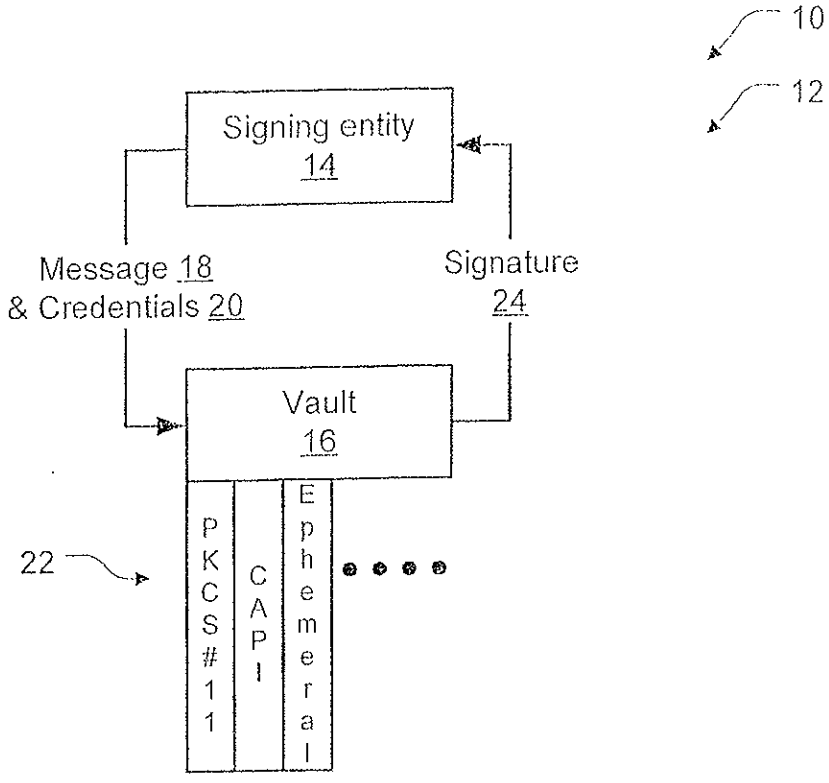

10
12
Signing entity
14
Message 18
& Credentials 20
Signature
24
Vault
16
22
PKCS#11
CAPI
Ephemeral

FIG. 1

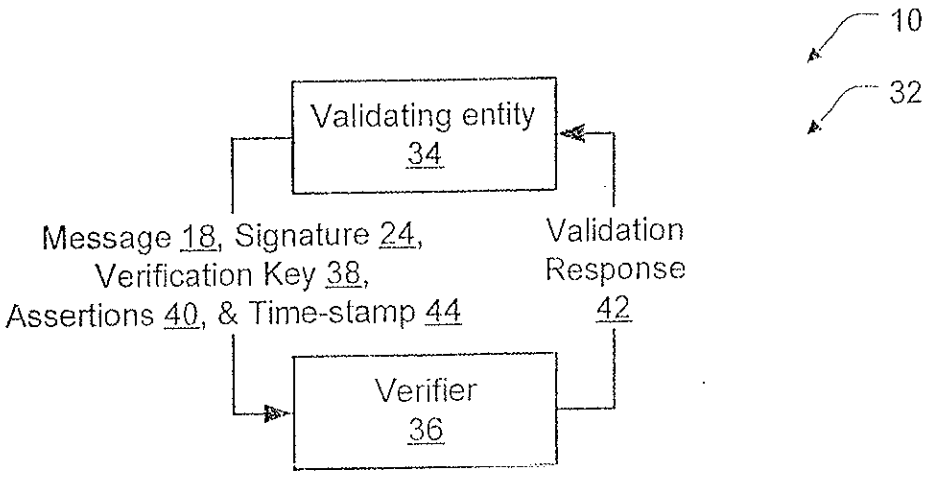

10
32
Validating entity
34
Message 18, Signature 24,
Verification Key 38,
Assertions 40, & Time-stamp 44
Validation
Response
42
Verifier
36

FIG. 2

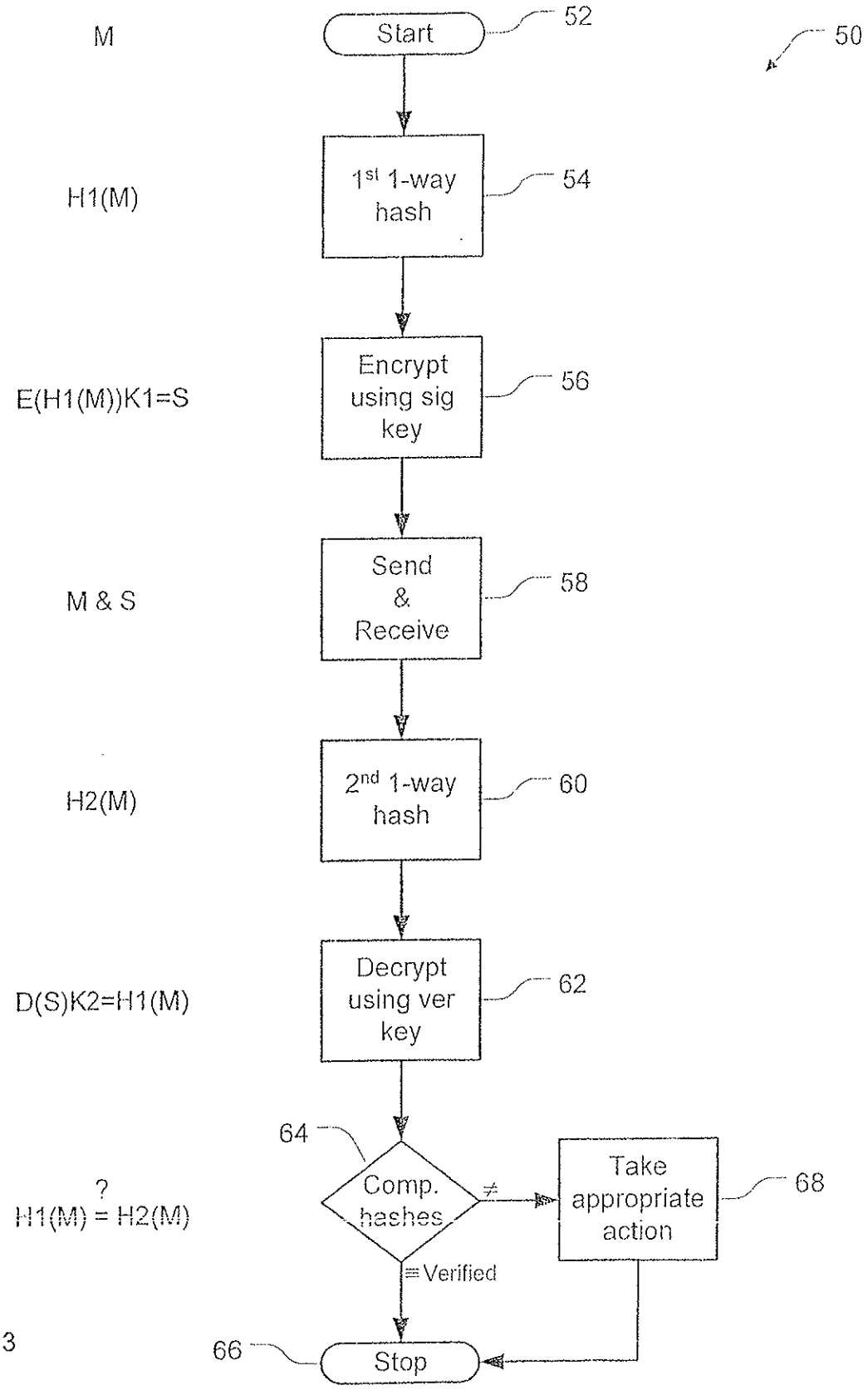

M
Start
52
50
H1(M)
1st 1-way hash
54
E(H1(M))K1=S
Encrypt using sig key
56
M & S
Send & Receive
58
H2(M)
2nd 1-way hash
60
D(S)K2=H1(M)
Decrypt using ver key
62
64
?
H1(M) = H2(M)
Comp. hashes
≠
Take appropriate action
68
≡ Verified
66
Stop

FIG.3

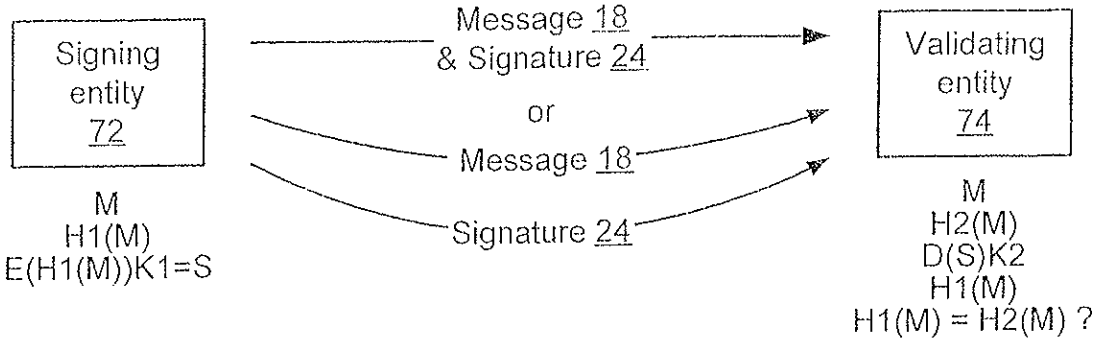


FIG. 4a

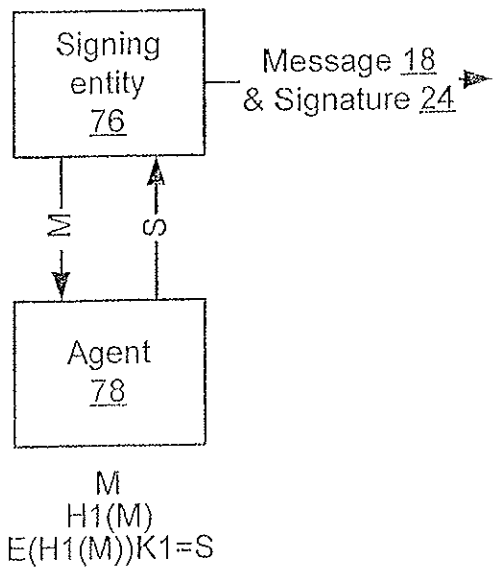


FIG. 4b

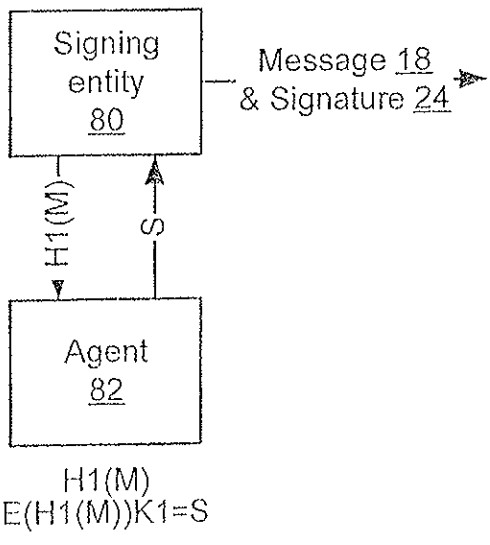


FIG. 4c

FIG. 4d

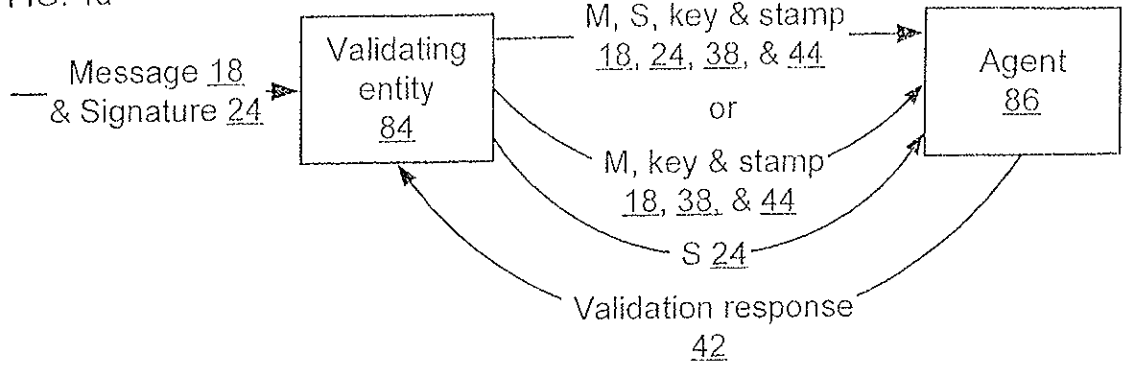


FIG. 4e

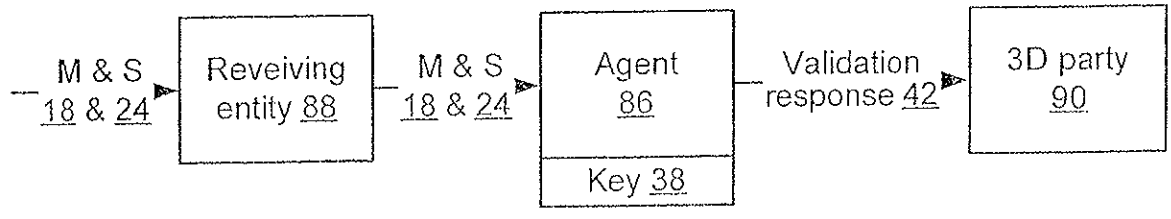


FIG. 4f

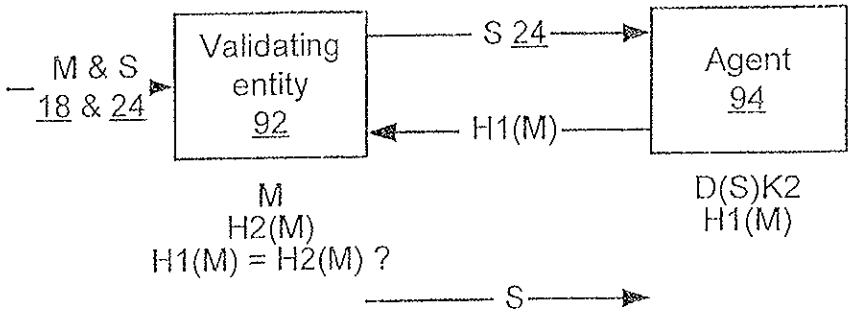


FIG. 4g

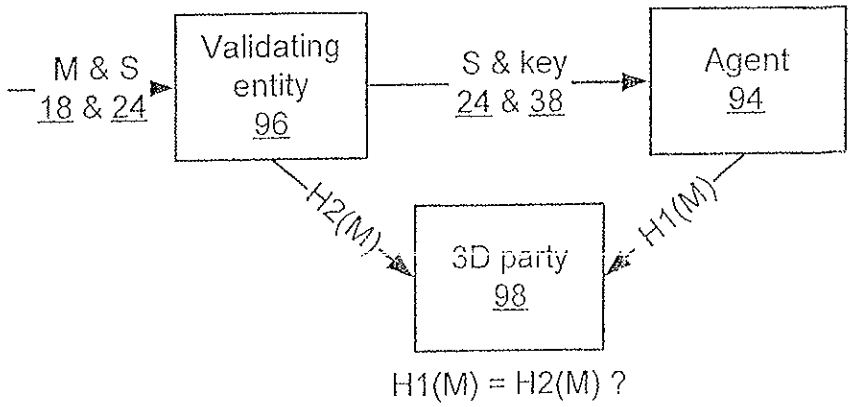
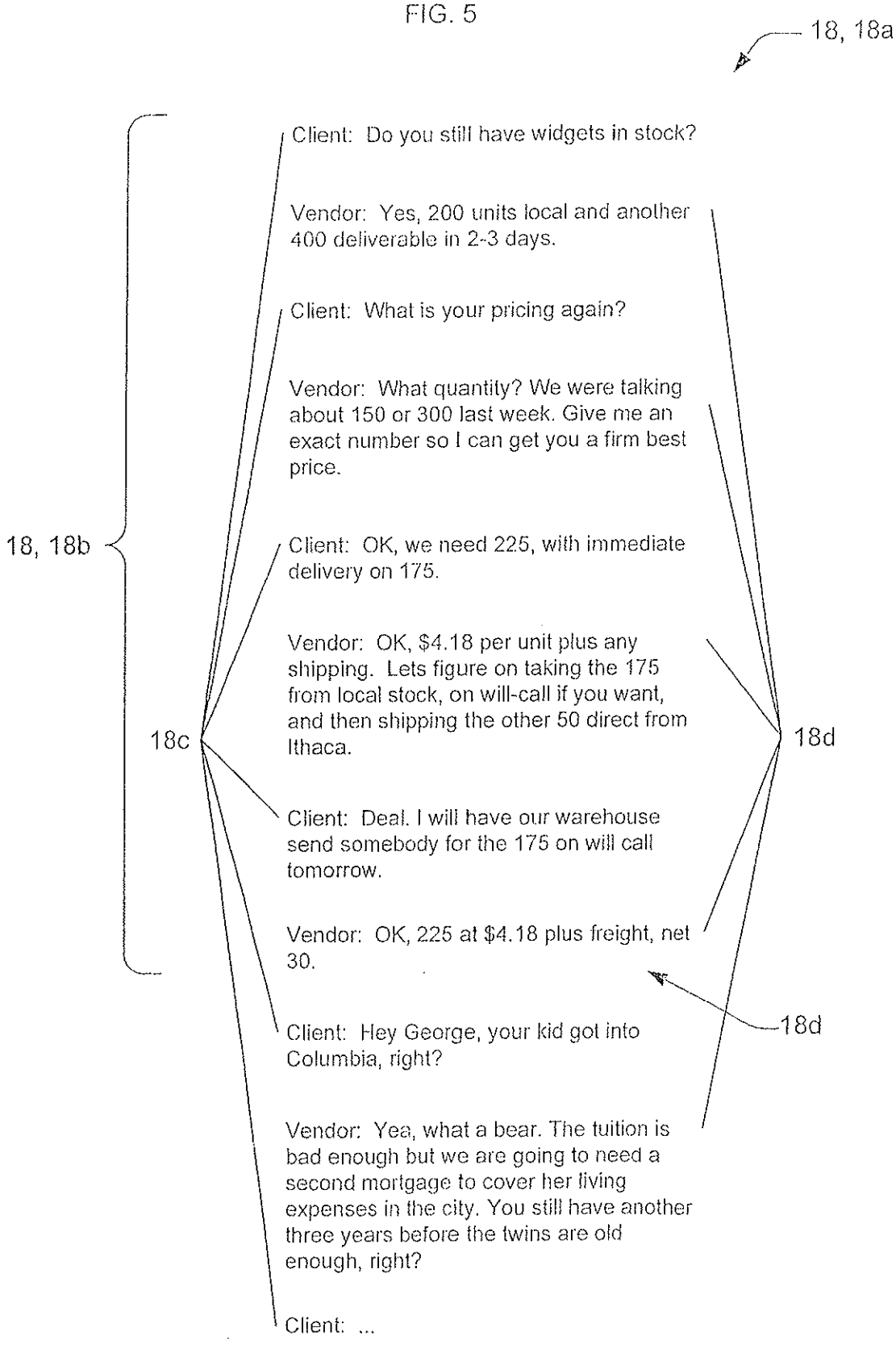


FIG. 5


18, 18a
Client: Do you still have widgets in stock?
Vendor: Yes, 200 units local and another 400 deliverable in 2-3 days.
Client: What is your pricing again?
Vendor: What quantity? We were talking about 150 or 300 last week. Give me an exact number so I can get you a firm best price.
Client: OK, we need 225, with immediate delivery on 175.
Vendor: OK, $4.18 per unit plus any shipping. Lets figure on taking the 175 from local stock, on will-call if you want, and then shipping the other 50 direct from Ithaca.
Client: Deal. I will have our warehouse send somebody for the 175 on will call tomorrow.
Vendor: OK, 225 at $4.18 plus freight, net 30.
Client: Hey George, your kid got into Columbia, right?
Vendor: Yea, what a bear. The tuition is bad enough but we are going to need a second mortgage to cover her living expenses in the city. You still have another three years before the twins are old enough, right?
Client: ...
18, 18b
18c
18d
18d

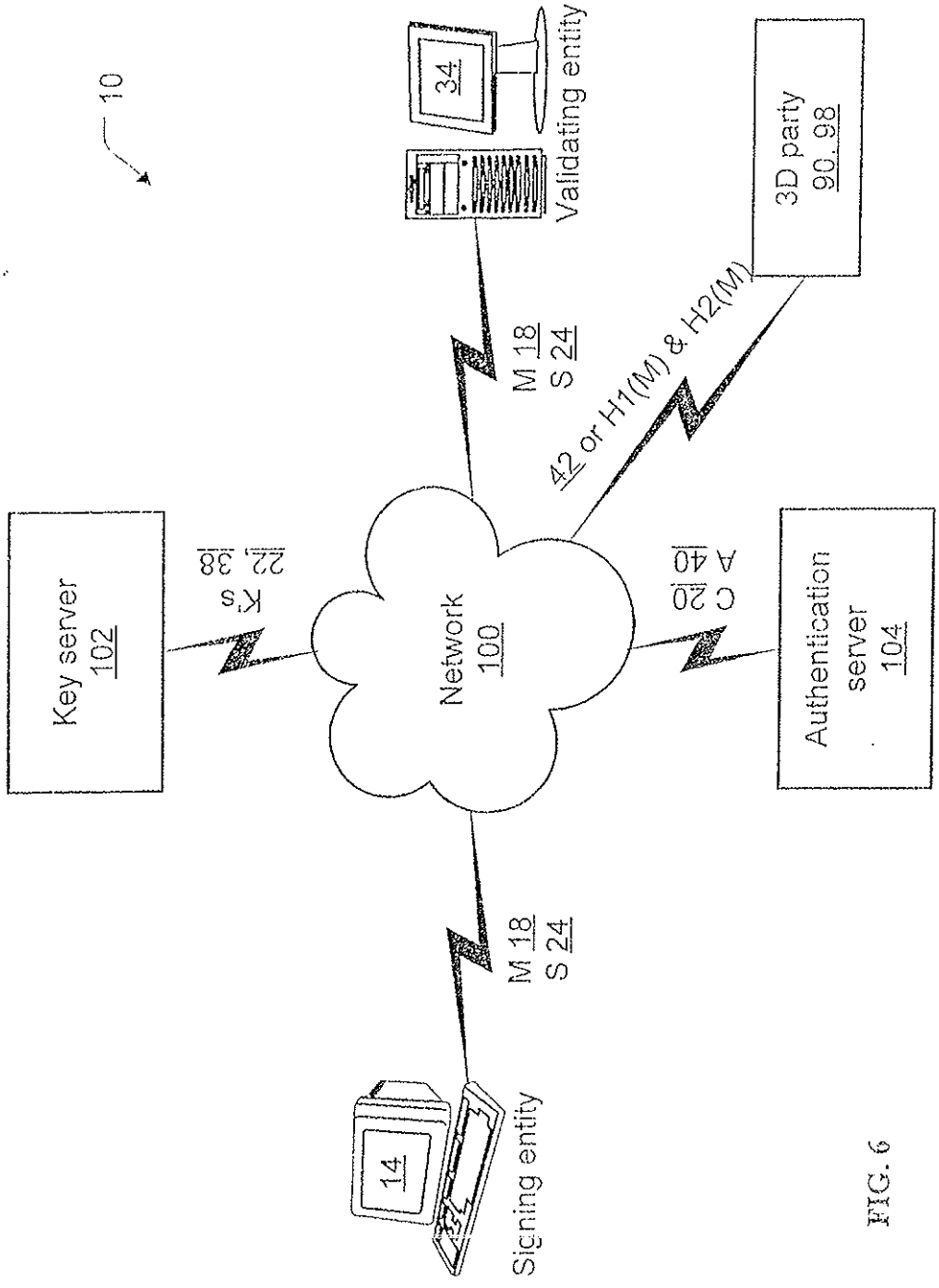

10
34
Validating entity
3D party
90, 98
M 18
S 24
42 or H1(M) & H2(M)
Key server
102
K's
22, 38
Network
100
C 20
A 40
Authentication
server
104
M 18
S 24
14
Signing entity

FIG. 6

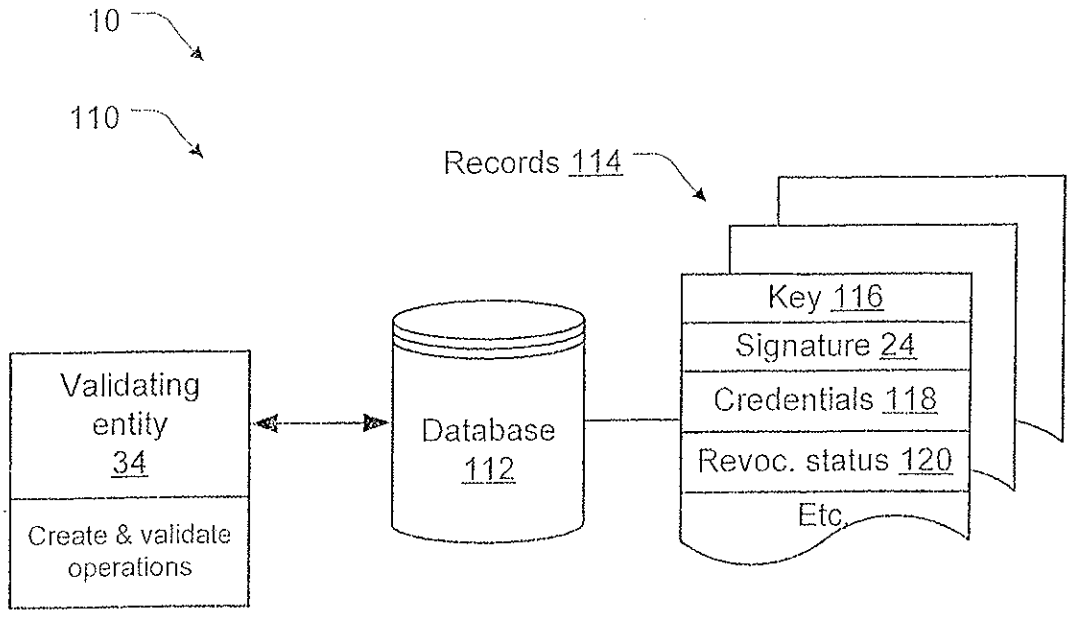

10
110
Records 114
Key 116
Signature 24
Credentials 118
Revoc. status 120
Etc.
Validating entity 34
Create & validate operations
Database 112

FIG. 7