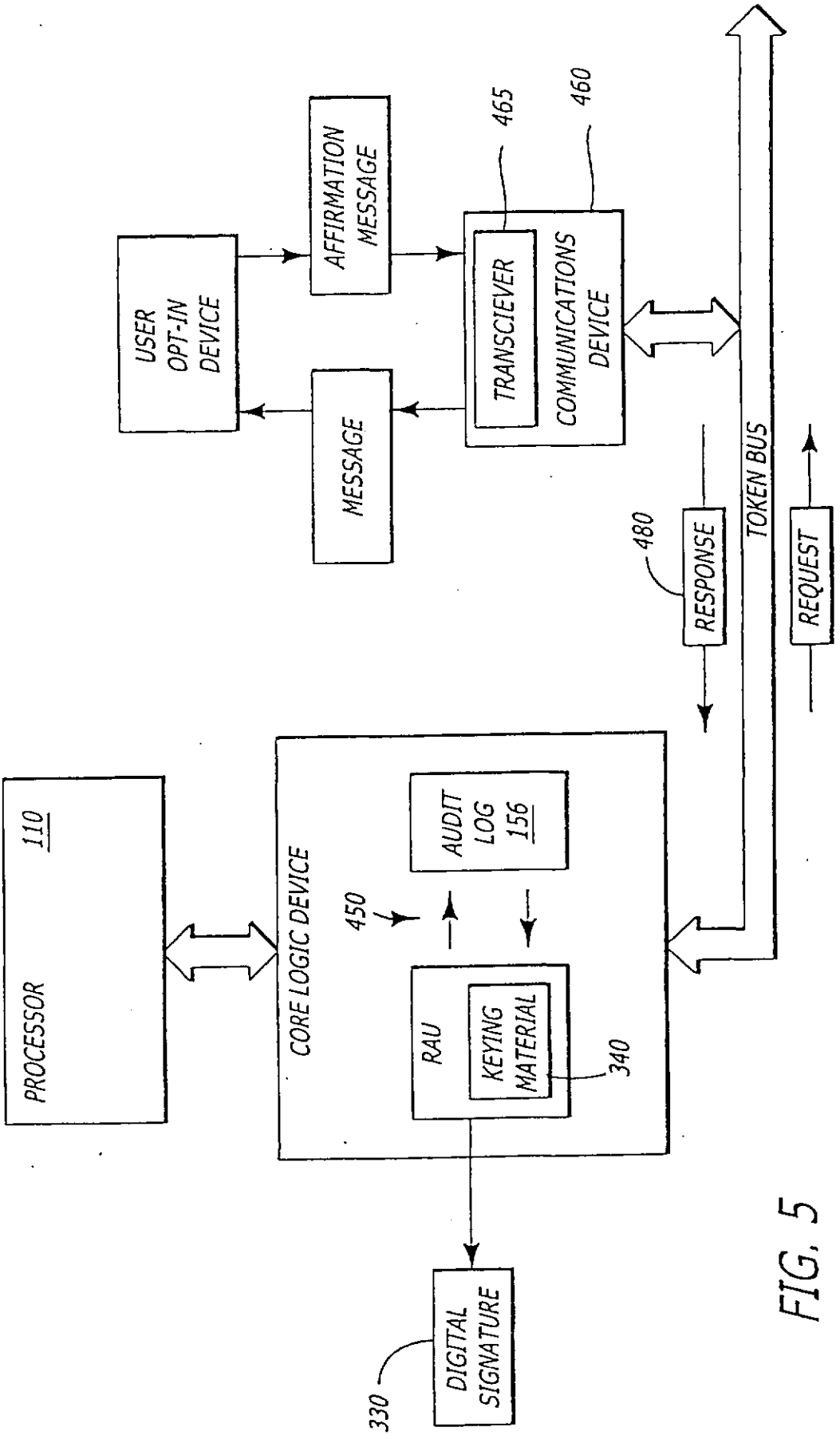

PROCESSOR
110
CORE LOGIC DEVICE
AUDIT LOG 156
450
RAU
KEYING MATERIAL
340
DIGITAL SIGNATURE
330
TOKEN BUS
REQUEST
480
RESPONSE
MESSAGE
AFFIRMATION MESSAGE
USER OPT-IN DEVICE
TRANSCIEVER
465
COMMUNICATIONS DEVICE
460

FIG. 5

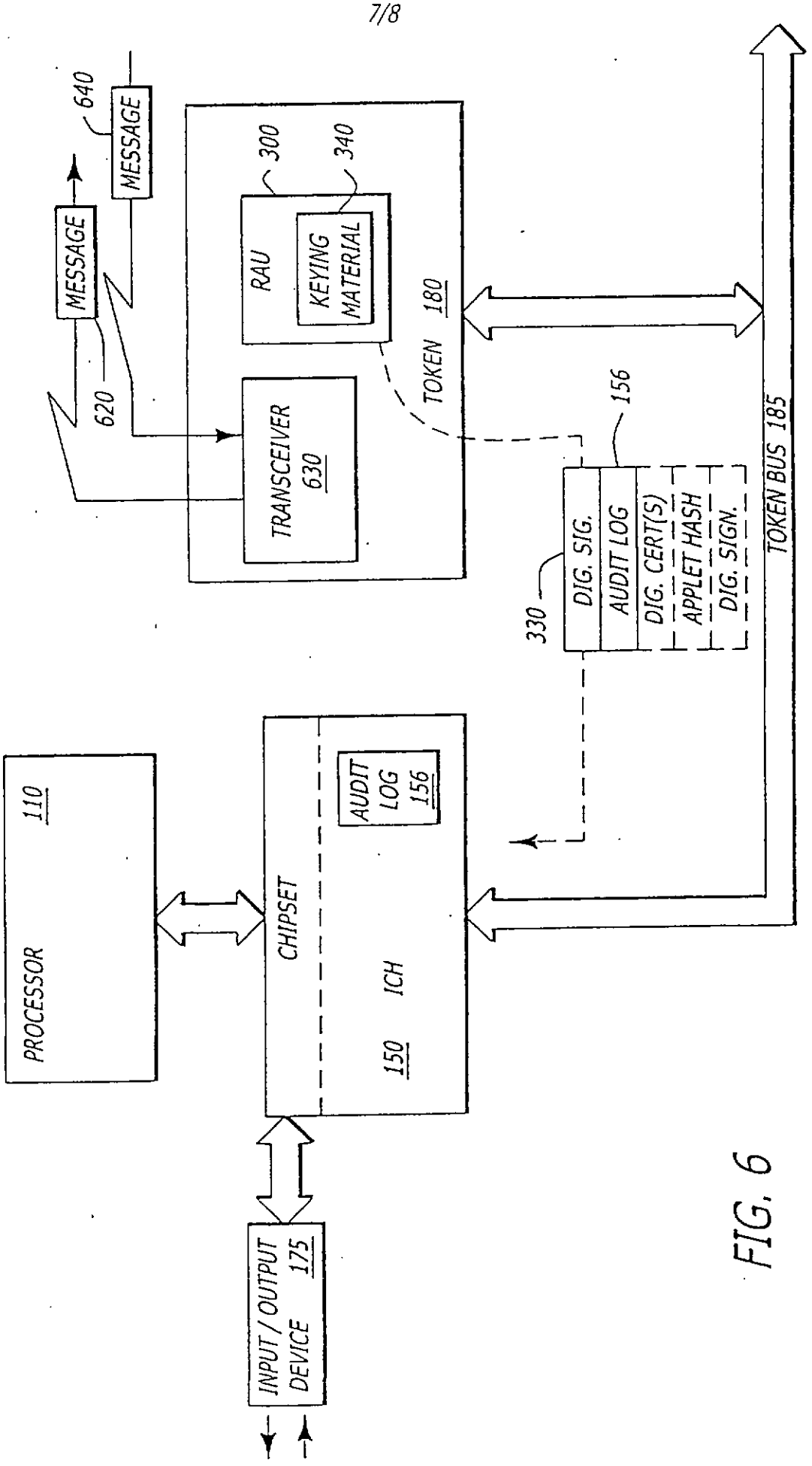

640
MESSAGE
MESSAGE
620
300
340
RAU
KEYING MATERIAL
TOKEN 180
TRANSCEIVER 630
156
330
DIG. SIG.
AUDIT LOG
DIG. CERT(S)
APPLET HASH
DIG. SIGN.
TOKEN BUS 185
PROCESSOR 110
CHIPSET
AUDIT LOG 156
ICH 150
INPUT / OUTPUT DEVICE 175

FIG. 6

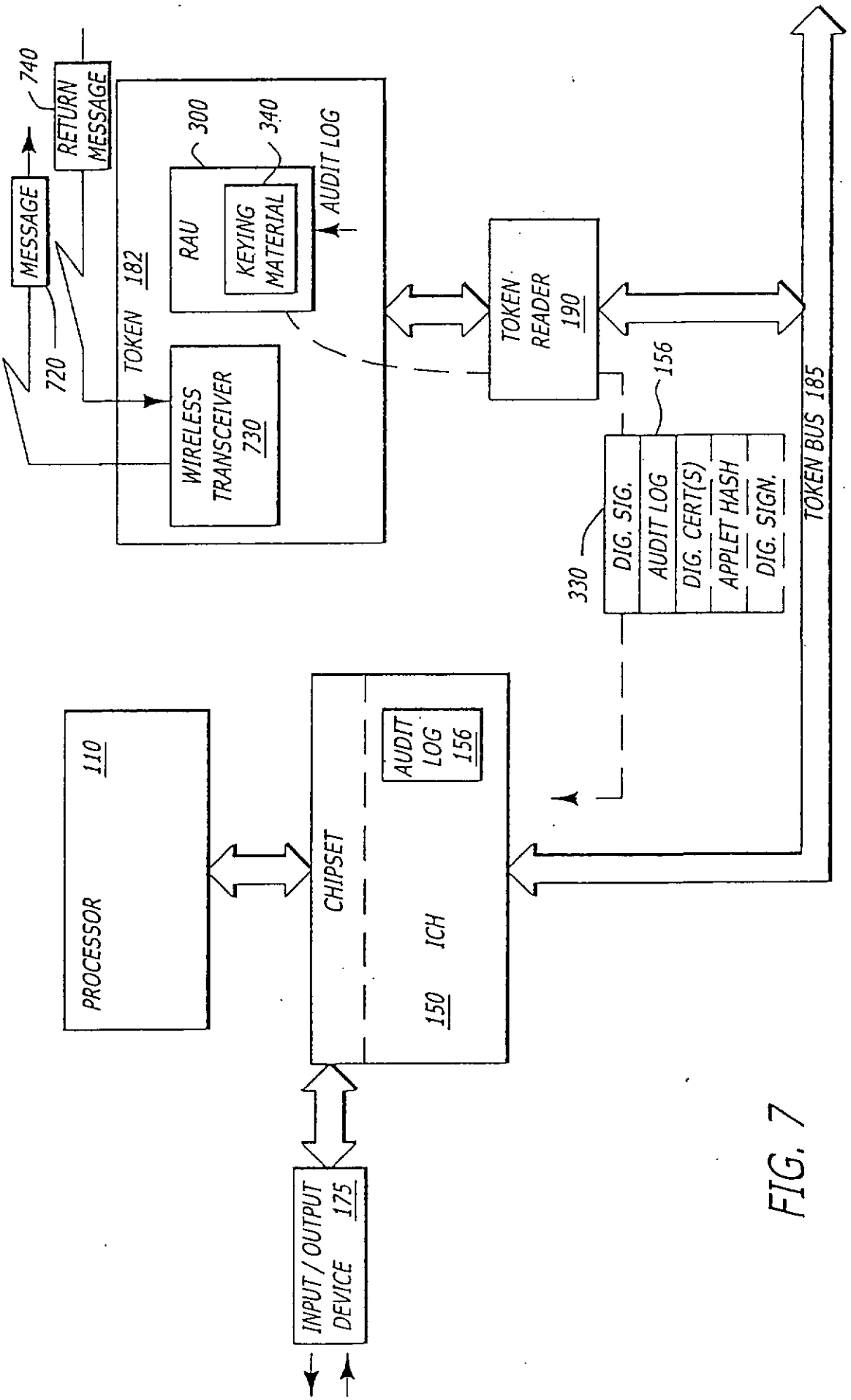

740
RETURN MESSAGE
MESSAGE
720
TOKEN 182
300
RAU
340
KEYING MATERIAL
AUDIT LOG
WIRELESS TRANSCEIVER 730
TOKEN READER 190
156
330
DIG. SIG.
AUDIT LOG
DIG. CERT(S)
APPLET HASH
DIG. SIGN.
TOKEN BUS 185
PROCESSOR 110
CHIPSET
AUDIT LOG 156
ICH
150
INPUT / OUTPUT DEVICE 175

FIG. 7