1/4

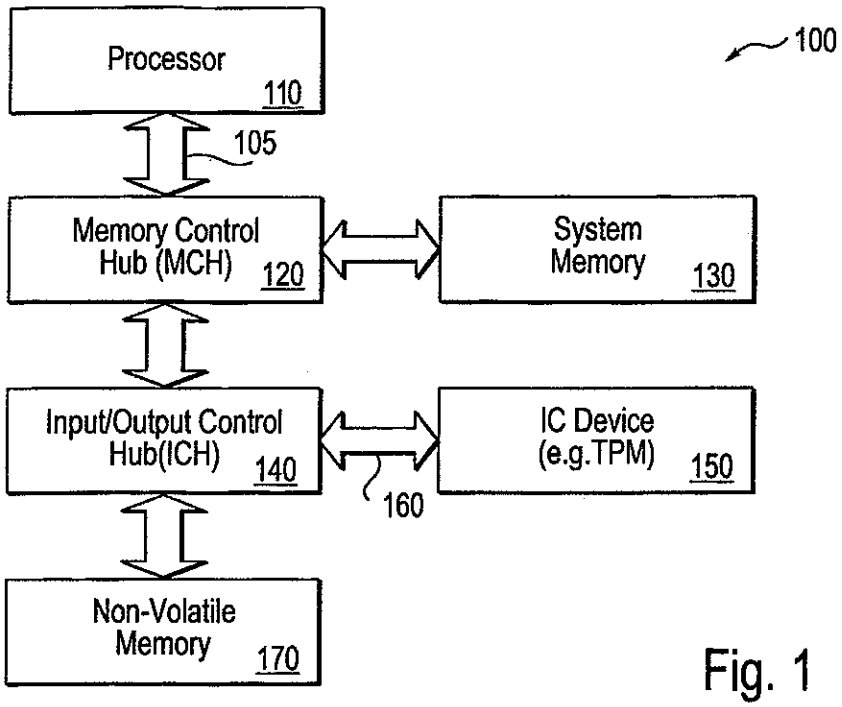

Processor
110
100
105
Memory Control
Hub (MCH)
120
System
Memory
130
Input/Output Control
Hub(ICH)
140
IC Device
(e.g.TPM)
150
160
Non-Volatile
Memory
170

Fig. 1

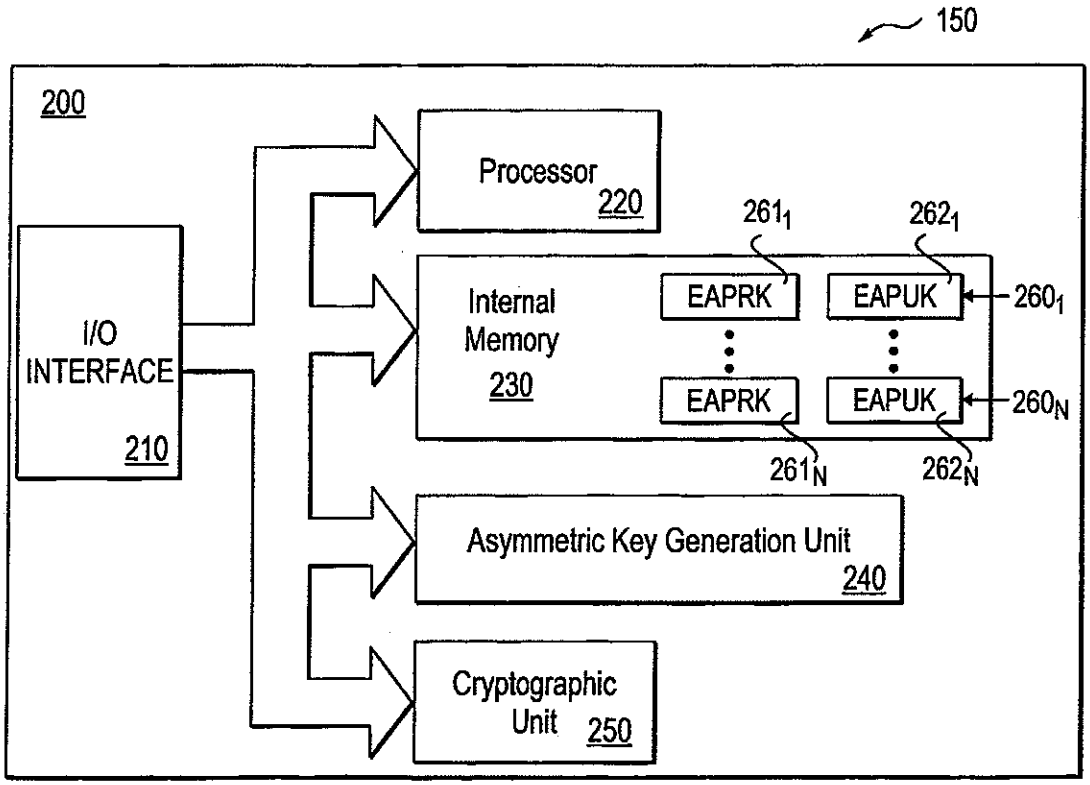

150
200
Processor
220
I/O
INTERFACE
210
Internal
Memory
230
261_1
262_1
EAPRK
EAPUK
260_1
EAPRK
EAPUK
260_N
261_N
262_N
Asymmetric Key Generation Unit
240
Cryptographic
Unit
250

Fig. 2

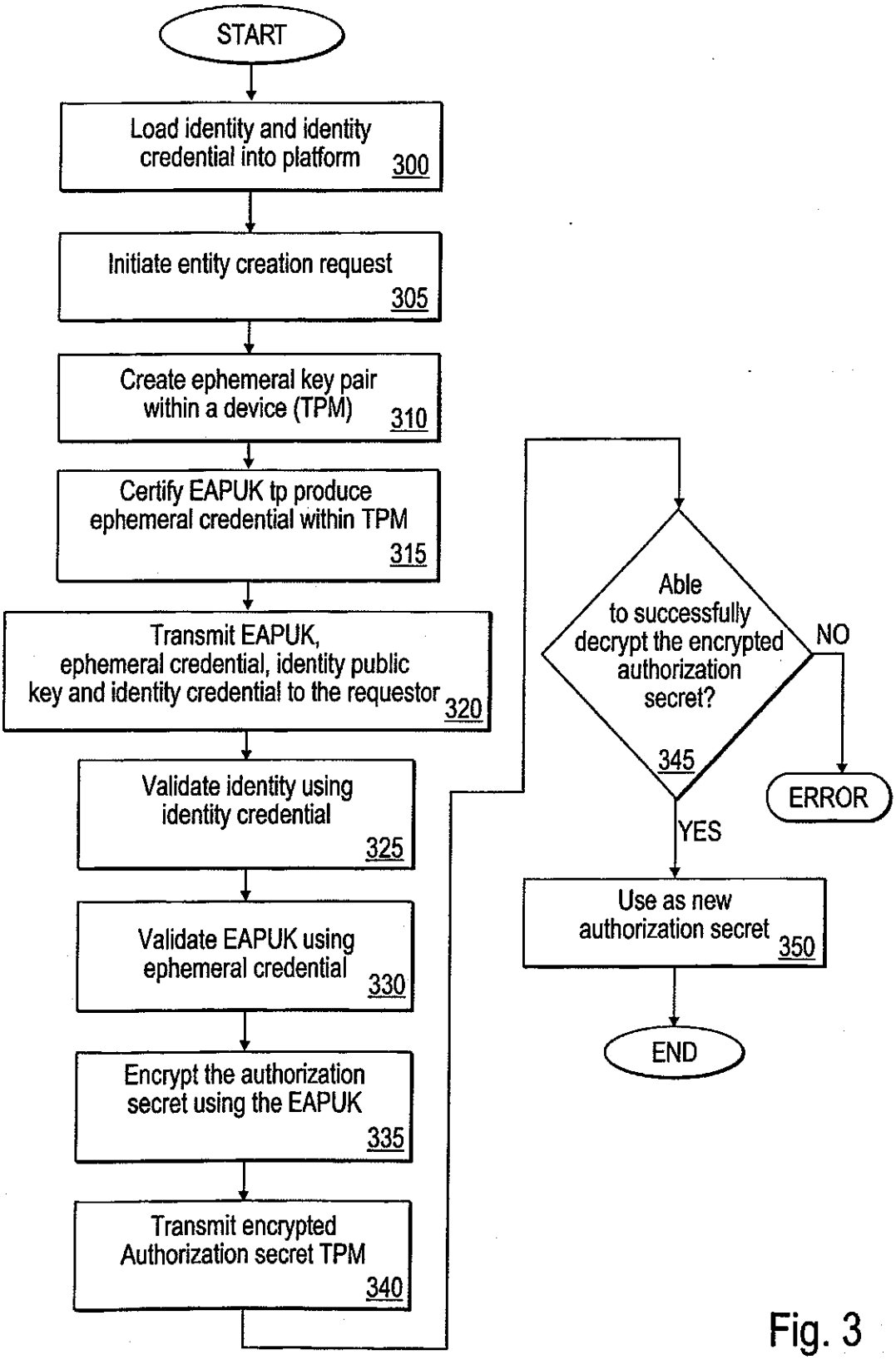

START
Load identity and identity credential into platform 300
Initiate entity creation request 305
Create ephemeral key pair within a device (TPM) 310
Certify EAPUK tp produce ephemeral credential within TPM 315
Transmit EAPUK, ephemeral credential, identity public key and identity credential to the requestor 320
Validate identity using identity credential 325
Validate EAPUK using ephemeral credential 330
Encrypt the authorization secret using the EAPUK 335
Transmit encrypted Authorization secret TPM 340
Able to successfully decrypt the encrypted authorization secret? 345
NO
ERROR
YES
Use as new authorization secret 350
END

Fig. 3

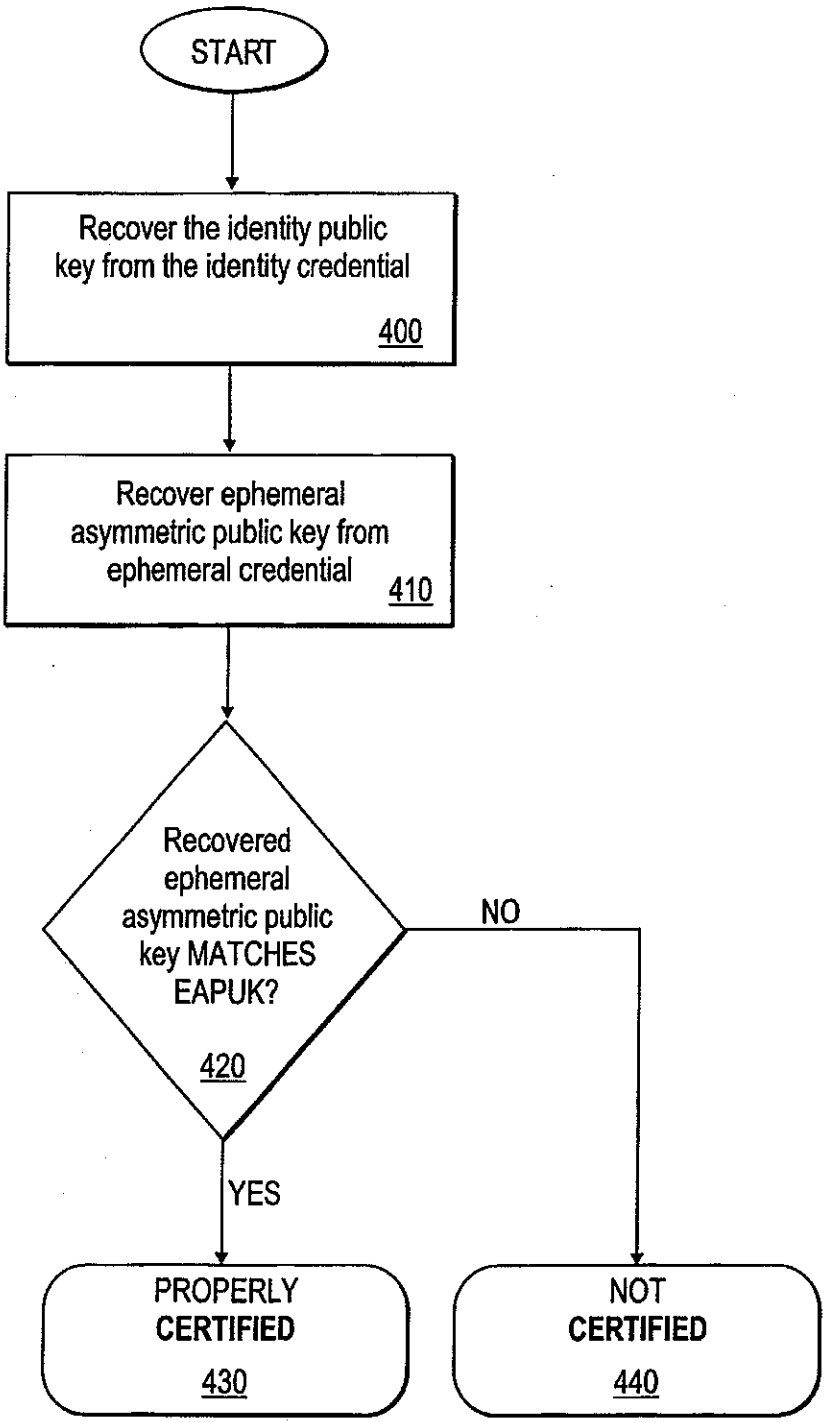

START
Recover the identity public key from the identity credential
400
Recover ephemeral asymmetric public key from ephemeral credential
410
Recovered ephemeral asymmetric public key MATCHES EAPUK?
420
NO
YES
PROPERLY CERTIFIED
430
NOT CERTIFIED
440

Fig. 4

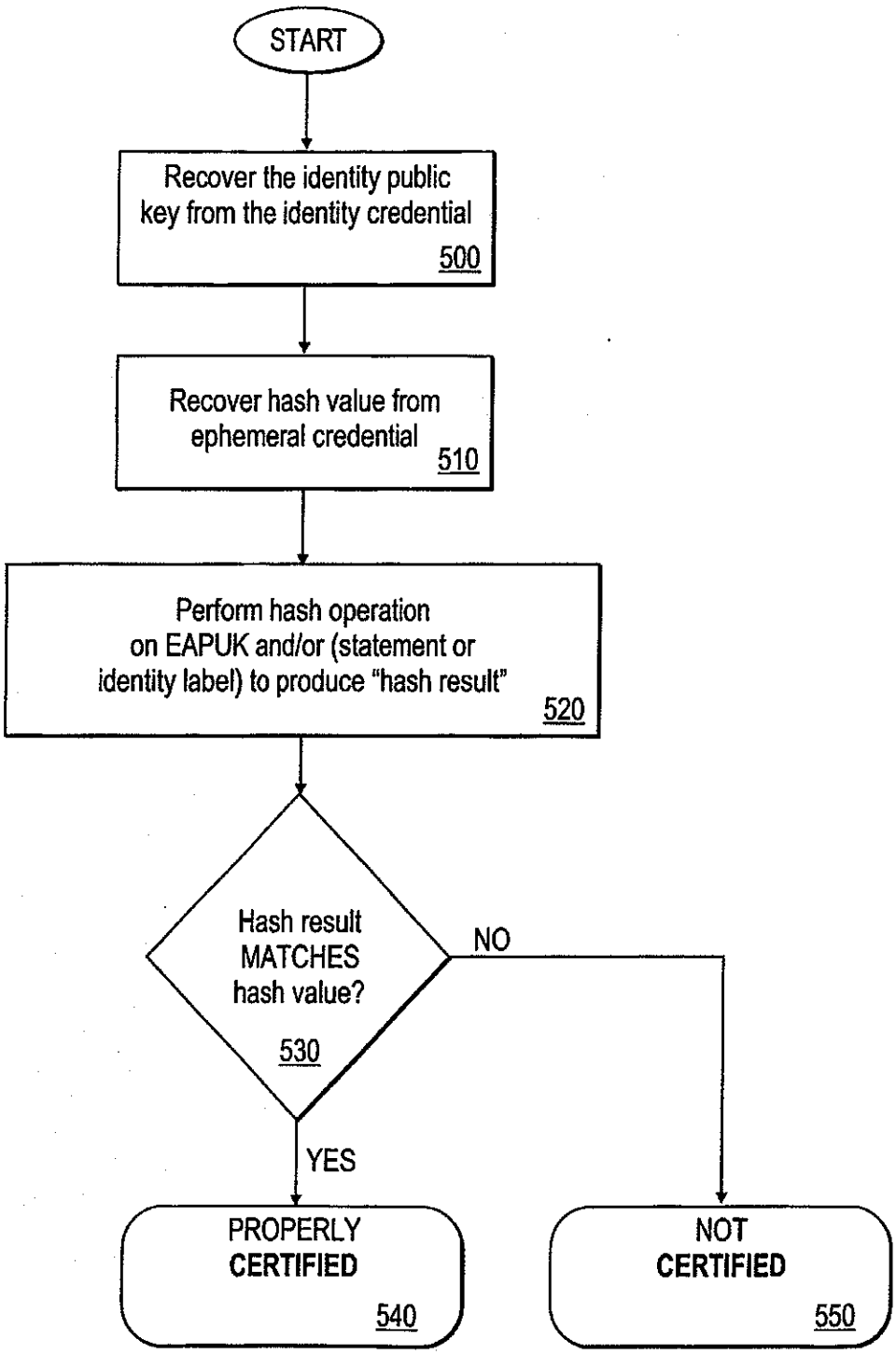

START
Recover the identity public key from the identity credential
500
Recover hash value from ephemeral credential
510
Perform hash operation on EAPUK and/or (statement or identity label) to produce "hash result"
520
Hash result MATCHES hash value?
530
NO
YES
PROPERLY CERTIFIED
540
NOT CERTIFIED
550

Fig. 5