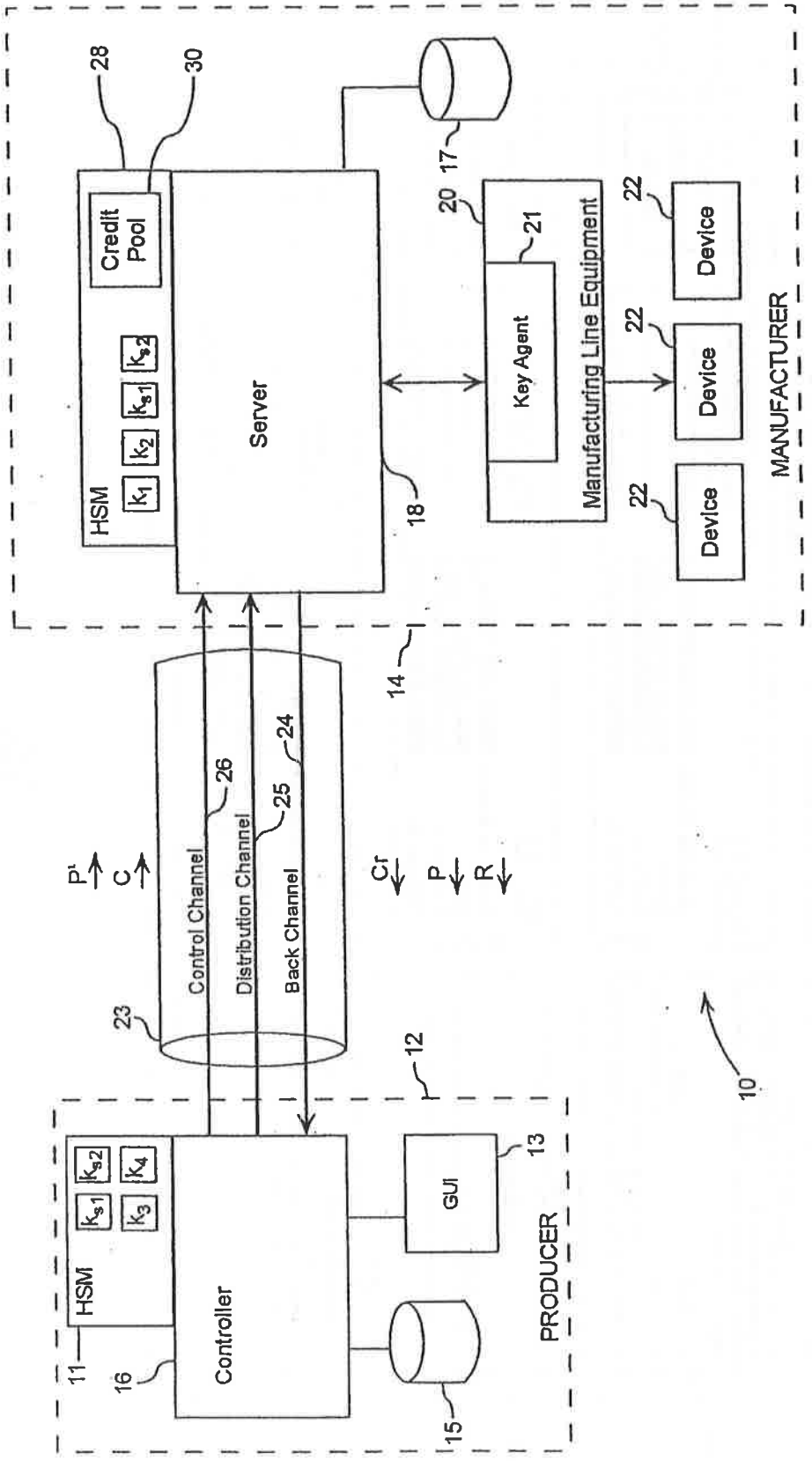

MANUFACTURER
PRODUCER
HSM
Credit Pool
Server
Key Agent
Manufacturing Line Equipment
Device
Device
Device
Controller
GUI
Control Channel
Distribution Channel
Back Channel
P'
C
Cr
P
R
10
11
12
13
14
15
16
17
18
20
21
22
23
24
25
26
28
30

FIG. 1

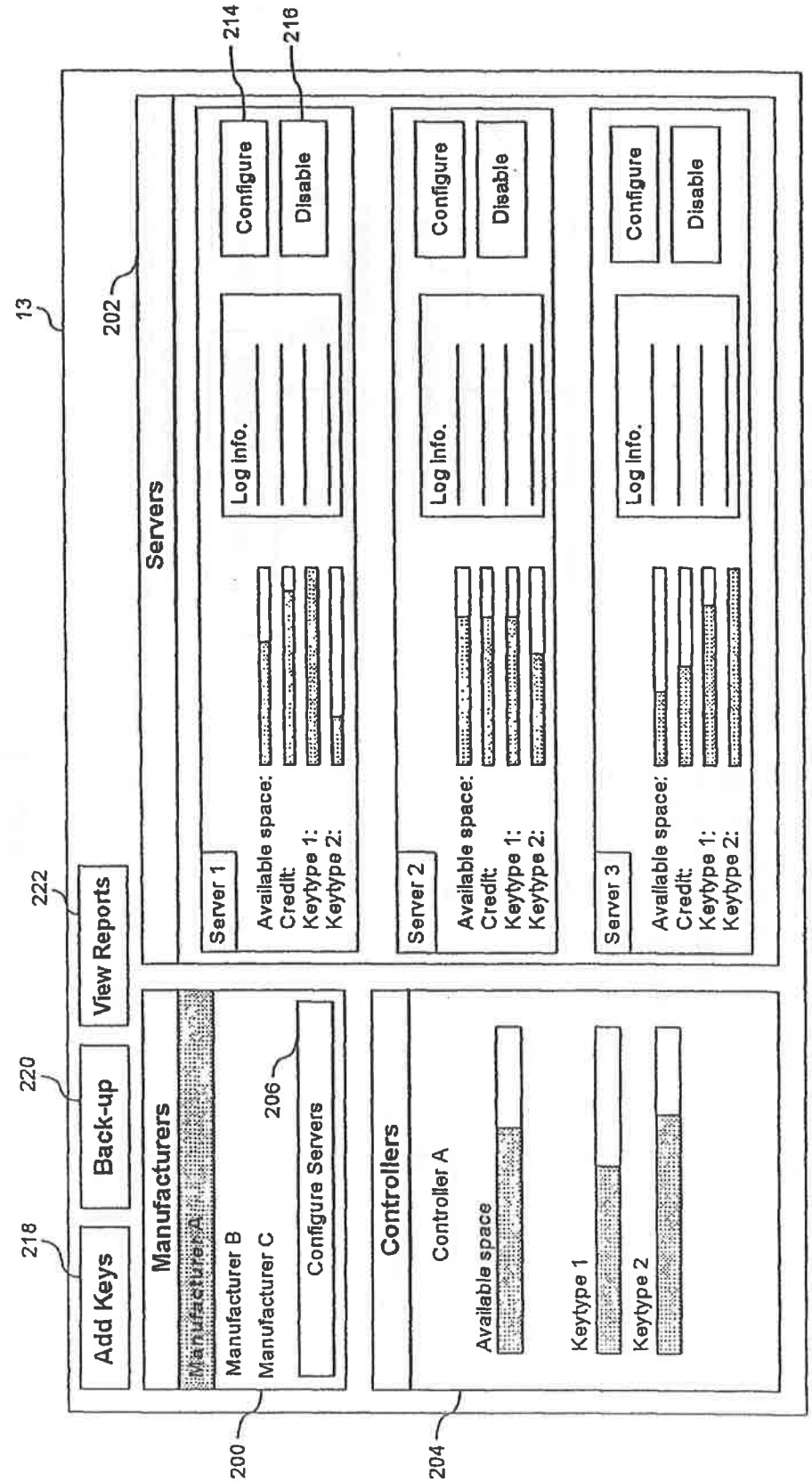

13
202
214
216
218
220
222
200
204
206
Add Keys
Back-up
View Reports
Manufacturers
Manufacturer A
Manufacturer B
Manufacturer C
Configure Servers
Controllers
Controller A
Available space
Keytype 1
Keytype 2
Servers
Server 1
Server 2
Server 3
Available space:
Credit:
Keytype 1:
Keytype 2:
Log Info.
Configure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

FIG. 2

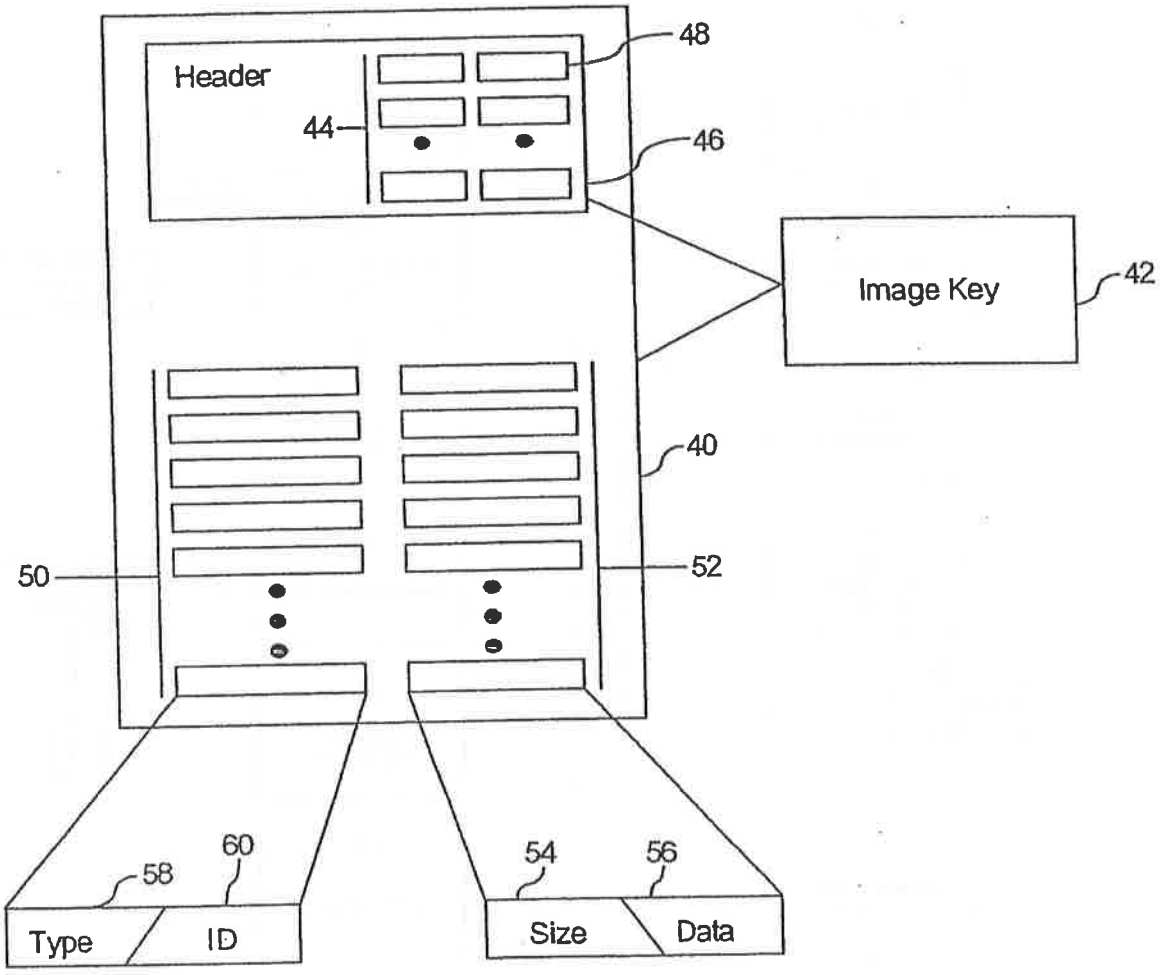

Header
44
48
46
Image Key
42
40
50
52
58
60
54
56
Type
ID
Size
Data

FIG. 3

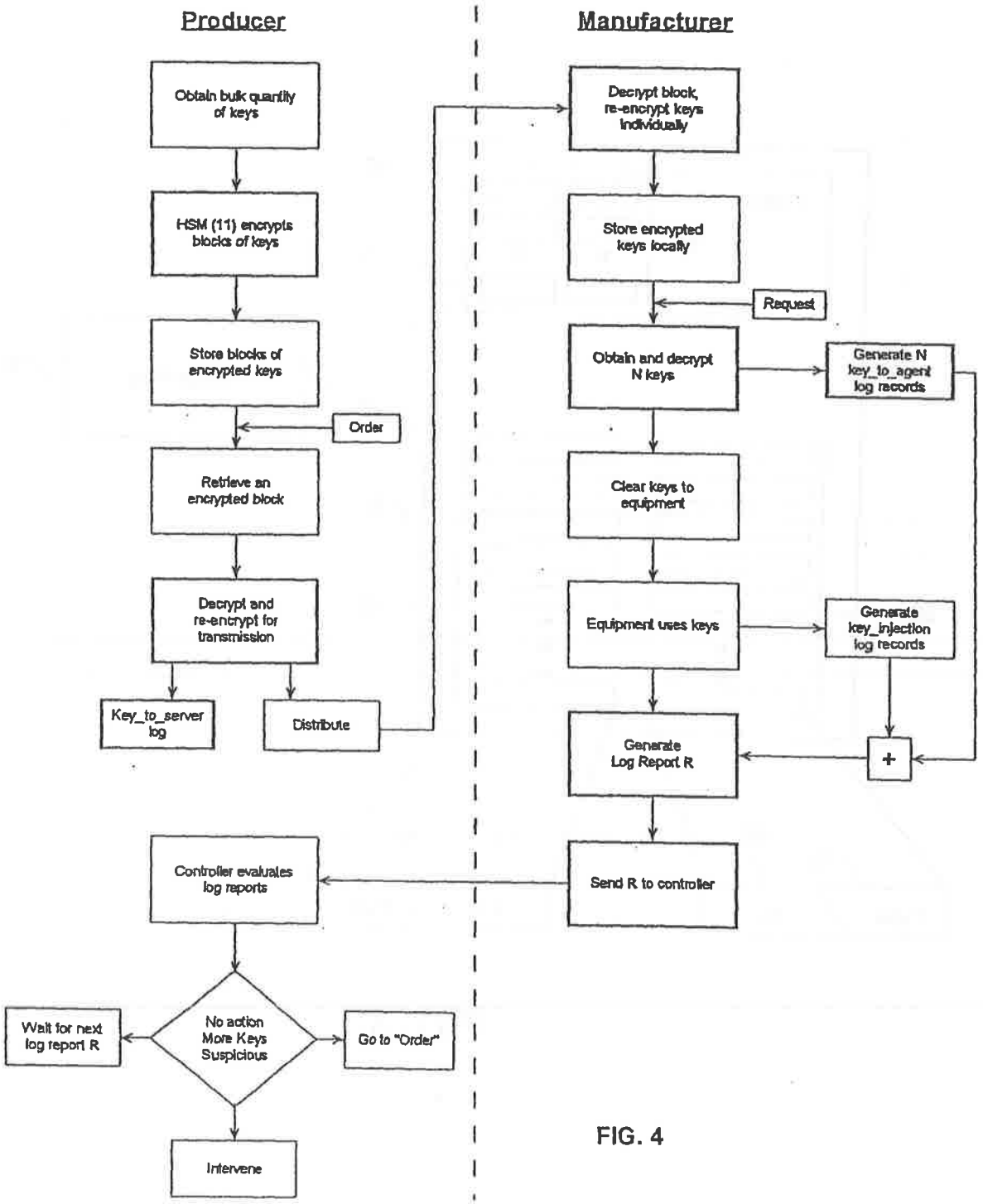
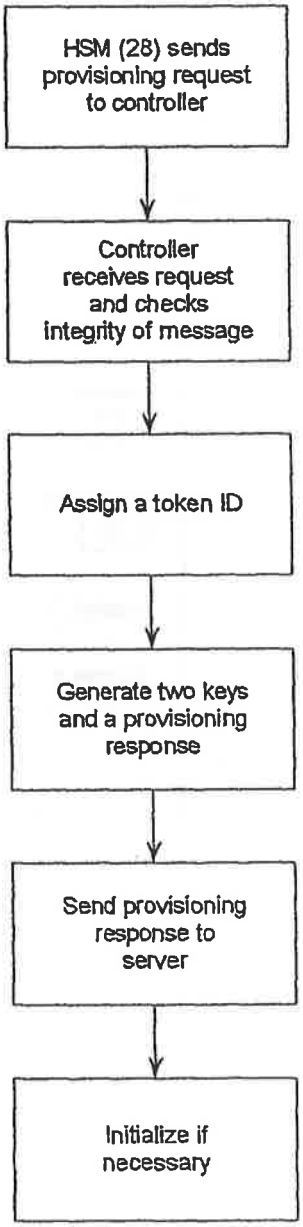

Producer
Manufacturer
Obtain bulk quantity of keys
HSM (11) encrypts blocks of keys
Store blocks of encrypted keys
Order
Retrieve an encrypted block
Decrypt and re-encrypt for transmission
Key_to_server log
Distribute
Decrypt block, re-encrypt keys individually
Store encrypted keys locally
Request
Obtain 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

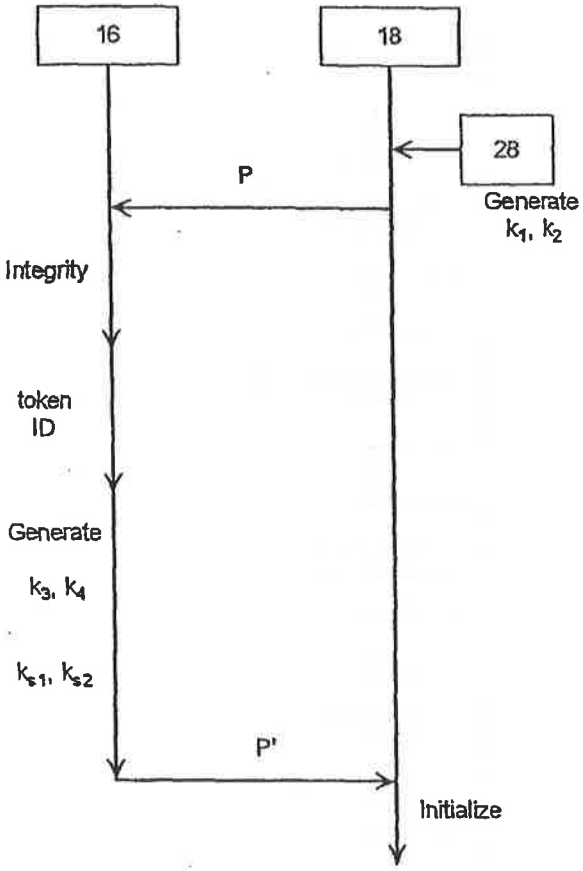
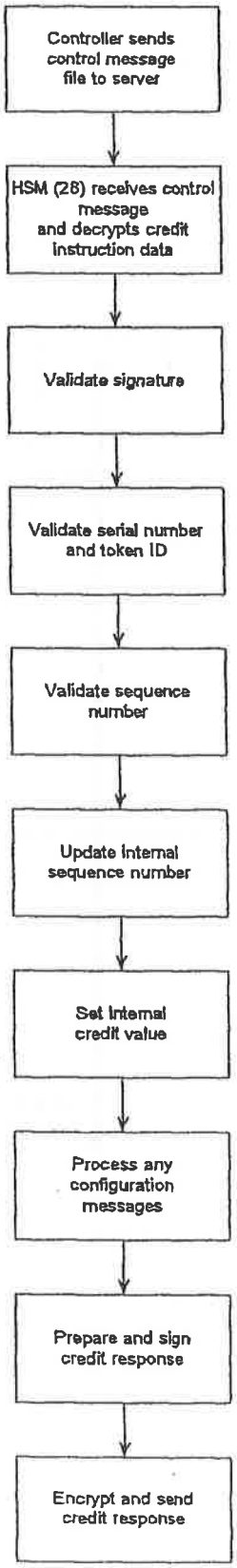

16
18
28
P
Generate
k_1, k_2
Integrity
token ID
Generate
k_3, k_4
k_{s1}, k_{s2}
P'
Initialize

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

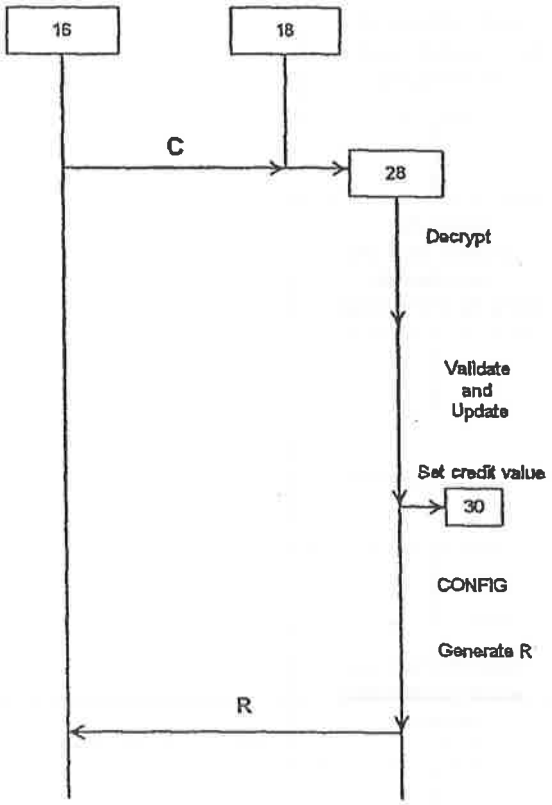

16
18
C
28
Decrypt
Validate and Update
Set credit value
30
CONFIG
Generate R
R

FIG. 6

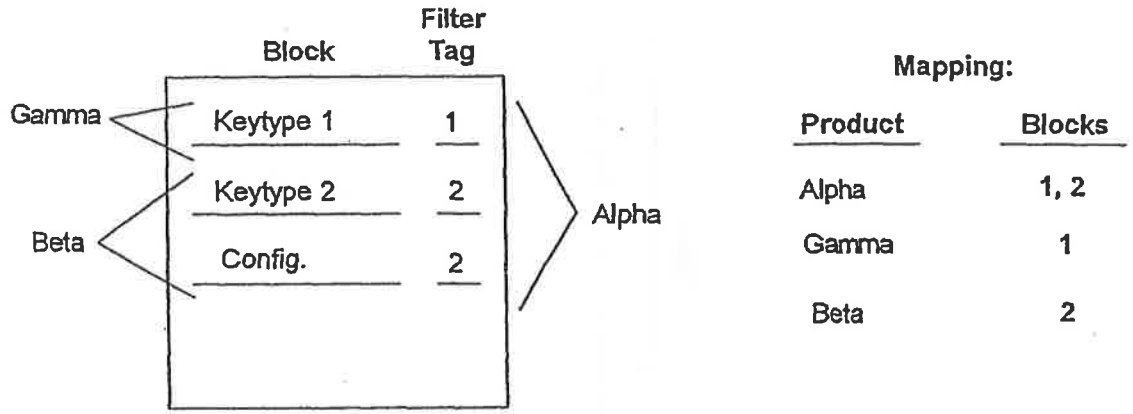

Block
Filter Tag
Gamma
Keytype 1
1
Keytype 2
2
Beta
Config.
2
Alpha
Mapping:
Product
Blocks
Alpha
1, 2
Gamma
1
Beta
2

FIG. 7

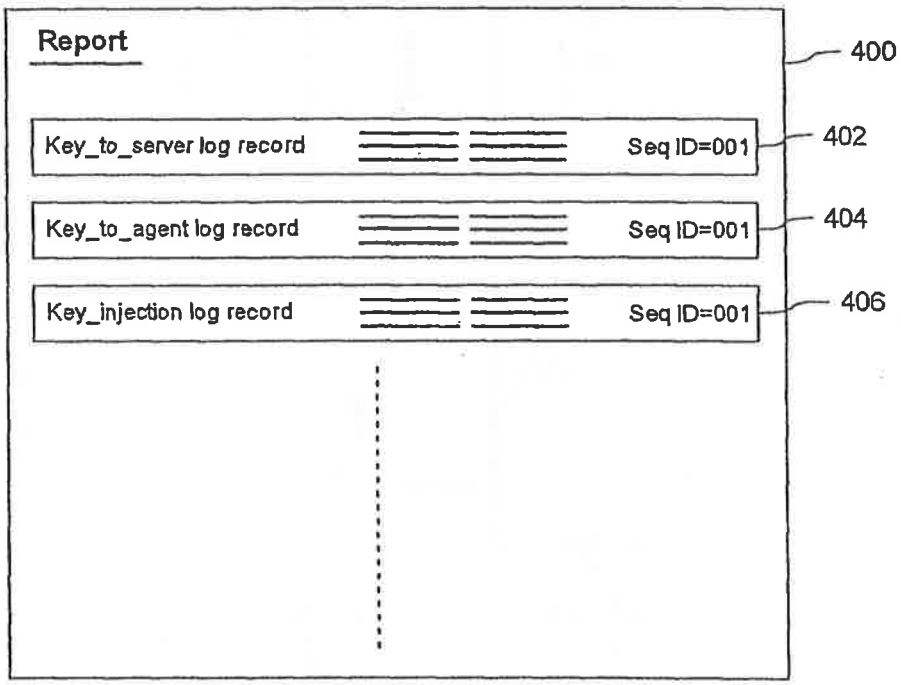

Report
400
Key_to_server log record
Seq ID=001
402
Key_to_agent log record
Seq ID=001
404
Key_injection log record
Seq ID=001
406

FIG. 8

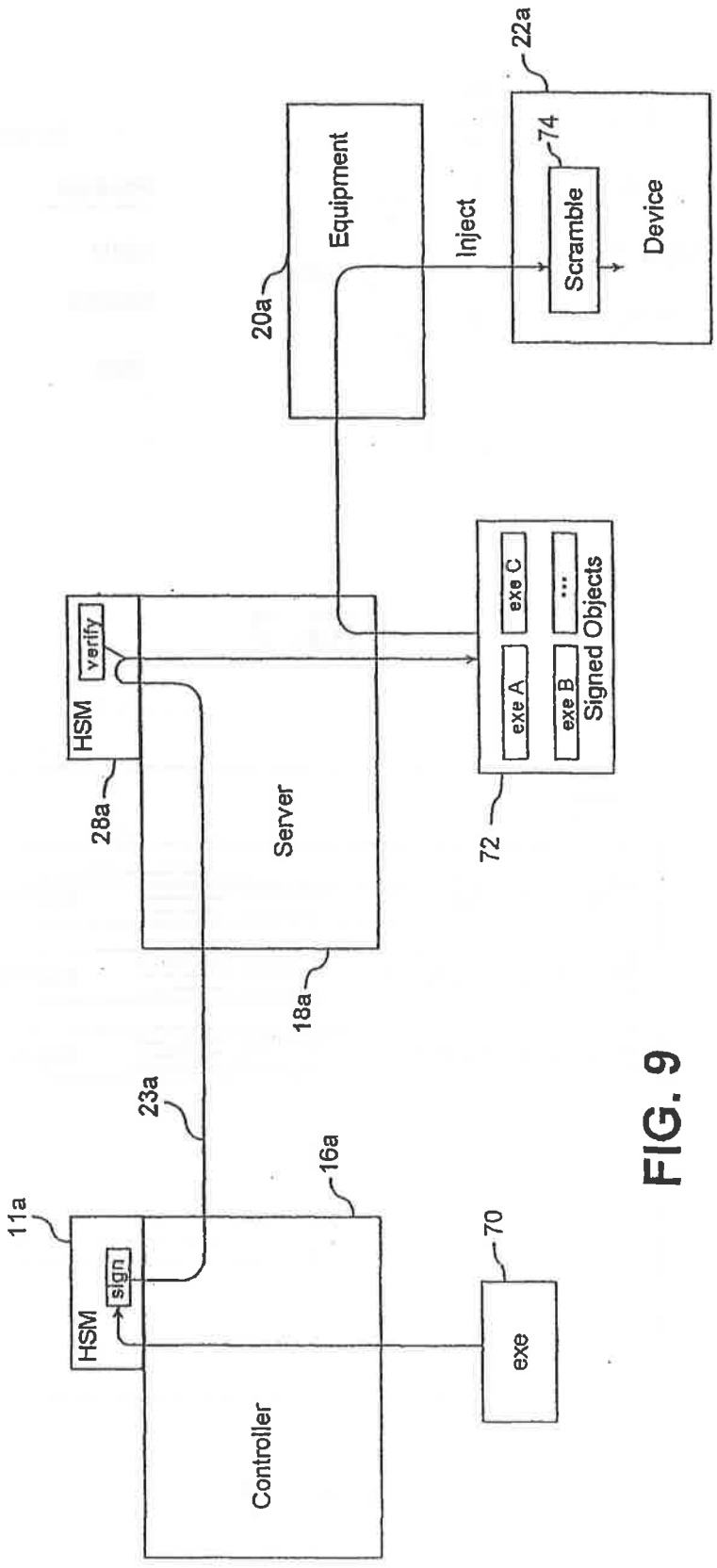

22a
74
Scramble
Device
Equipment
Inject
20a
exe C
...
exe A
exe B
Signed Objects
72
verify
HSM
28a
Server
18a
23a
16a
11a
sign
HSM
70
exe
Controller

FIG. 9

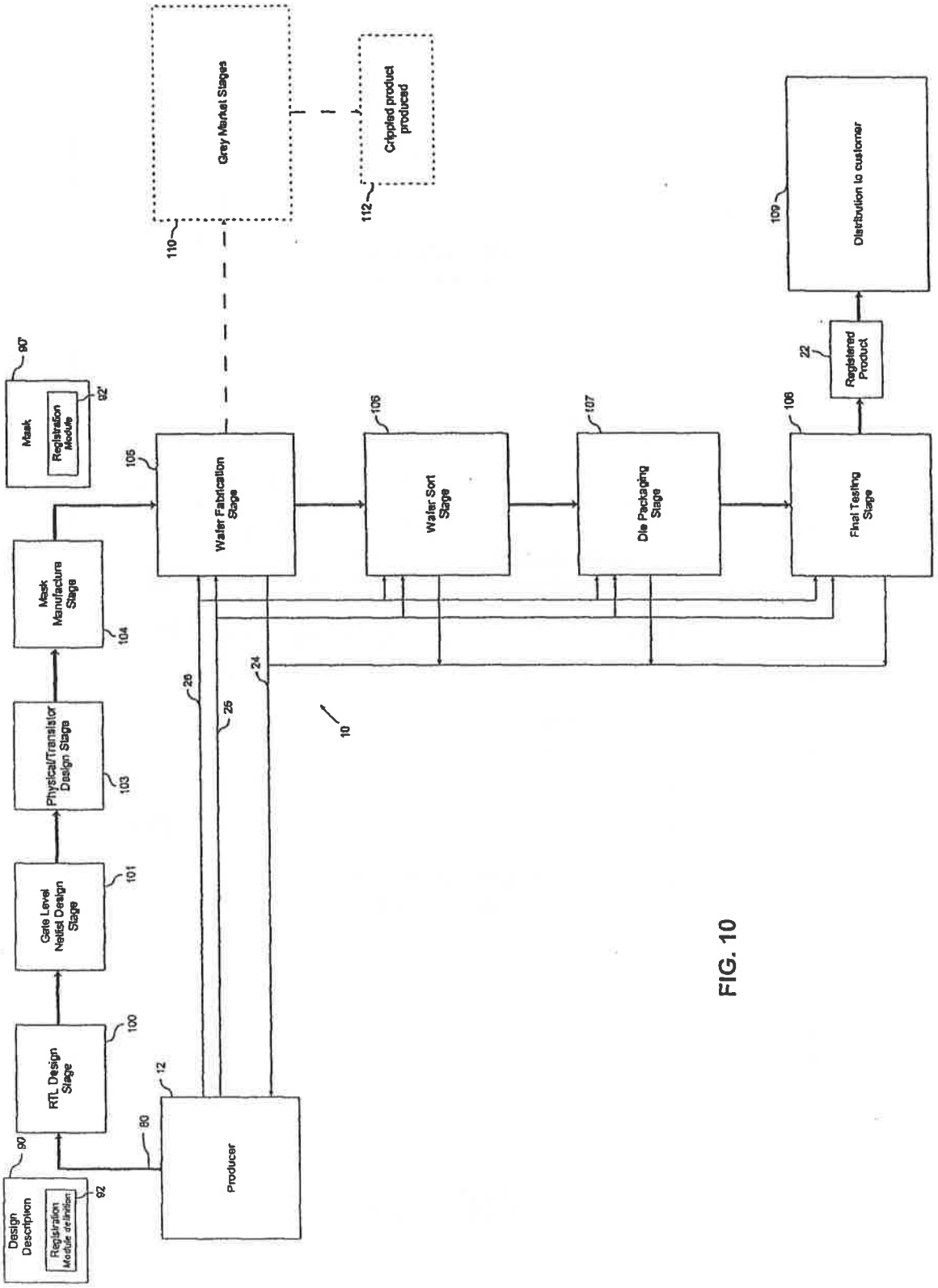

Grey Market Stages
110
Crippled product produced
112
Distribution to customer
109
Registered Product
22
Mask
Registration Module
90'
92'
Wafer Fabrication Stage
105
Wafer Sort Stage
106
Die Packaging Stage
107
Final Testing Stage
108
Mask Manufacture Stage
104
Physical/Transistor Design Stage
103
Gate Level Netlist Design Stage
101
RTL Design Stage
100
Design Description
Registration Module definition
90
92
Producer
12
80
26
25
24
10

FIG. 10

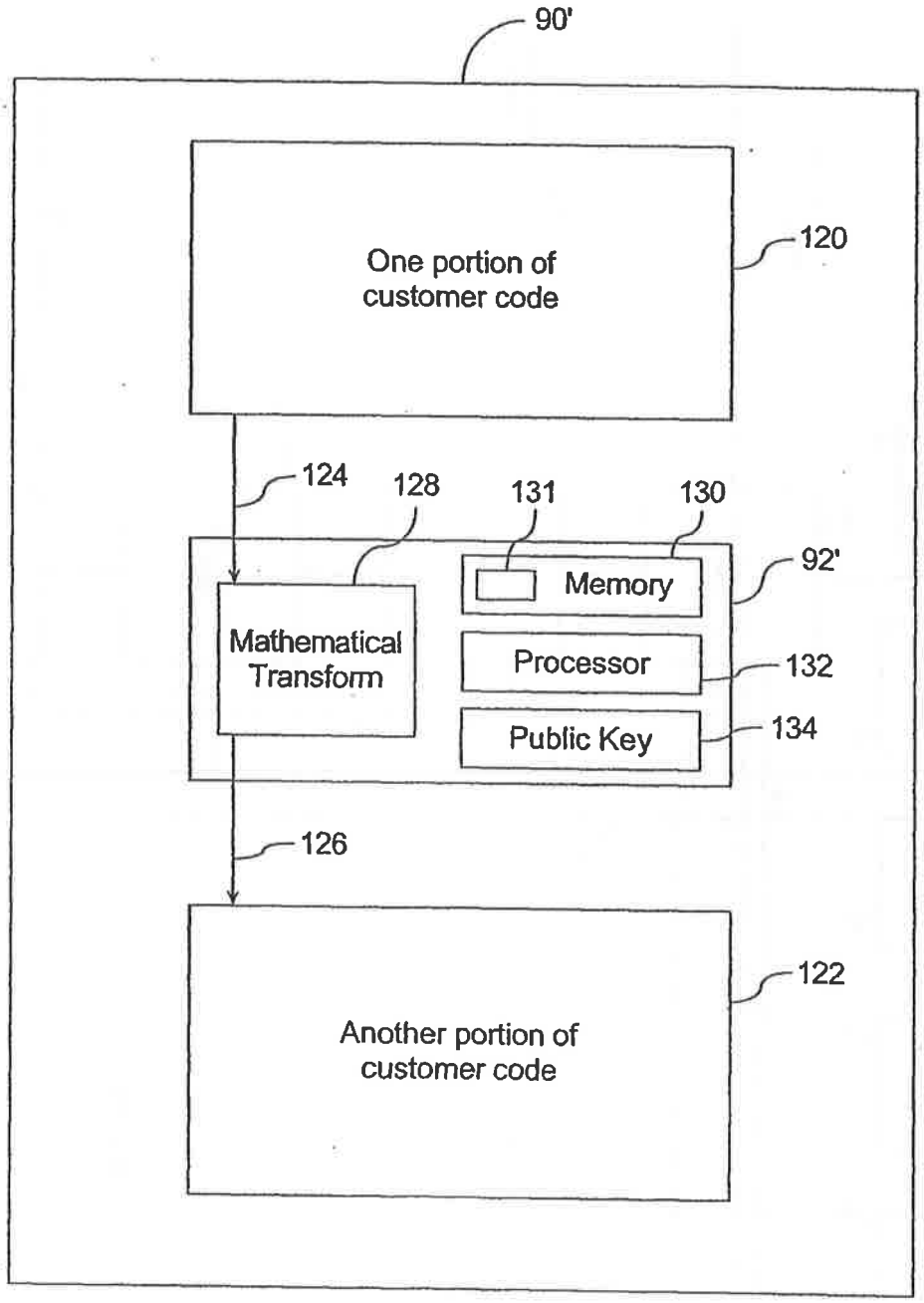

90'
One portion of customer code
120
124
128
131
130
Memory
92'
Mathematical Transform
Processor
132
Public Key
134
126
Another portion of customer code
122

FIG. 11

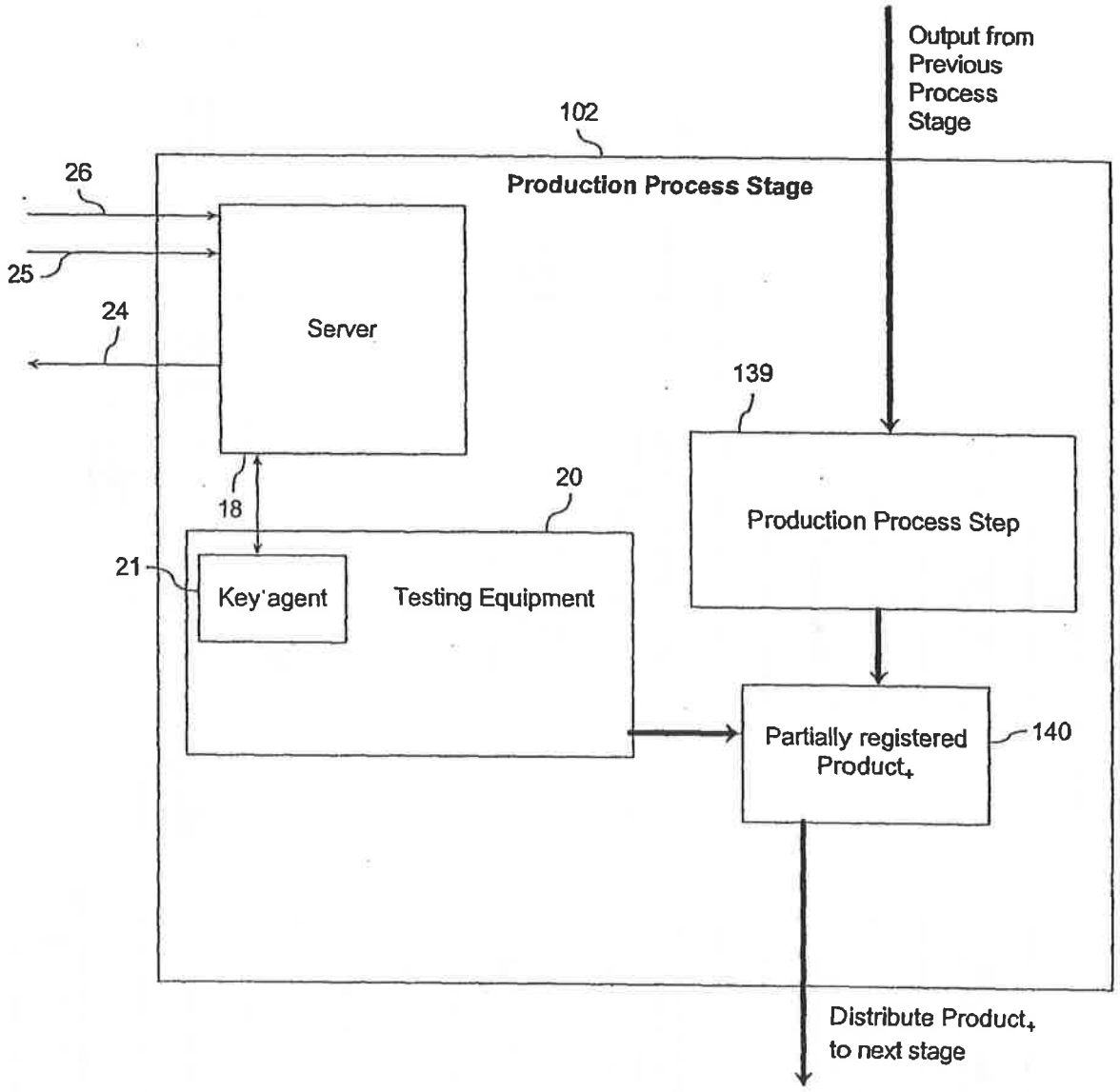

Output from Previous Process Stage
102
Production Process Stage
26
25
24
Server
139
18
20
Production Process Step
21
Key agent
Testing Equipment
Partially registered Product+
140
Distribute Product+ to next stage

FIG. 12

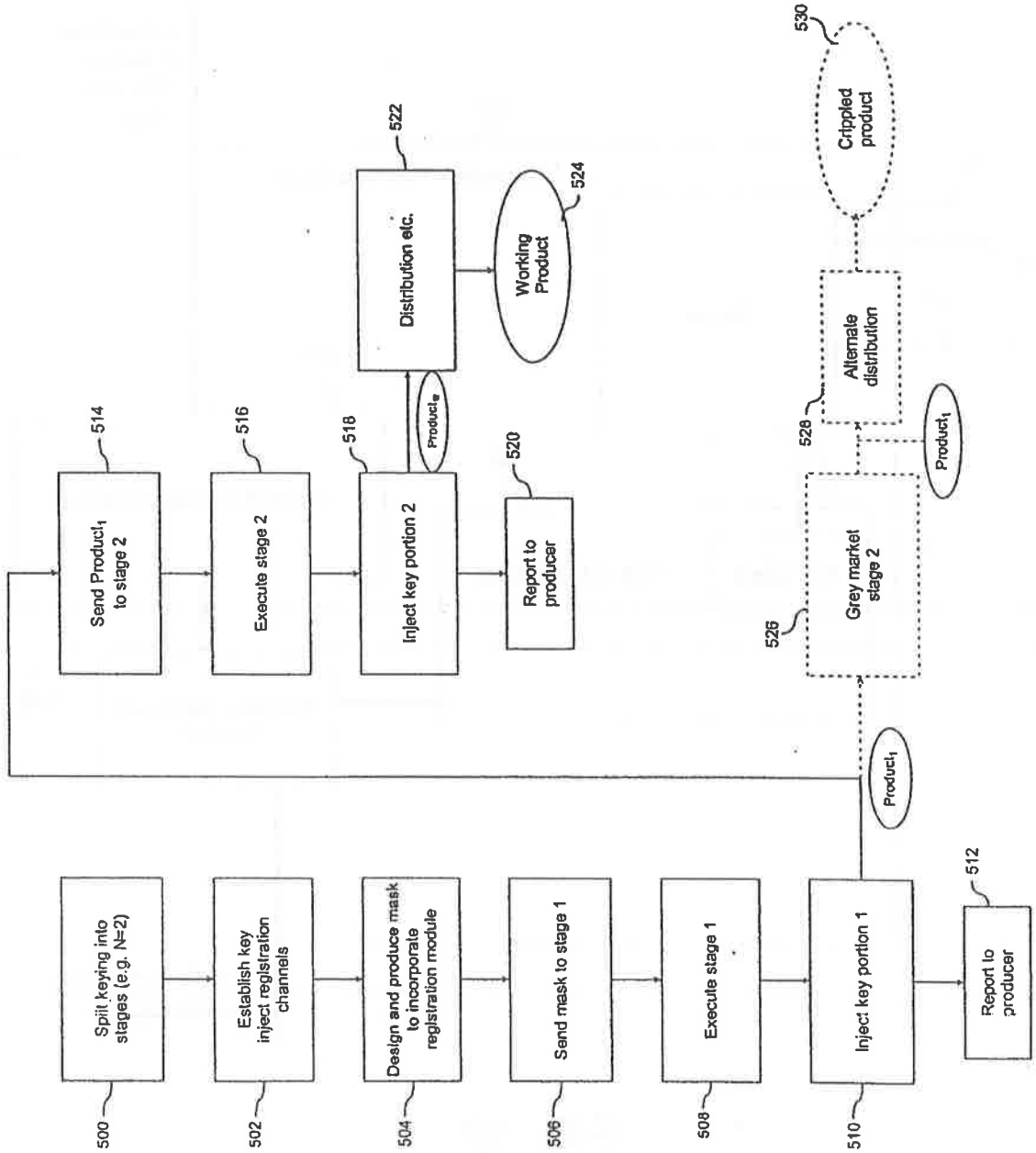

Split keying into stages (e.g. N=2)
Establish key inject registration channels
Design and produce mask to incorporate registration module
Send mask to stage 1
Execute stage 1
Inject key portion 1
Report to producer
Send Product1 to stage 2
Execute stage 2
Inject key portion 2
Report to producer
Distribution etc.
Working Product
Product2
Product1
Grey market stage 2
Alternate distribution
Crippled product
500
502
504
506
508
510
512
514
516
518
520
522
524
526
528
530

FIG. 13

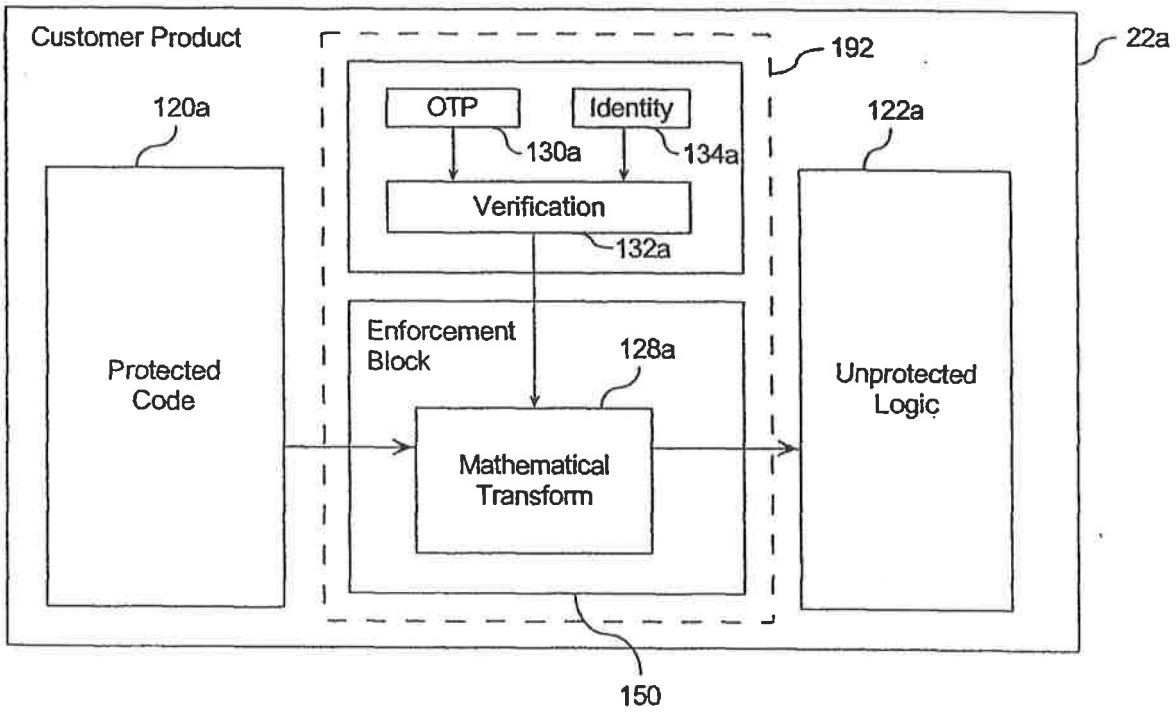

Customer Product
192
22a
120a
OTP
Identity
130a
134a
122a
Verification
132a
Enforcement
Block
128a
Protected
Code
Unprotected
Logic
Mathematical
Transform
150

FIG. 14