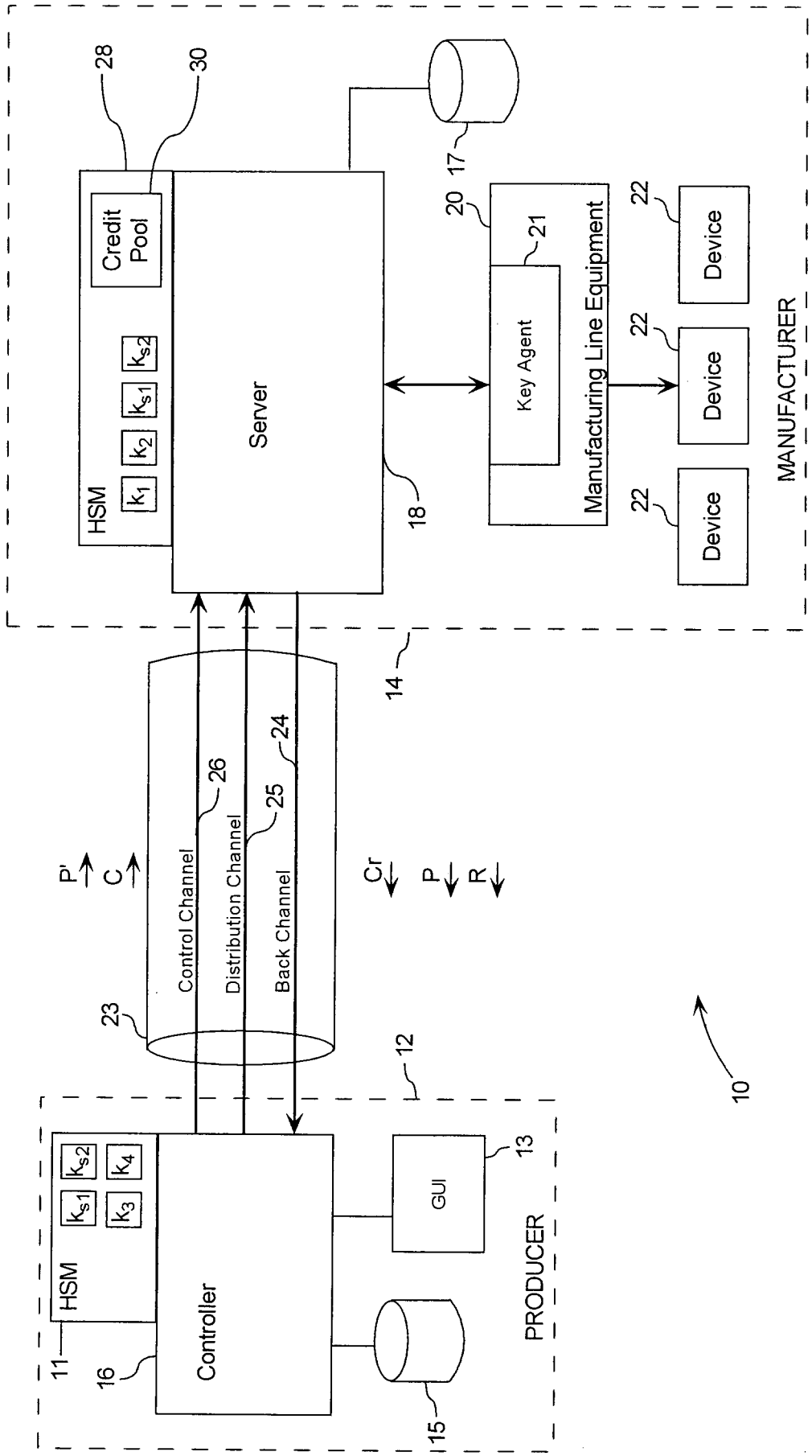

MANUFACTURER
14
HSM
k_1
k_2
k_{s1}
k_{s2}
Credit Pool
28
30
Server
18
17
20
Key Agent
21
Manufacturing Line Equipment
22
Device
Device
Device
Control Channel
Distribution Channel
Back Channel
26
25
24
23
12
P'
C
Cr
P
R
PRODUCER
HSM
k_{s1}
k_{s2}
k_3
k_4
11
16
Controller
GUI
13
15
10

FIG. 1

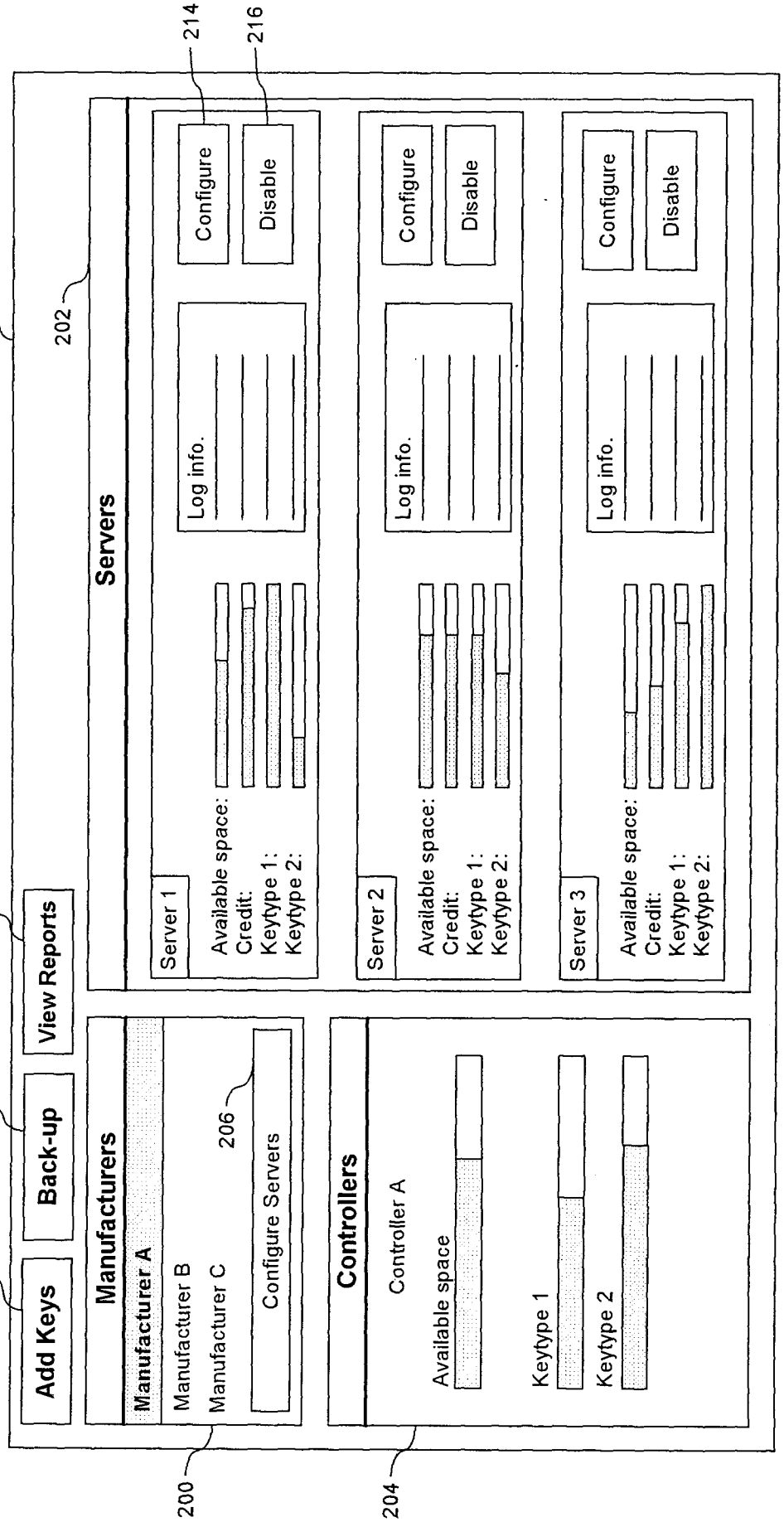

13
Add Keys
218
Back-up
220
View Reports
222
Manufacturers
Manufacturer A
Manufacturer B
Manufacturer C
206
Configure Servers
200
Controllers
Controller A
Available space
Keytype 1
Keytype 2
204
Servers
202
Server 1
Available space:
Credit:
Keytype 1:
Keytype 2:
Log info.
Configure
214
Disable
216
Server 2
Available space:
Credit:
Keytype 1:
Keytype 2:
Log info.
Configure
Disable
Server 3
Available space:
Credit:
Keytype 1:
Keytype 2:
Log info.
Configure
Disable

FIG. 2

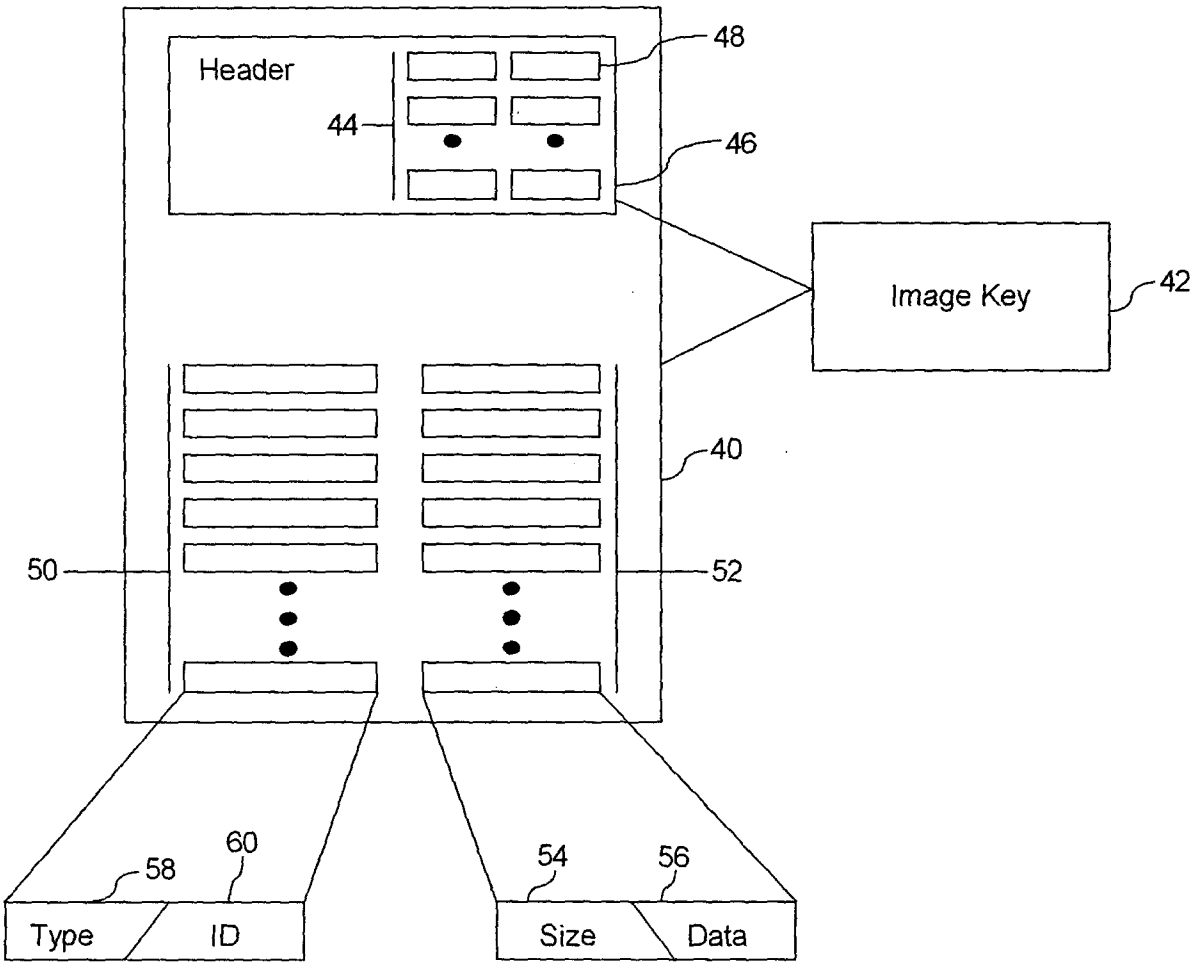

Header
48
44
46
Image Key
42
40
50
52
60
58
54
56
Type
ID
Size
Data

FIG. 3

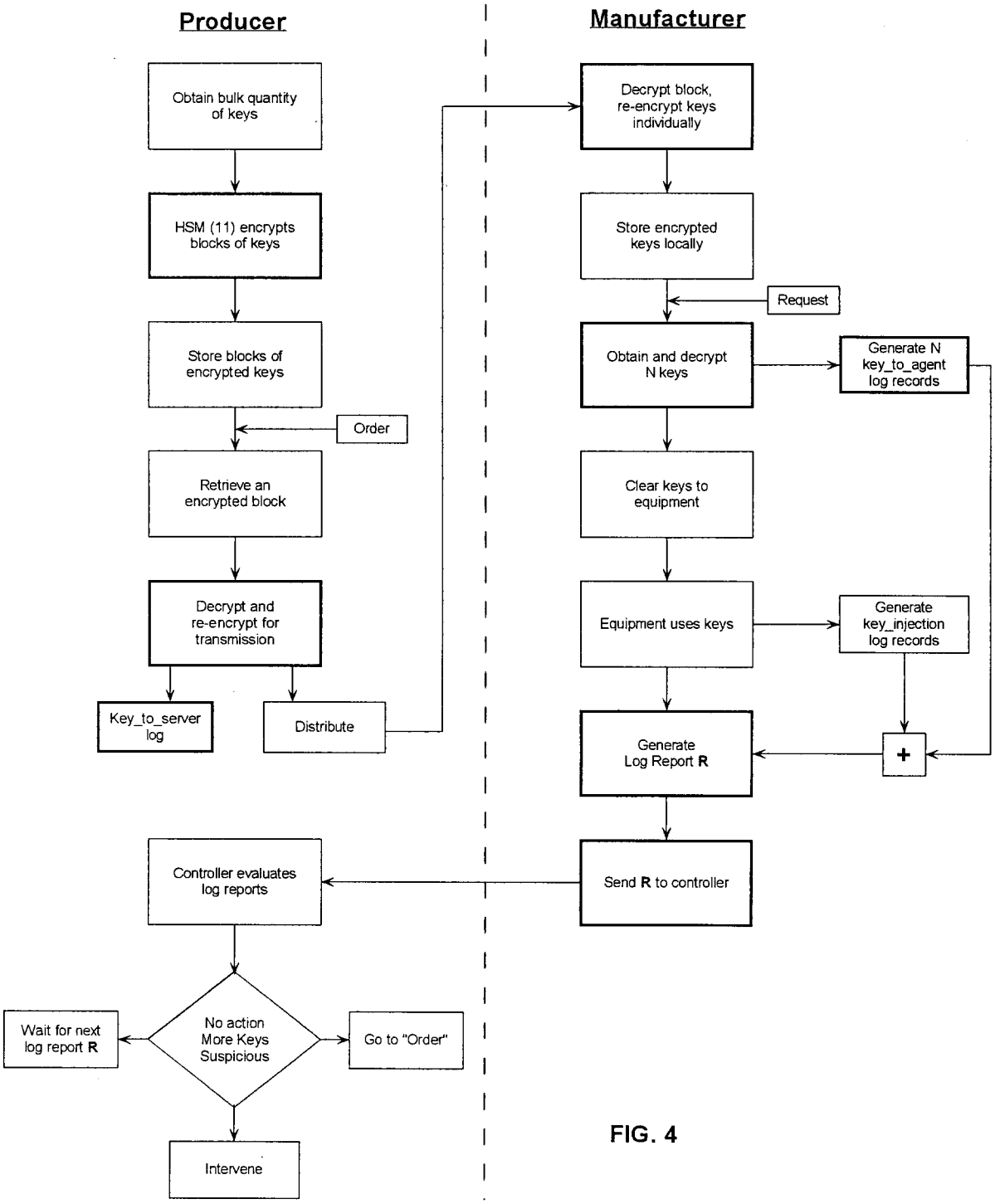
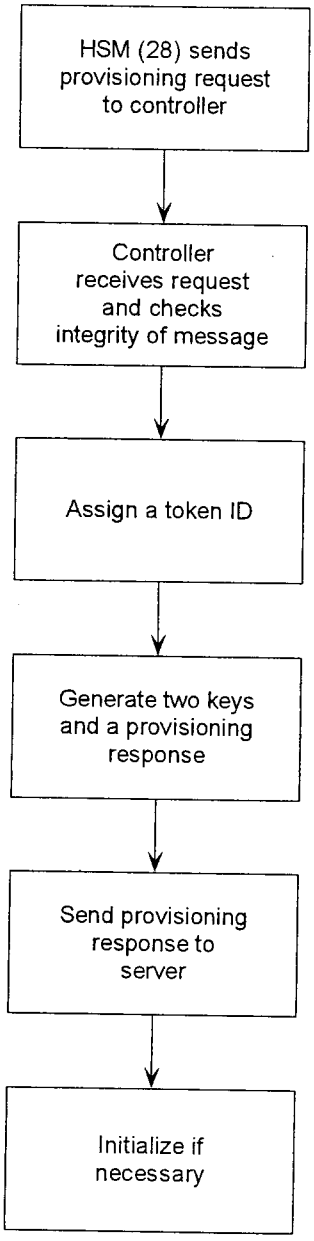

Producer
Manufacturer
Obtain bulk quantity of keys
HSM (11) encrypts blocks of keys
Store blocks of encrypted keys
Order
Retrieve an encrypted block
Decrypt and re-encrypt for transmission
Key_to_server log
Distribute
Decrypt block, re-encrypt keys individually
Store encrypted keys locally
Request
Obtain and decrypt N keys
Generate N key_to_agent log records
Clear keys to equipment
Equipment uses keys
Generate key_injection log records
+
Generate Log Report R
Send R to controller
Controller evaluates log reports
No action More Keys Suspicious
Wait for next log report R
Go to "Order"
Intervene

FIG. 4


HSM (28) sends provisioning request to controller
Controller receives request and checks integrity of message
Assign a token ID
Generate two keys and a provisioning response
Send provisioning response to server
Initialize if necessary

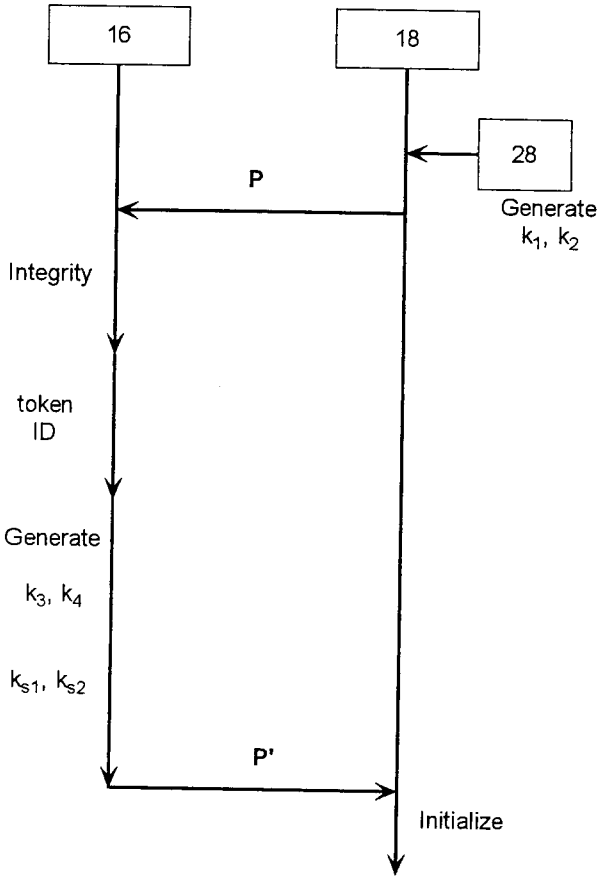
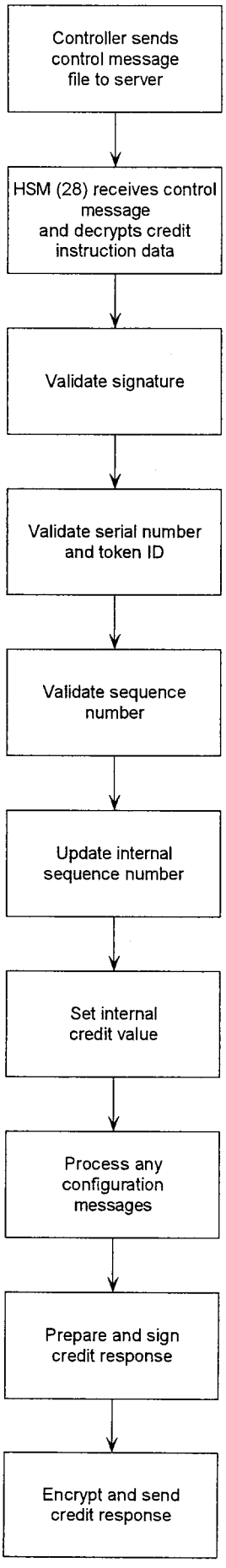

16
18
28
P
Generate
k_1, k_2
Integrity
token
ID
Generate
k_3, k_4
k_{s1}, k_{s2}
P'
Initialize

FIG.5


Controller sends control message file to server
HSM (28) receives control message and decrypts credit instruction data
Validate signature
Validate serial number and token ID
Validate sequence number
Update internal sequence number
Set internal credit value
Process any configuration messages
Prepare and sign credit response
Encrypt and send credit response

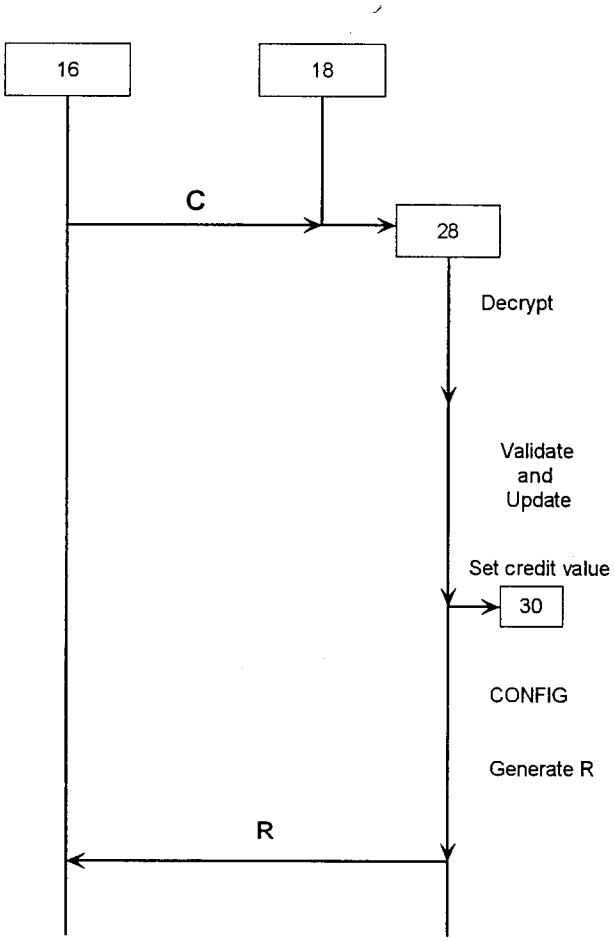

16
18
C
28
Decrypt
Validate and Update
Set credit value
30
CONFIG
Generate R
R

FIG. 6

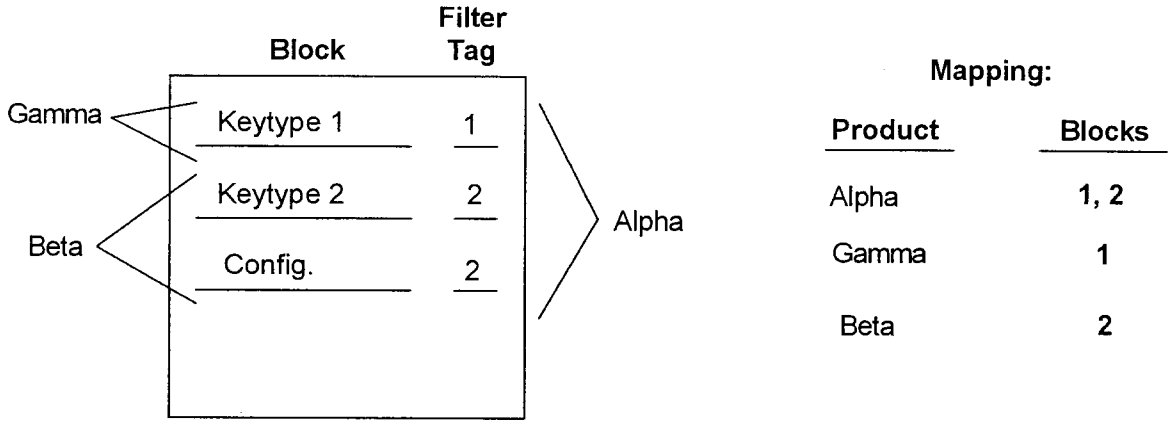

Block
Filter Tag
Gamma
Keytype 1
1
Keytype 2
2
Beta
Config.
2
Alpha
Mapping:
Product
Blocks
Alpha
1, 2
Gamma
1
Beta
2

FIG. 7

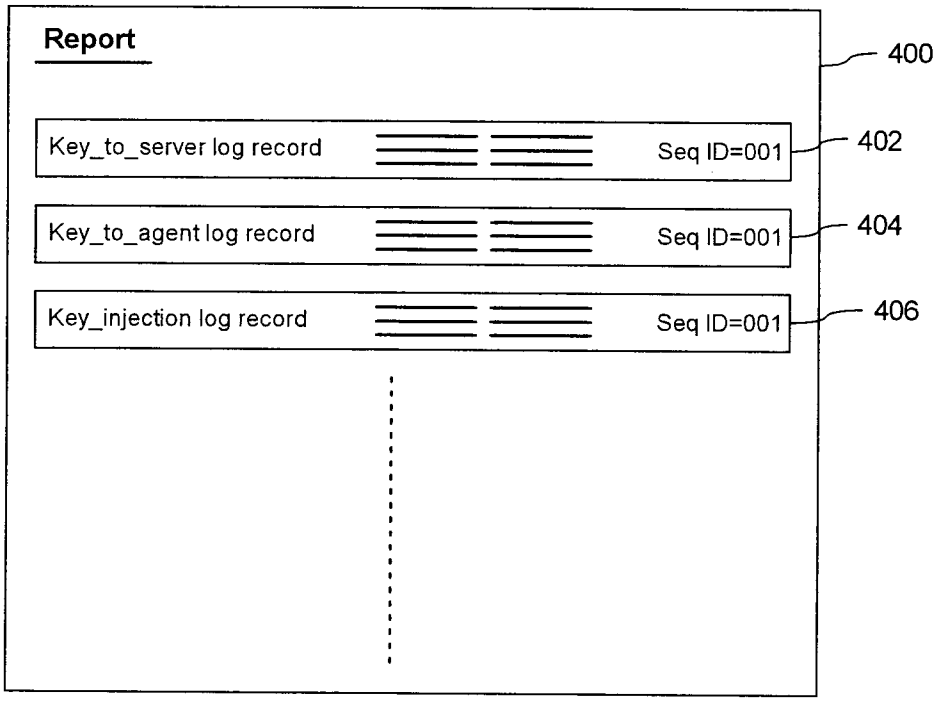

Report
400
Key_to_server log record
Seq ID=001
402
Key_to_agent log record
Seq ID=001
404
Key_injection log record
Seq ID=001
406

FIG. 8

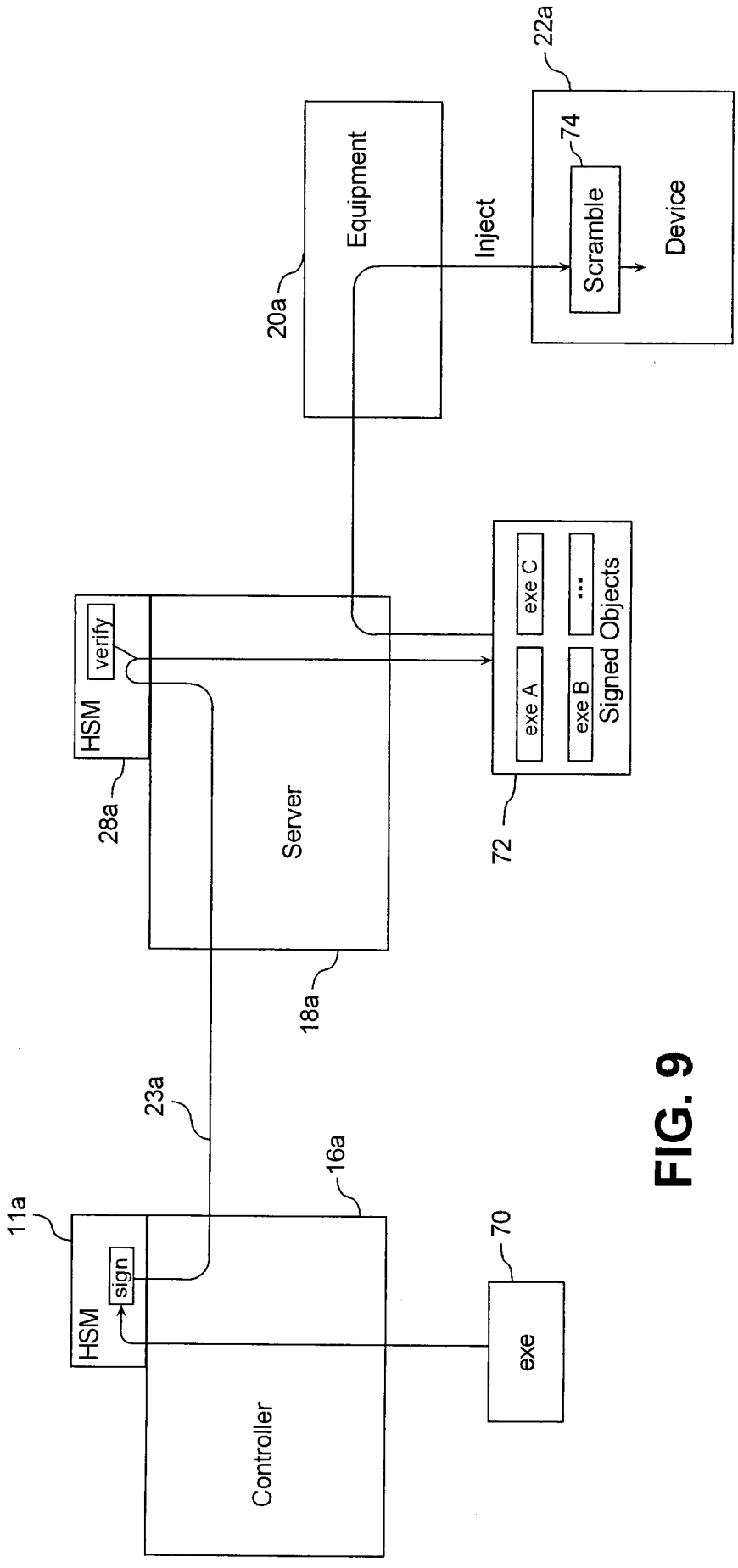

22a
74
Scramble
Device
Inject
Equipment
20a
exe C
...
exe A
exe B
Signed Objects
72
verify
HSM
28a
Server
18a
23a
16a
11a
sign
HSM
70
exe
Controller

FIG. 9

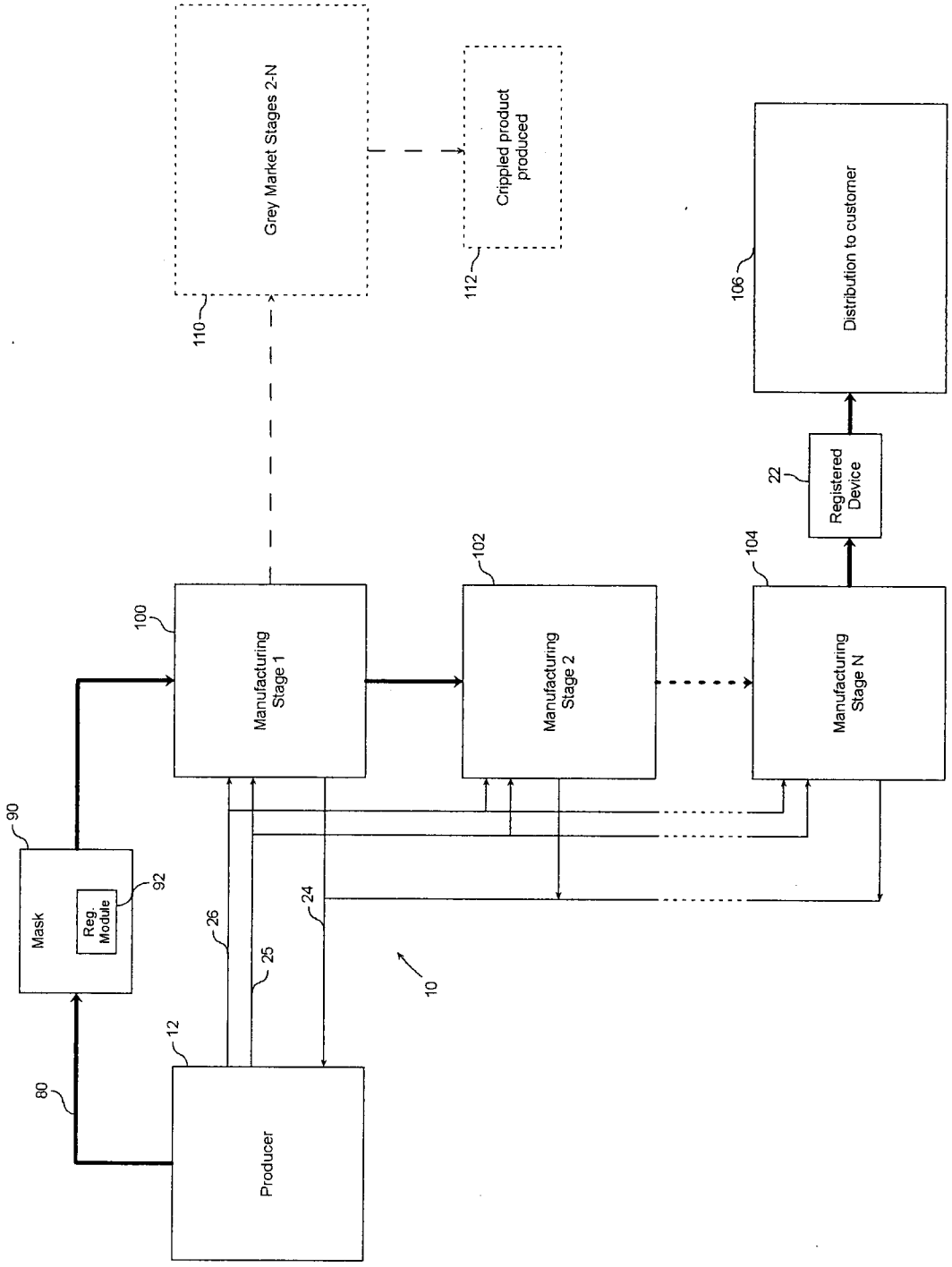

Grey Market Stages 2-N
Crippled product produced
110
112
106
Distribution to customer
22
Registered Device
100
Manufacturing Stage 1
102
Manufacturing Stage 2
104
Manufacturing Stage N
90
Mask
Reg. Module
92
26
25
24
10
12
80
Producer

FIG. 10

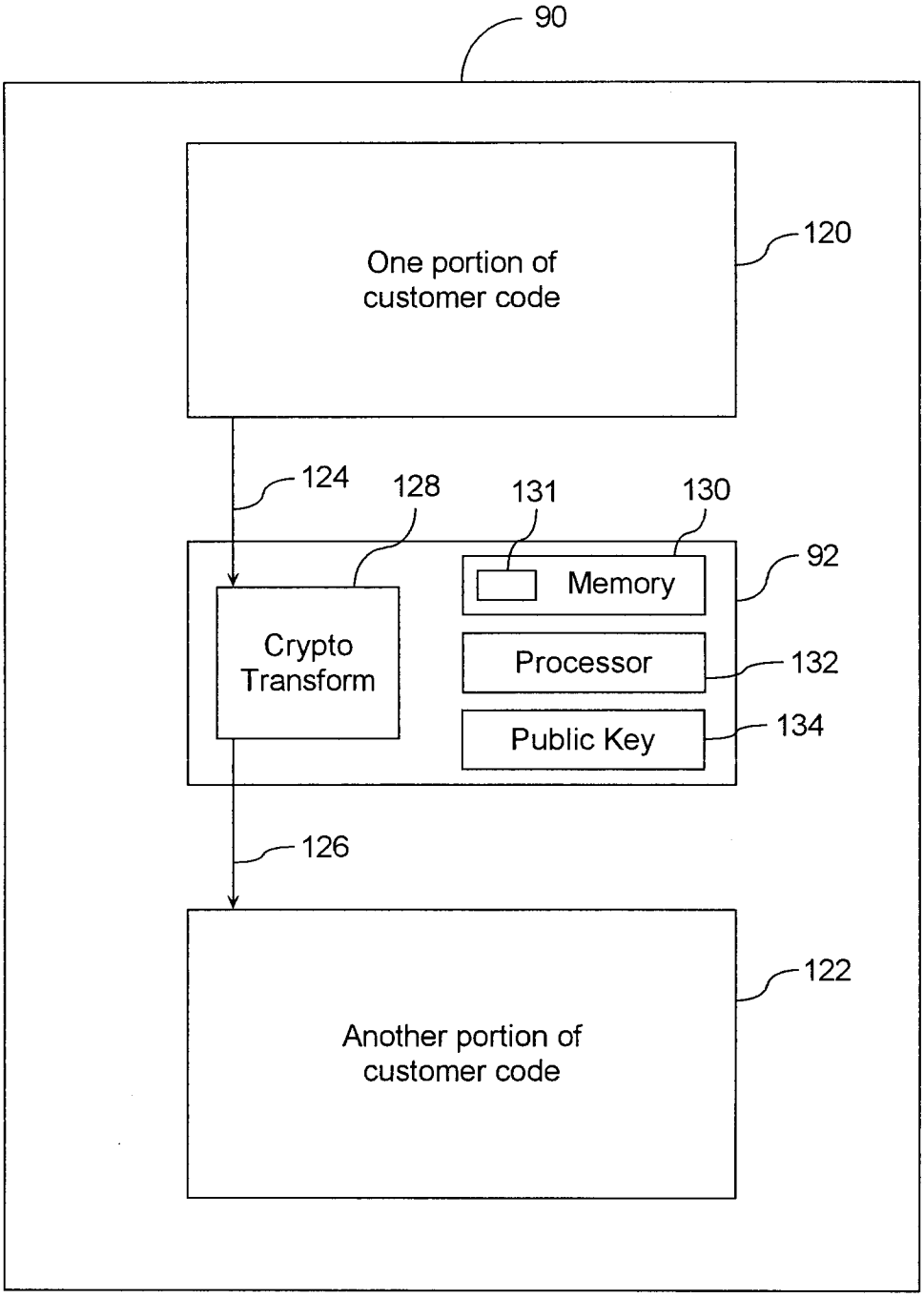

90
One portion of customer code
120
124
128
131
130
92
Memory
Crypto Transform
Processor
132
Public Key
134
126
Another portion of customer code
122

FIG. 11

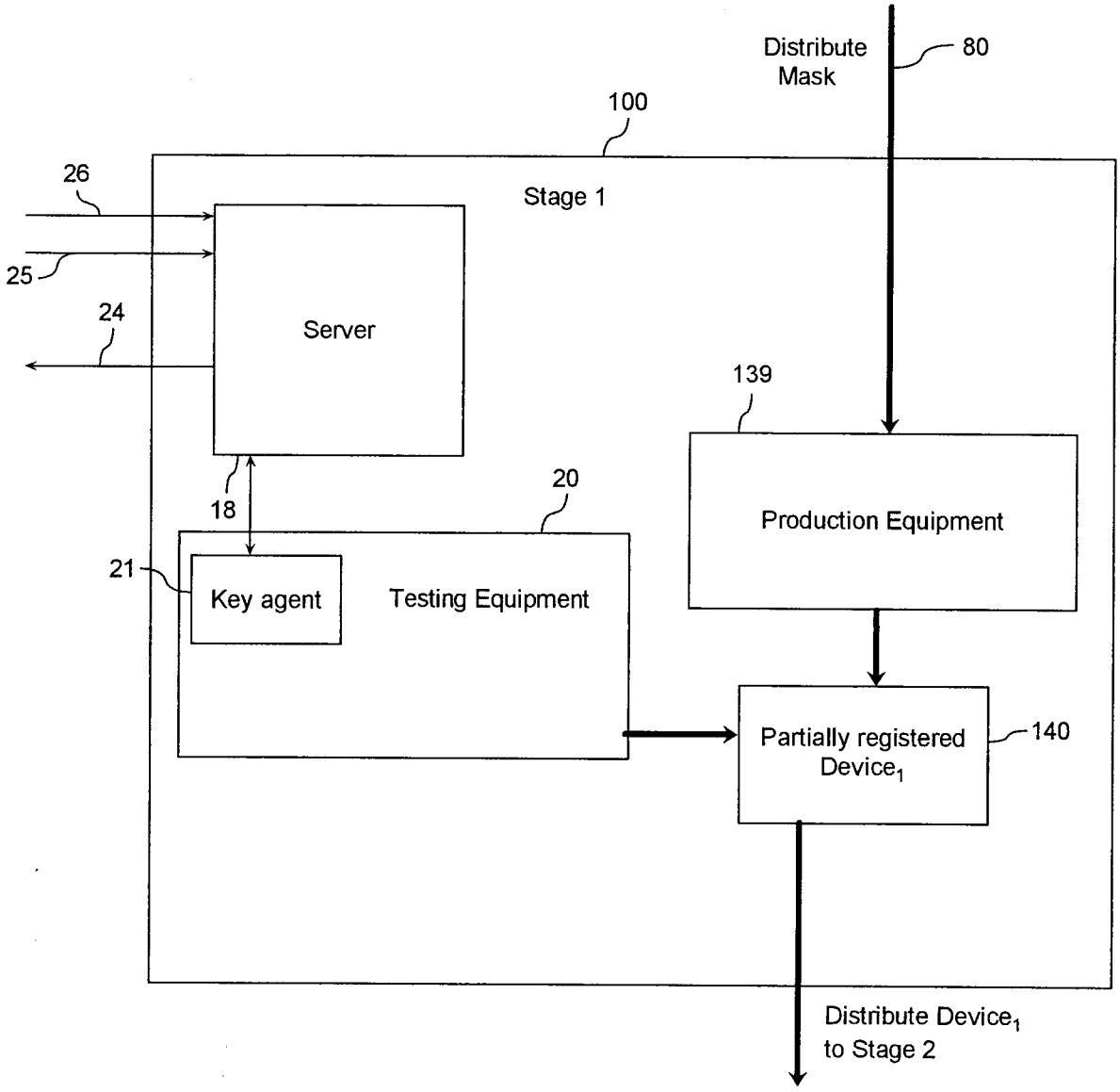

Distribute
Mask
80
100
Stage 1
26
25
24
Server
139
Production Equipment
18
20
21
Key agent
Testing Equipment
Partially registered
Device1
140
Distribute Device1
to Stage 2

FIG. 12

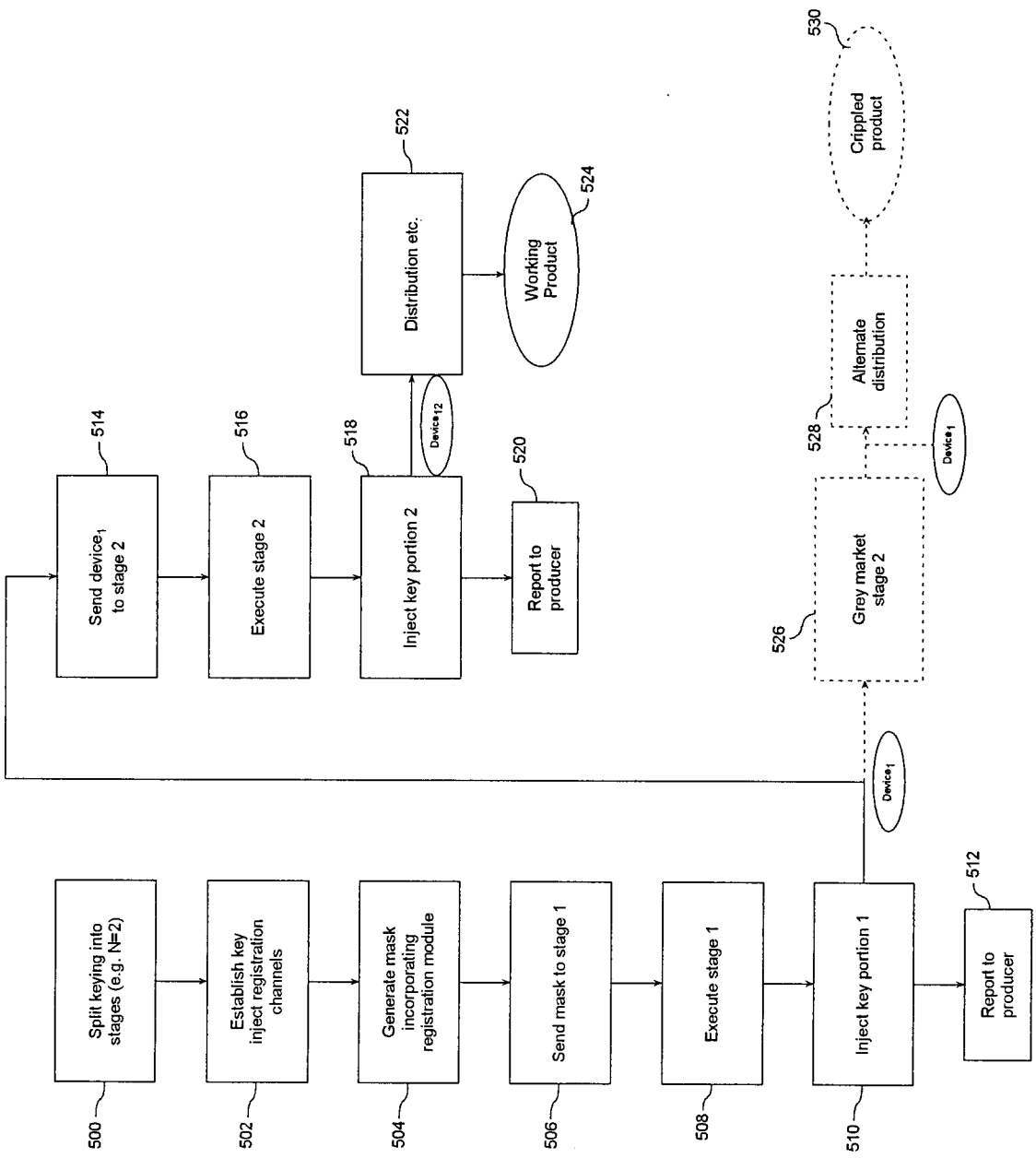

Split keying into stages (e.g. N=2)
Establish key inject registration channels
Generate mask incorporating registration module
Send mask to stage 1
Execute stage 1
Inject key portion 1
Report to producer
Device1
Grey market stage 2
Alternate distribution
Crippled product
Device1
Send device1 to stage 2
Execute stage 2
Inject key portion 2
Report to producer
Device12
Distribution etc.
Working Product
500
502
504
506
508
510
512
514
516
518
520
522
524
526
528
530

FIG. 13

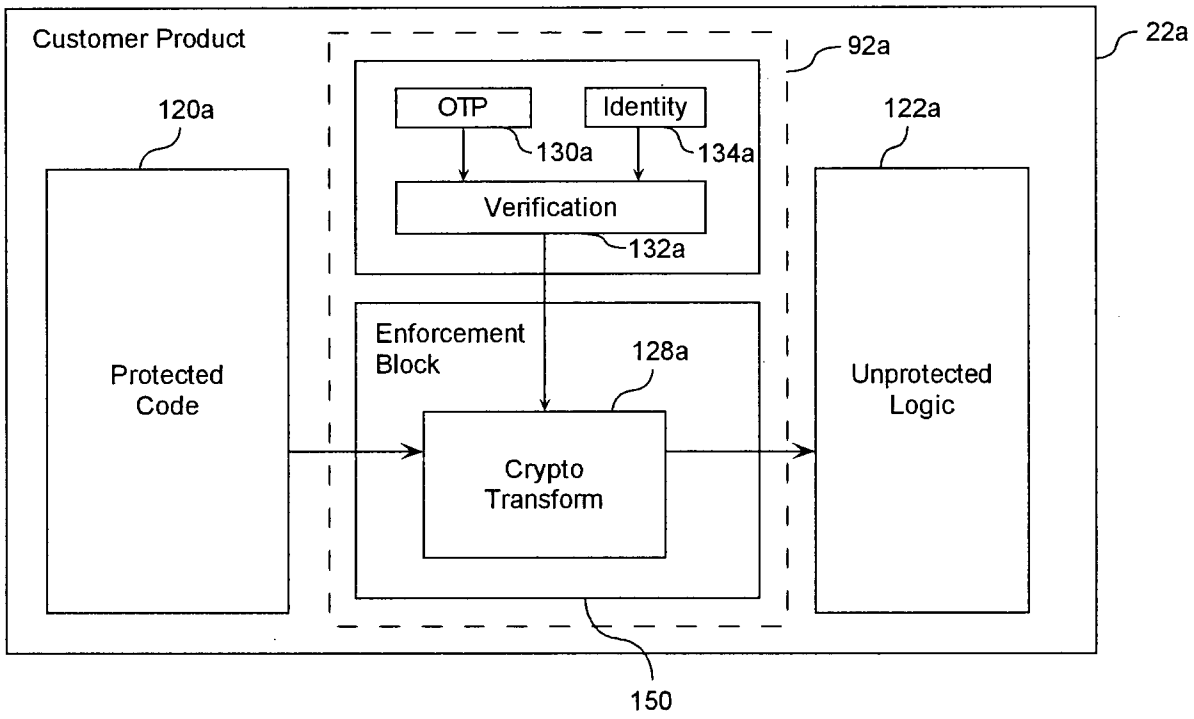

Customer Product
22a
92a
120a
OTP
Identity
122a
130a
134a
Verification
132a
Enforcement
Block
128a
Protected
Code
Unprotected
Logic
Crypto
Transform
150

FIG. 14