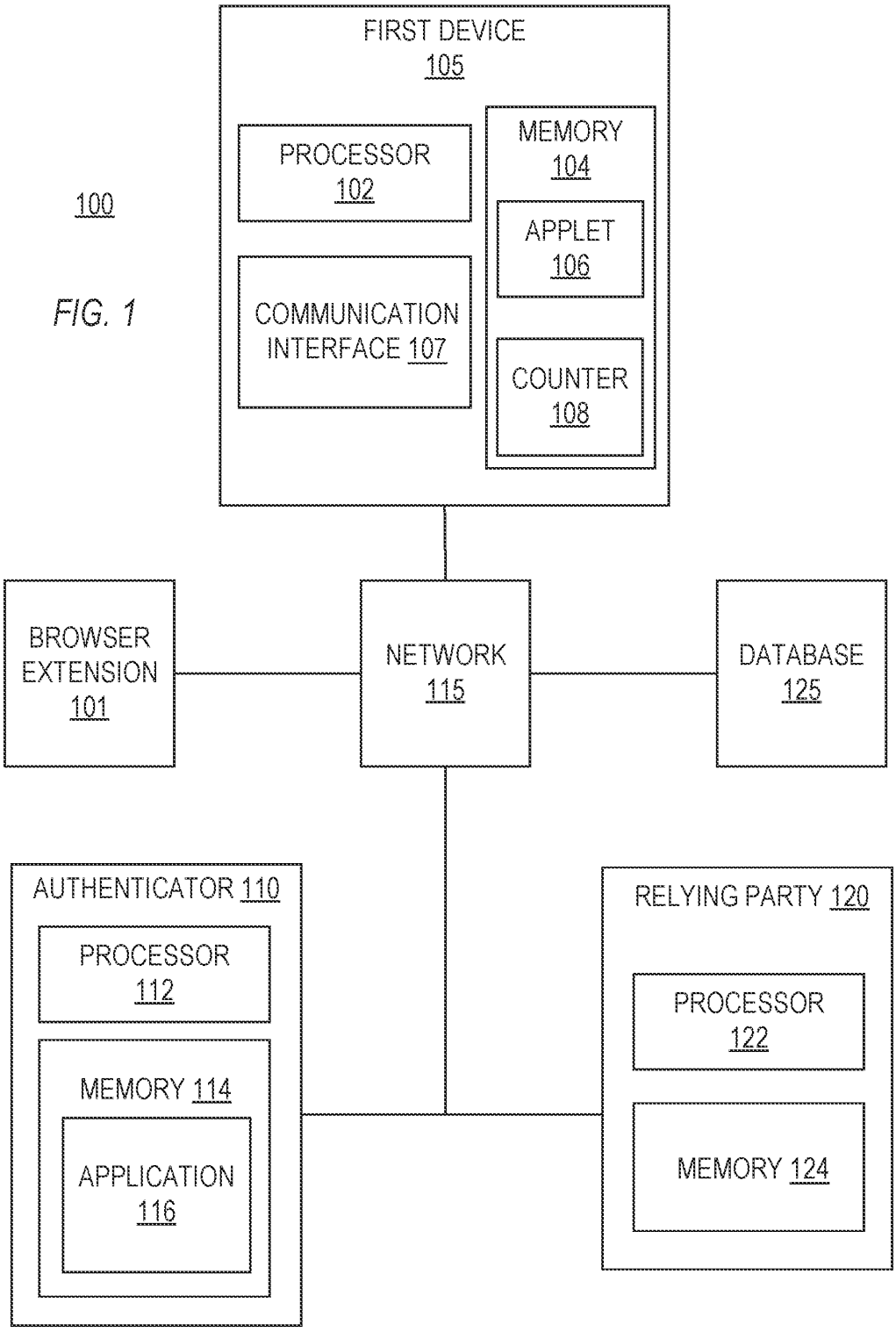
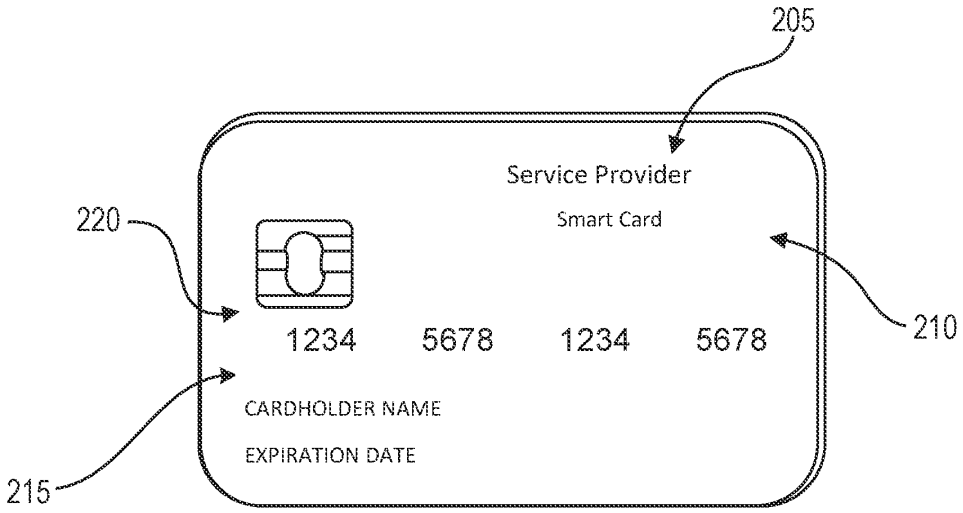

100
FIRST DEVICE
105
PROCESSOR
102
MEMORY
104
APPLET
106
COMMUNICATION
INTERFACE 107
COUNTER
108
BROWSER
EXTENSION
101
NETWORK
115
DATABASE
125
AUTHENTICATOR 110
PROCESSOR
112
MEMORY 114
APPLICATION
116
RELYING PARTY 120
PROCESSOR
122
MEMORY 124

FIG. 1


205
Service Provider
Smart Card
220
1234 5678 1234 5678
210
CARDHOLDER NAME
EXPIRATION DATE
215

200

FIG. 2A

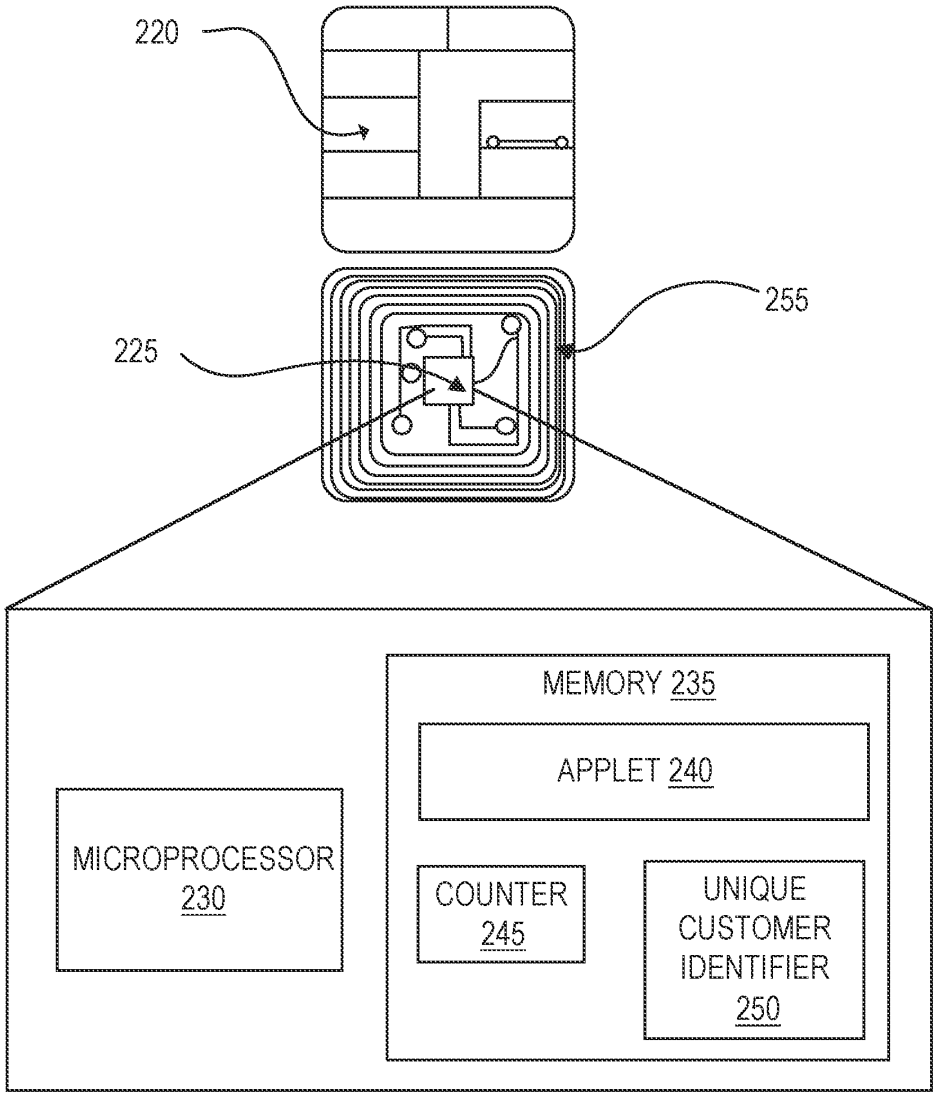
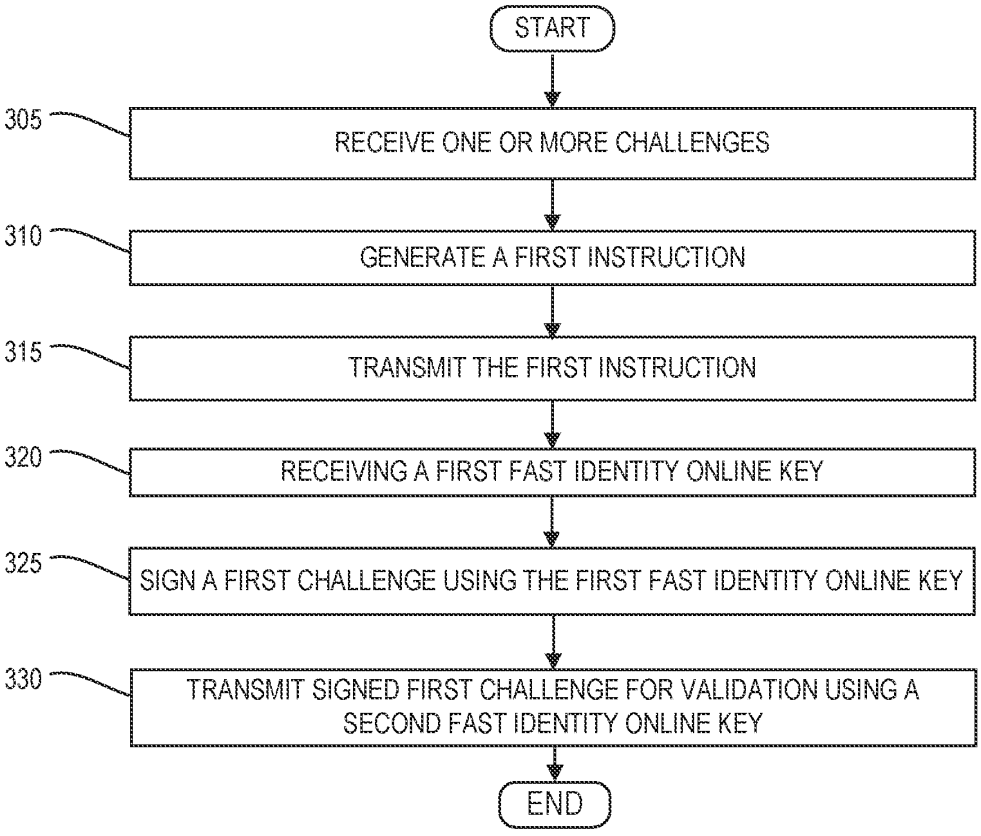

220
225
255
MEMORY 235
APPLET 240
MICROPROCESSOR 230
COUNTER 245
UNIQUE CUSTOMER IDENTIFIER 250

FIG. 2B


START
305
RECEIVE ONE OR MORE CHALLENGES
310
GENERATE A FIRST INSTRUCTION
315
TRANSMIT THE FIRST INSTRUCTION
320
RECEIVING A FIRST FAST IDENTITY ONLINE KEY
325
SIGN A FIRST CHALLENGE USING THE FIRST FAST IDENTITY ONLINE KEY
330
TRANSMIT SIGNED FIRST CHALLENGE FOR VALIDATION USING A SECOND FAST IDENTITY ONLINE KEY
END

300

FIG. 3

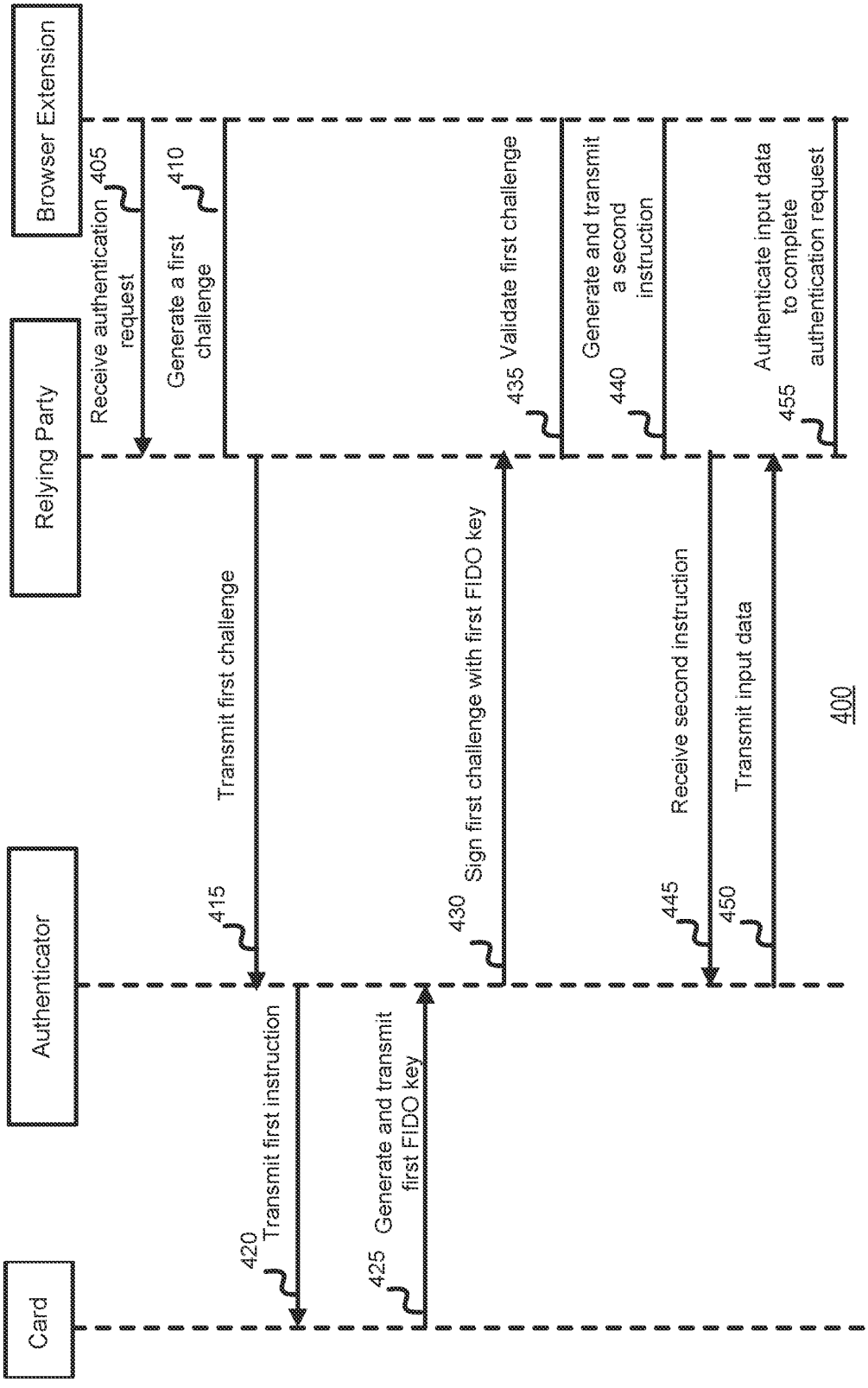

Card
Authenticator
Relying Party
Browser Extension
Receive authentication request
405
Generate a first challenge
410
Transmit first challenge
415
Transmit first instruction
420
Generate and transmit first FIDO key
425
Sign first challenge with first FIDO key
430
Validate first challenge
435
Generate and transmit a second instruction
440
Receive second instruction
445
Transmit input data
450
Authenticate input data to complete authentication request
455
400

FIG. 4

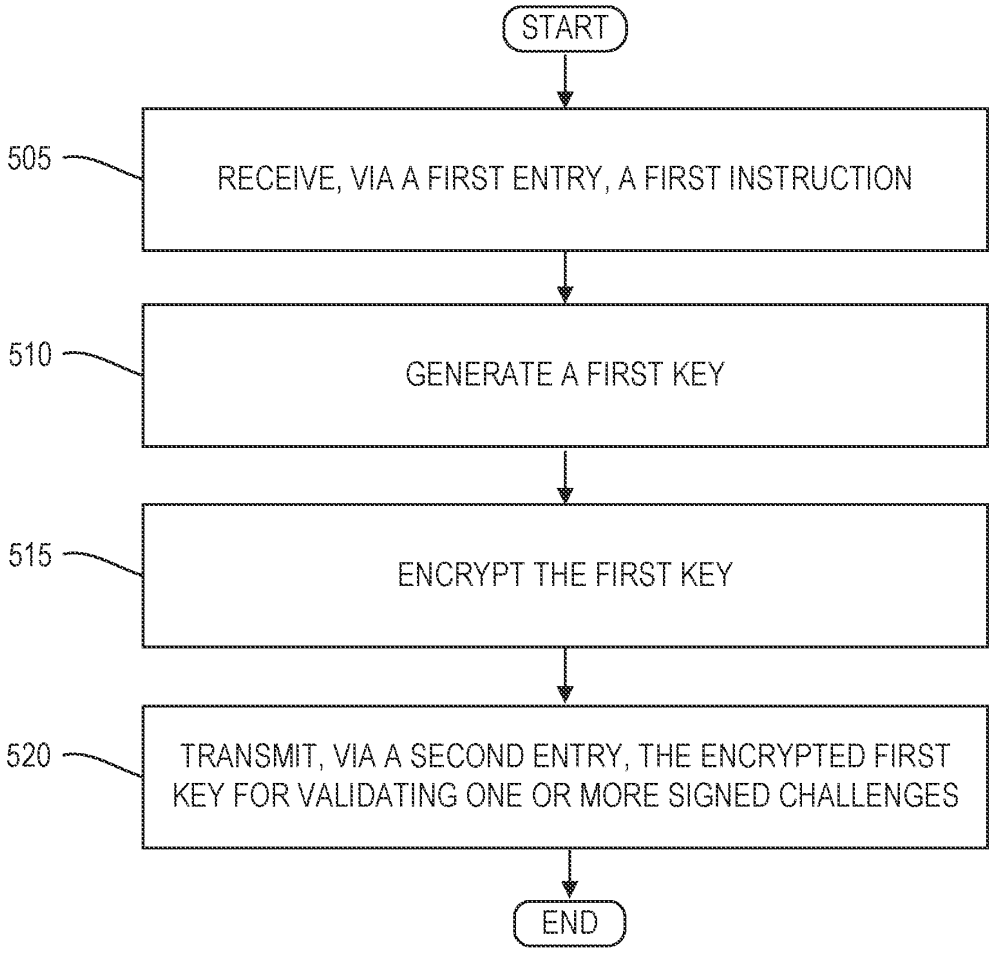
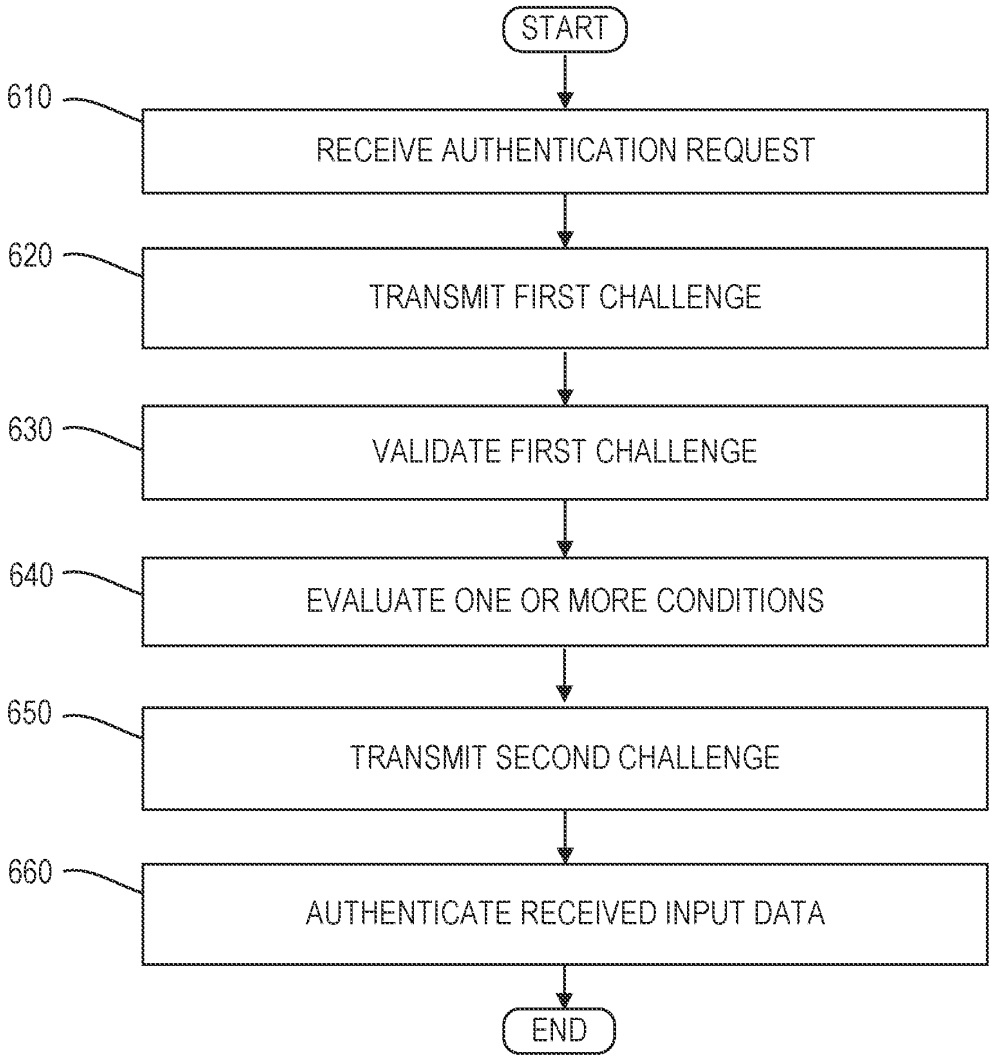

START
505
RECEIVE, VIA A FIRST ENTRY, A FIRST INSTRUCTION
510
GENERATE A FIRST KEY
515
ENCRYPT THE FIRST KEY
520
TRANSMIT, VIA A SECOND ENTRY, THE ENCRYPTED FIRST KEY FOR VALIDATING ONE OR MORE SIGNED CHALLENGES
END
500

FIG. 5


START
610
RECEIVE AUTHENTICATION REQUEST
620
TRANSMIT FIRST CHALLENGE
630
VALIDATE FIRST CHALLENGE
640
EVALUATE ONE OR MORE CONDITIONS
650
TRANSMIT SECOND CHALLENGE
660
AUTHENTICATE RECEIVED INPUT DATA
END

600

FIG. 6