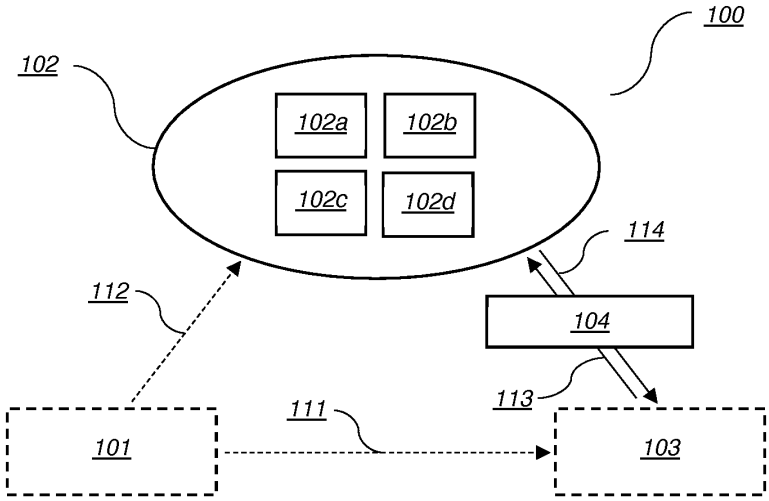



FIG. 1

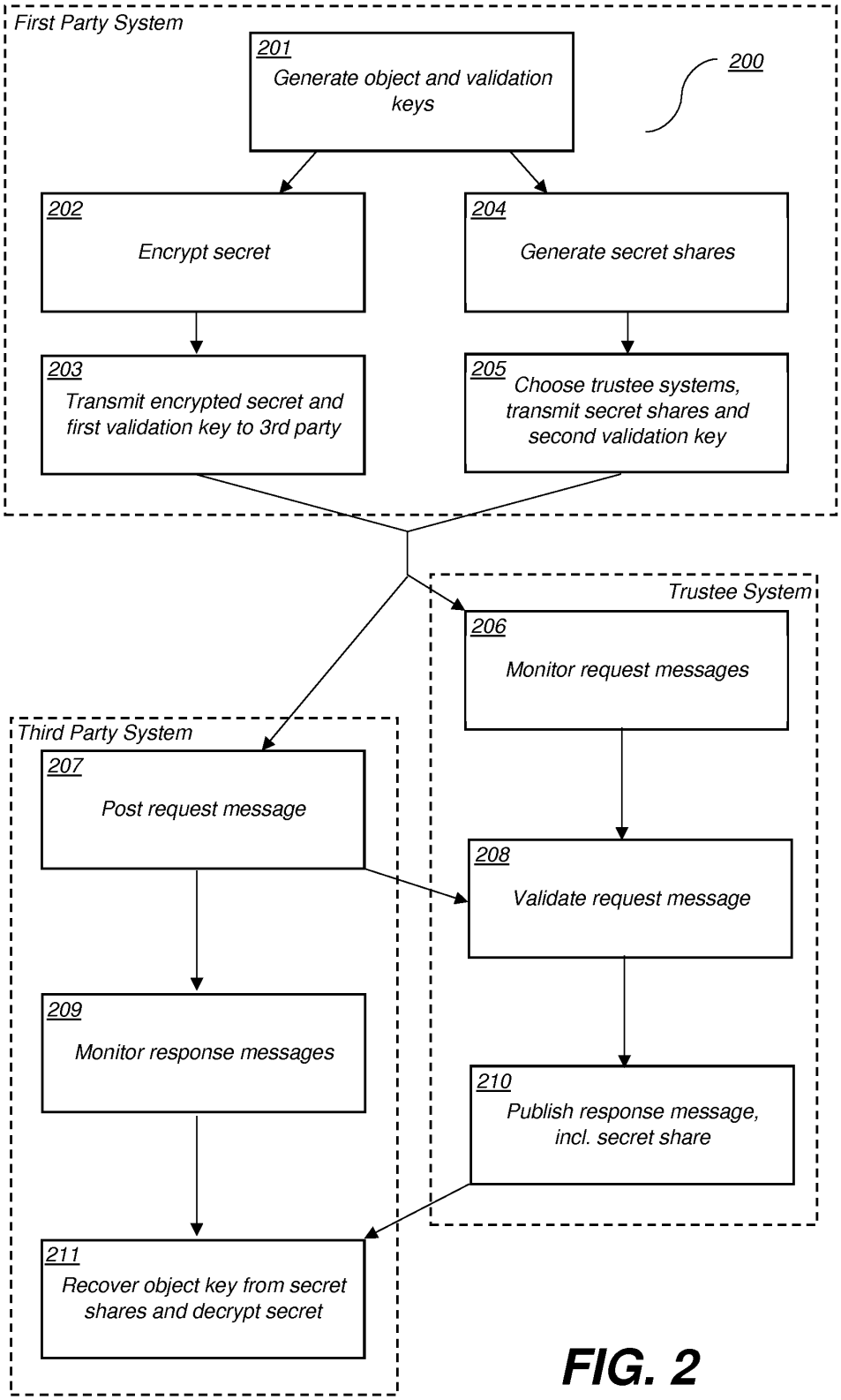
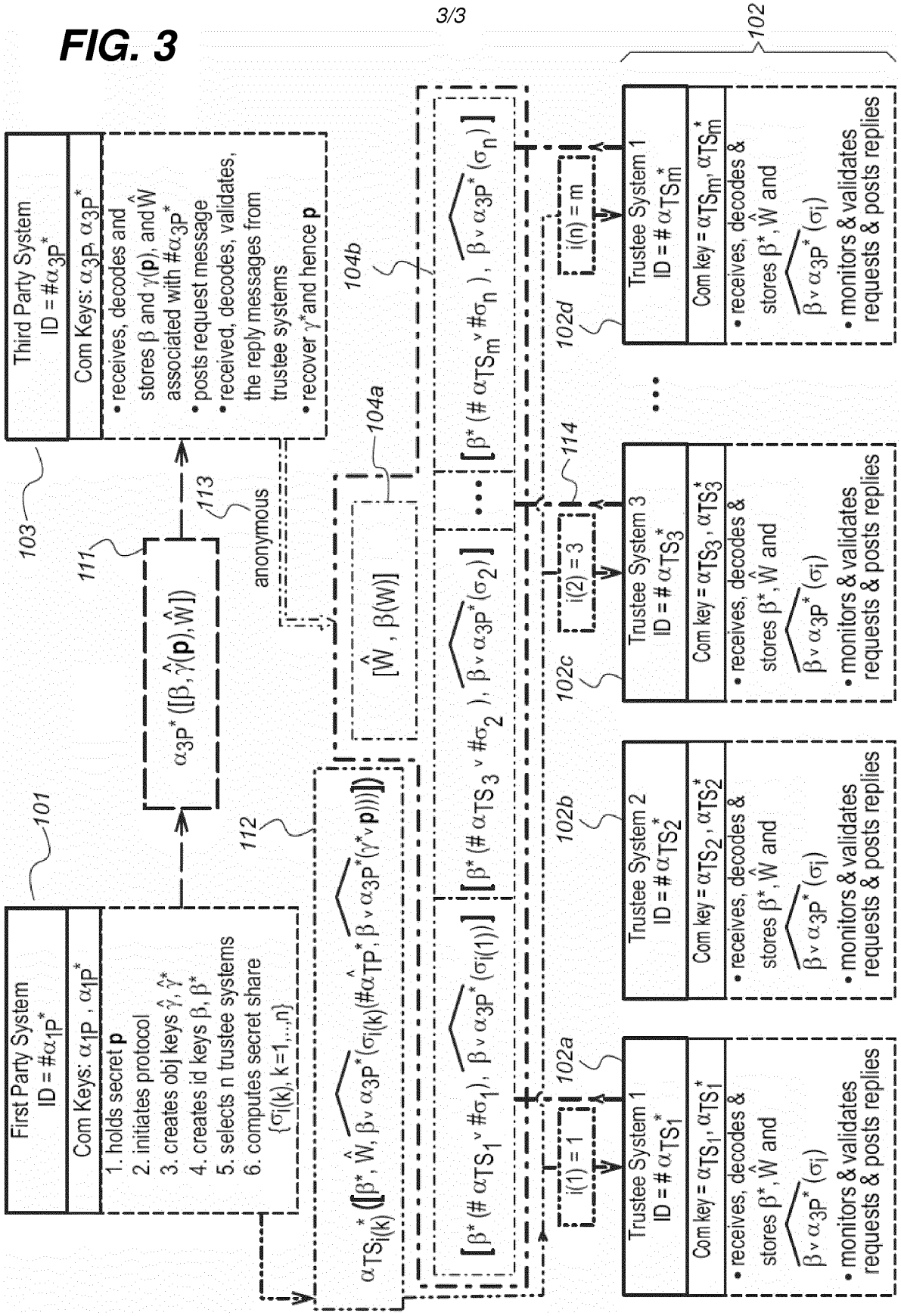

First Party System
201
Generate object and validation keys
200
202
Encrypt secret
204
Generate secret shares
203
Transmit encrypted secret and first validation key to 3rd party
205
Choose trustee systems, transmit secret shares and second validation key
Trustee System
206
Monitor request messages
Third Party System
207
Post request message
208
Validate request message
209
Monitor response messages
210
Publish response message, incl. secret share
211
Recover object key from secret shares and decrypt secret

FIG. 2

**FIG. 3**


First Party System
ID = #α1P*
Com Keys: α1P , α1P*
1. holds secret p
2. initiates protocol
3. creates obj keys γ̂, γ̂*
4. creates id keys β, β*
5. selects n trustee systems
6. computes secret share {σi(k), k=1,..,n}
101
Third Party System
ID = #α3P*
Com Keys: α3P, α3P*
• receives, decodes and stores β and γ(p), and Ŵ associated with #α3P*
• posts request message
• received, decodes, validates, the reply messages from trustee systems
• recover γ* and hence p
103
111
α3P* ([β, γ̂(p), Ŵ])
113
112
anonymous
104a
104b
[Ŵ , β(W)]
102
Trustee System 1
ID = # αTS1*
Com key = αTS1, αTS1*
• receives, decodes & stores β*, Ŵ and
• monitors & validates requests & posts replies
102a
i(1) = 1
Trustee System 2
ID = # αTS2*
Com key = αTS2 , αTS2*
102b
i(2) = 3
Trustee System 3
ID = # αTS3*
Com key = αTS3 , αTS3*
114
102c
i(n) = m
Trustee System 1
ID = # αTSm*
Com key = αTSm, αTSm*
102d