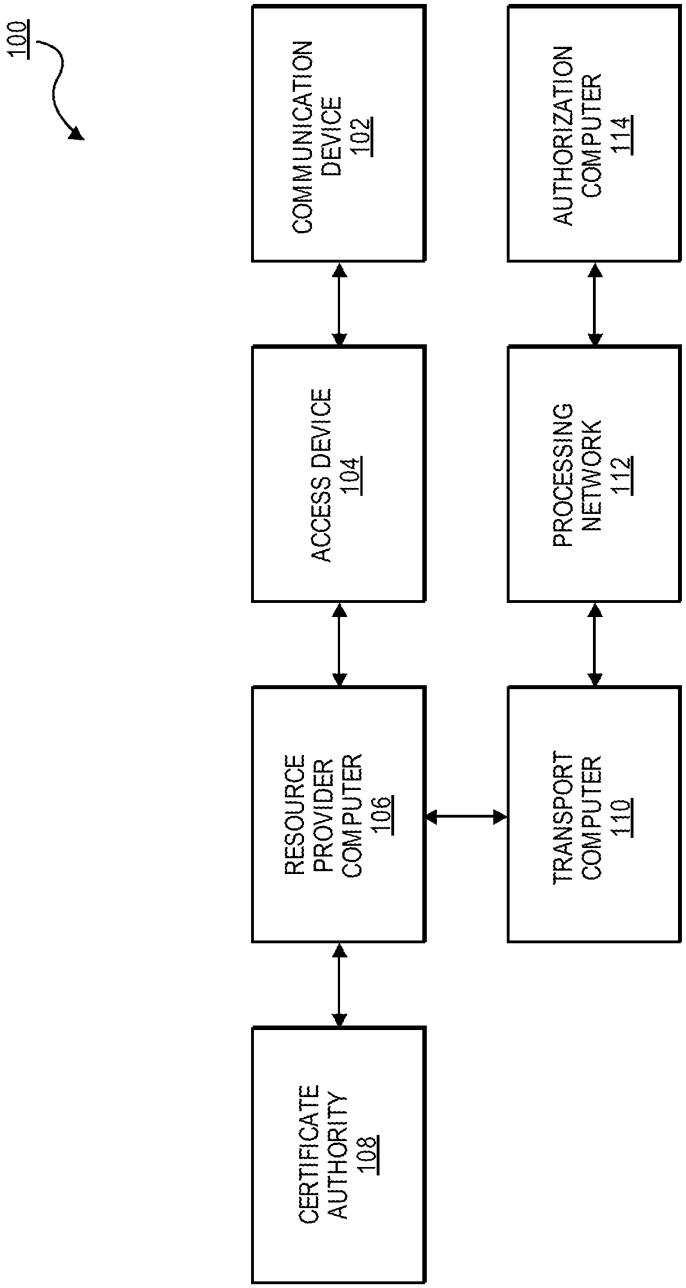
100
COMMUNICATION DEVICE 102
AUTHORIZATION COMPUTER 114
ACCESS DEVICE 104
PROCESSING NETWORK 112
RESOURCE PROVIDER COMPUTER 106
TRANSPORT COMPUTER 110
CERTIFICATE AUTHORITY 108

FIG. 1

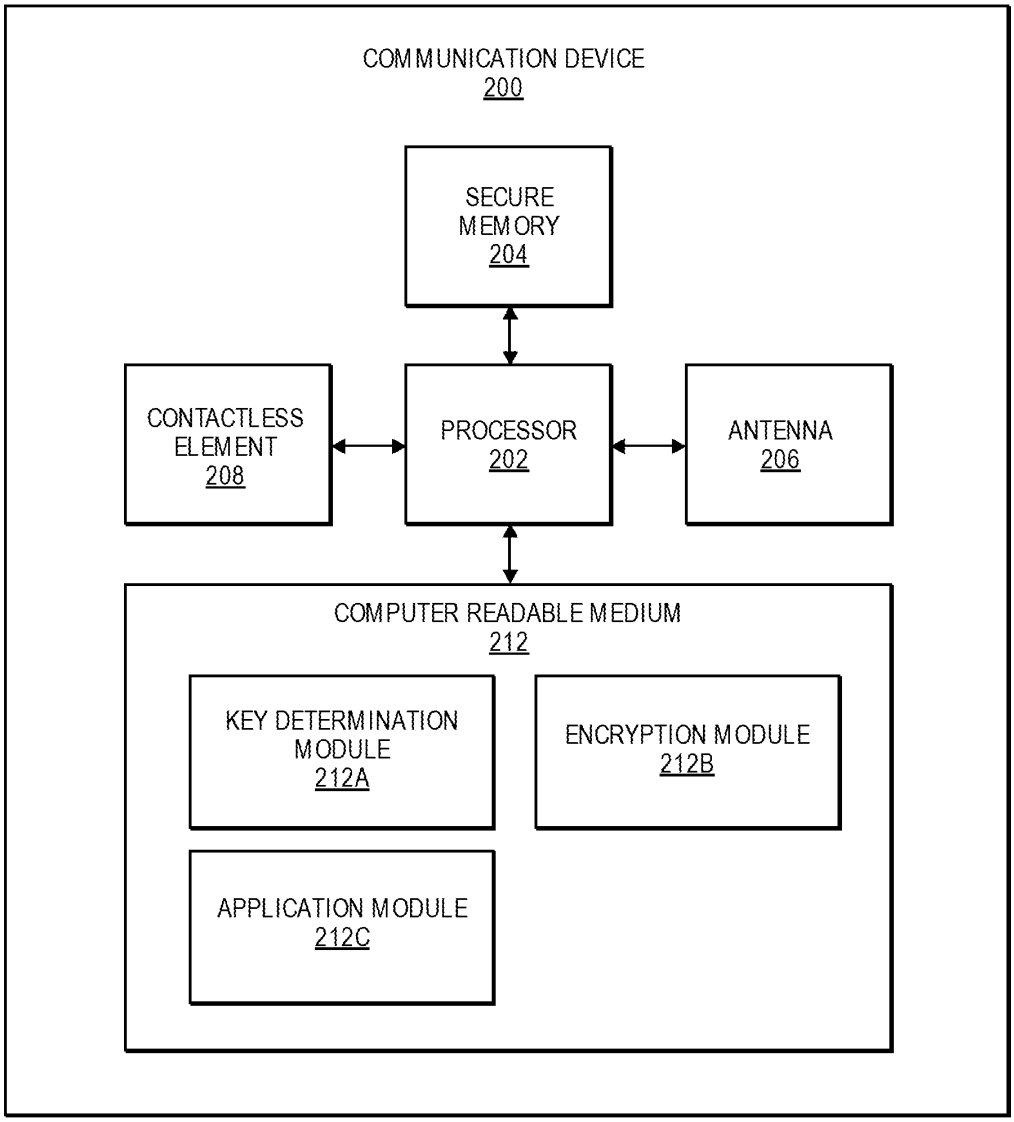
COMMUNICATION DEVICE
200
SECURE MEMORY
204
CONTACTLESS ELEMENT
208
PROCESSOR
202
ANTENNA
206
COMPUTER READABLE MEDIUM
212
KEY DETERMINATION MODULE
212A
ENCRYPTION MODULE
212B
APPLICATION MODULE
212C

FIG. 2

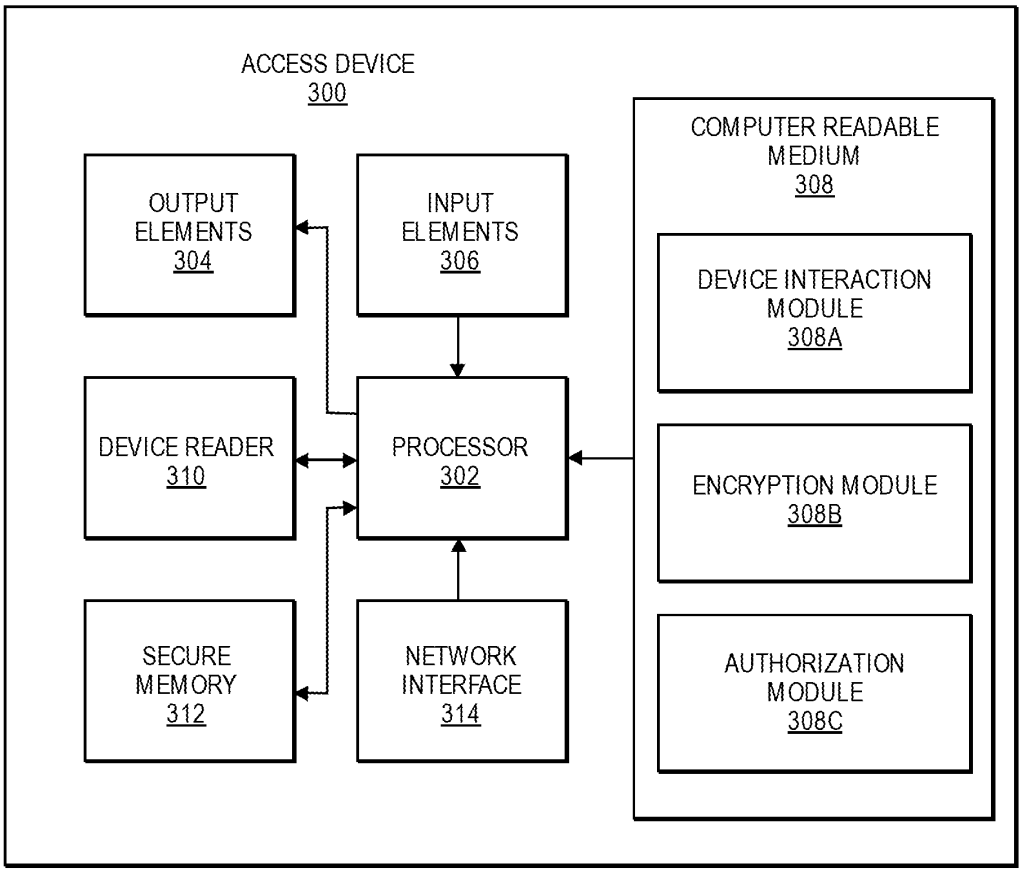
ACCESS DEVICE
300
OUTPUT ELEMENTS
304
INPUT ELEMENTS
306
DEVICE READER
310
PROCESSOR
302
SECURE MEMORY
312
NETWORK INTERFACE
314
COMPUTER READABLE MEDIUM
308
DEVICE INTERACTION MODULE
308A
ENCRYPTION MODULE
308B
AUTHORIZATION MODULE
308C

FIG. 3

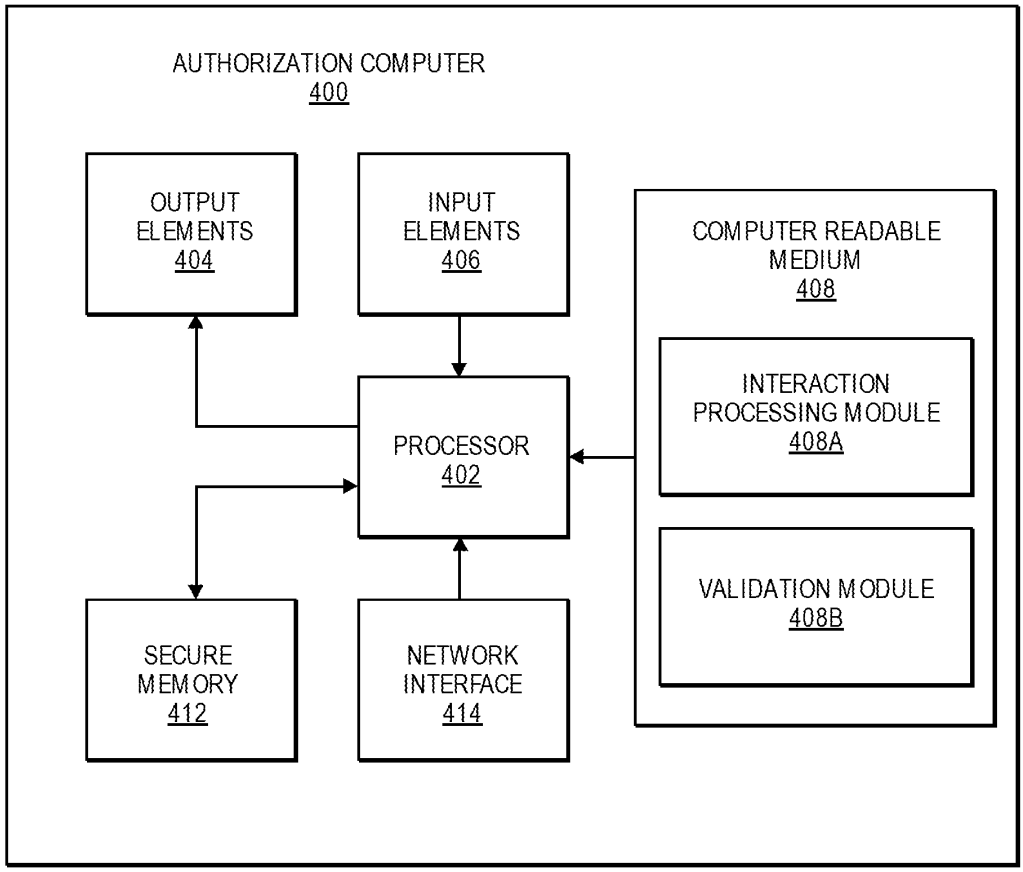
AUTHORIZATION COMPUTER
400
OUTPUT ELEMENTS
404
INPUT ELEMENTS
406
COMPUTER READABLE MEDIUM
408
INTERACTION PROCESSING MODULE
408A
PROCESSOR
402
VALIDATION MODULE
408B
SECURE MEMORY
412
NETWORK INTERFACE
414

FIG. 4

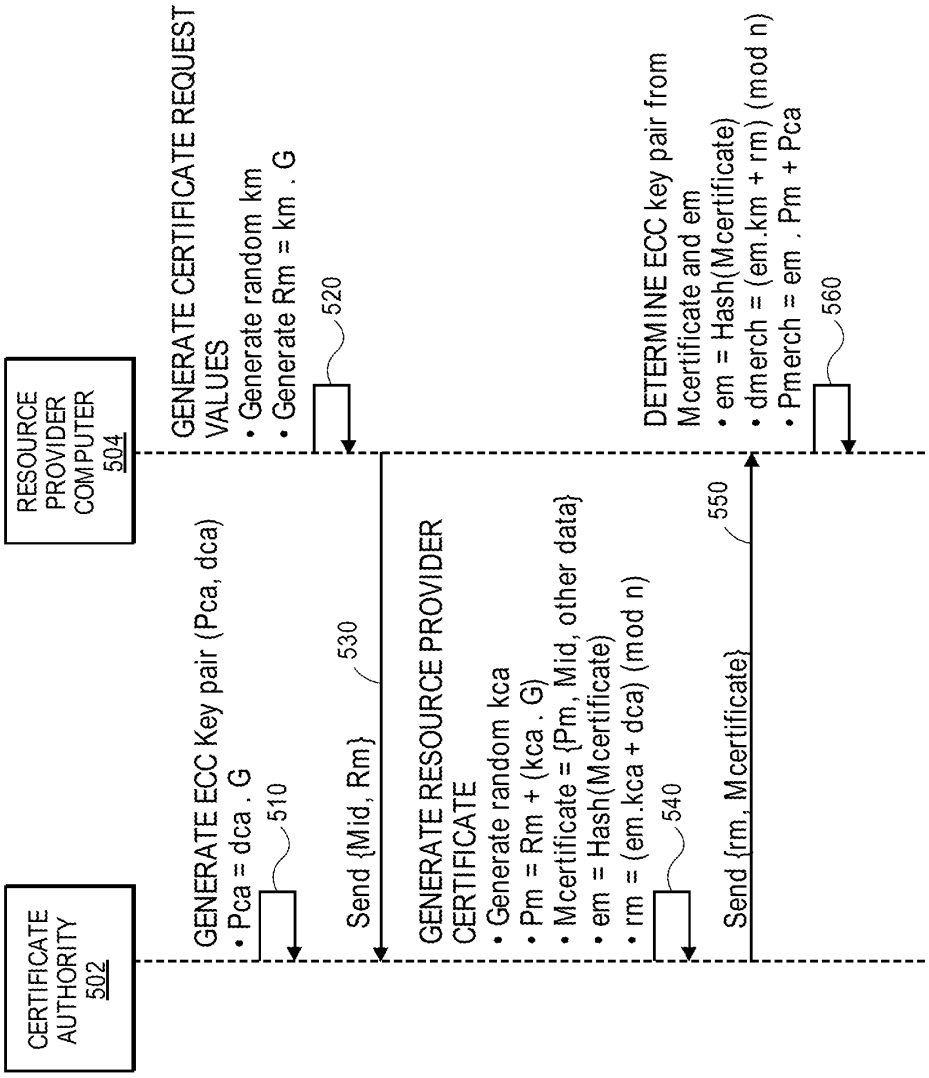
CERTIFICATE AUTHORITY 502
RESOURCE PROVIDER COMPUTER 504
GENERATE ECC Key pair (Pca, dca)
• Pca = dca . G
510
GENERATE CERTIFICATE REQUEST VALUES
• Generate random km
• Generate Rm = km . G
520
Send {Mid, Rm}
530
GENERATE RESOURCE PROVIDER CERTIFICATE
• Generate random kca
• Pm = Rm + (kca . G)
• Mcertificate = {Pm, Mid, other data}
• em = Hash(Mcertificate)
• rm = (em.kca + dca) (mod n)
540
Send {rm, Mcertificate}
550
DETERMINE ECC key pair from Mcertificate and em
• em = Hash(Mcertificate)
• dmerch = (em.km + rm) (mod n)
• Pmerch = em . Pm + Pca
560

FIG. 5

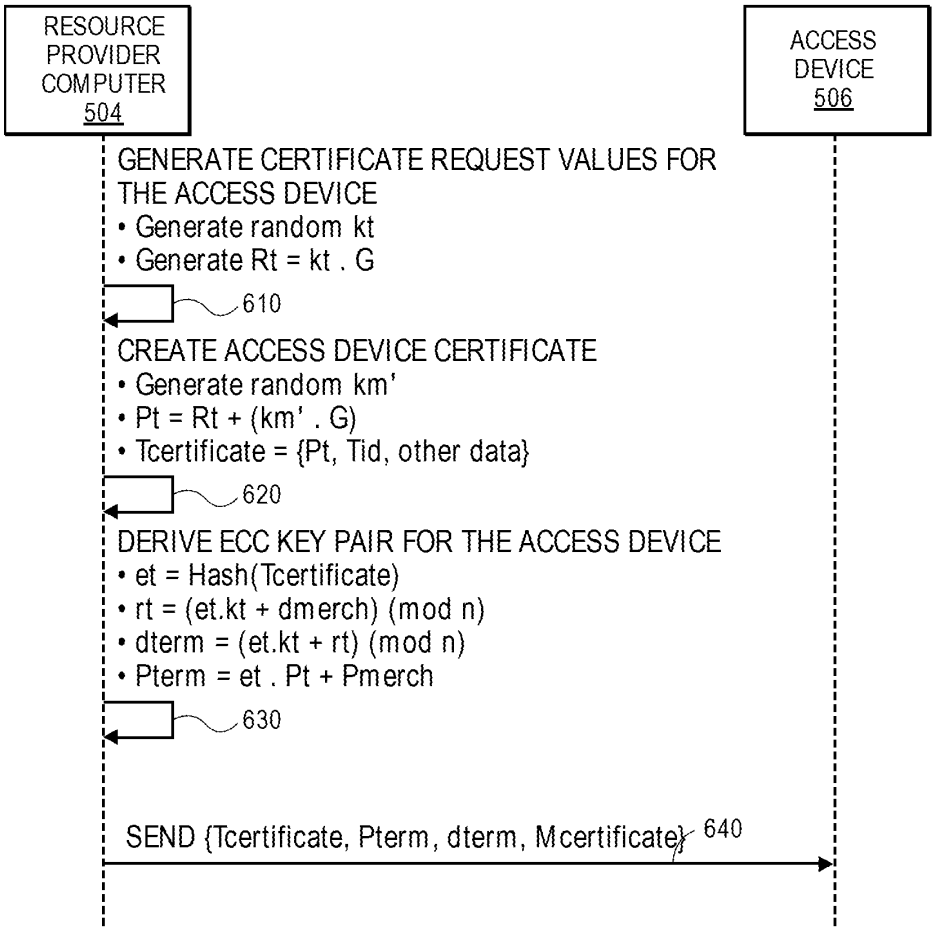
RESOURCE PROVIDER COMPUTER 504
ACCESS DEVICE 506
GENERATE CERTIFICATE REQUEST VALUES FOR THE ACCESS DEVICE
• Generate random kt
• Generate Rt = kt . G
610
CREATE ACCESS DEVICE CERTIFICATE
• Generate random km'
• Pt = Rt + (km' . G)
• Tcertificate = {Pt, Tid, other data}
620
DERIVE ECC KEY PAIR FOR THE ACCESS DEVICE
• et = Hash(Tcertificate)
• rt = (et.kt + dmerch) (mod n)
• dterm = (et.kt + rt) (mod n)
• Pterm = et . Pt + Pmerch
630
SEND {Tcertificate, Pterm, dterm, Mcertificate}
640

FIG. 6

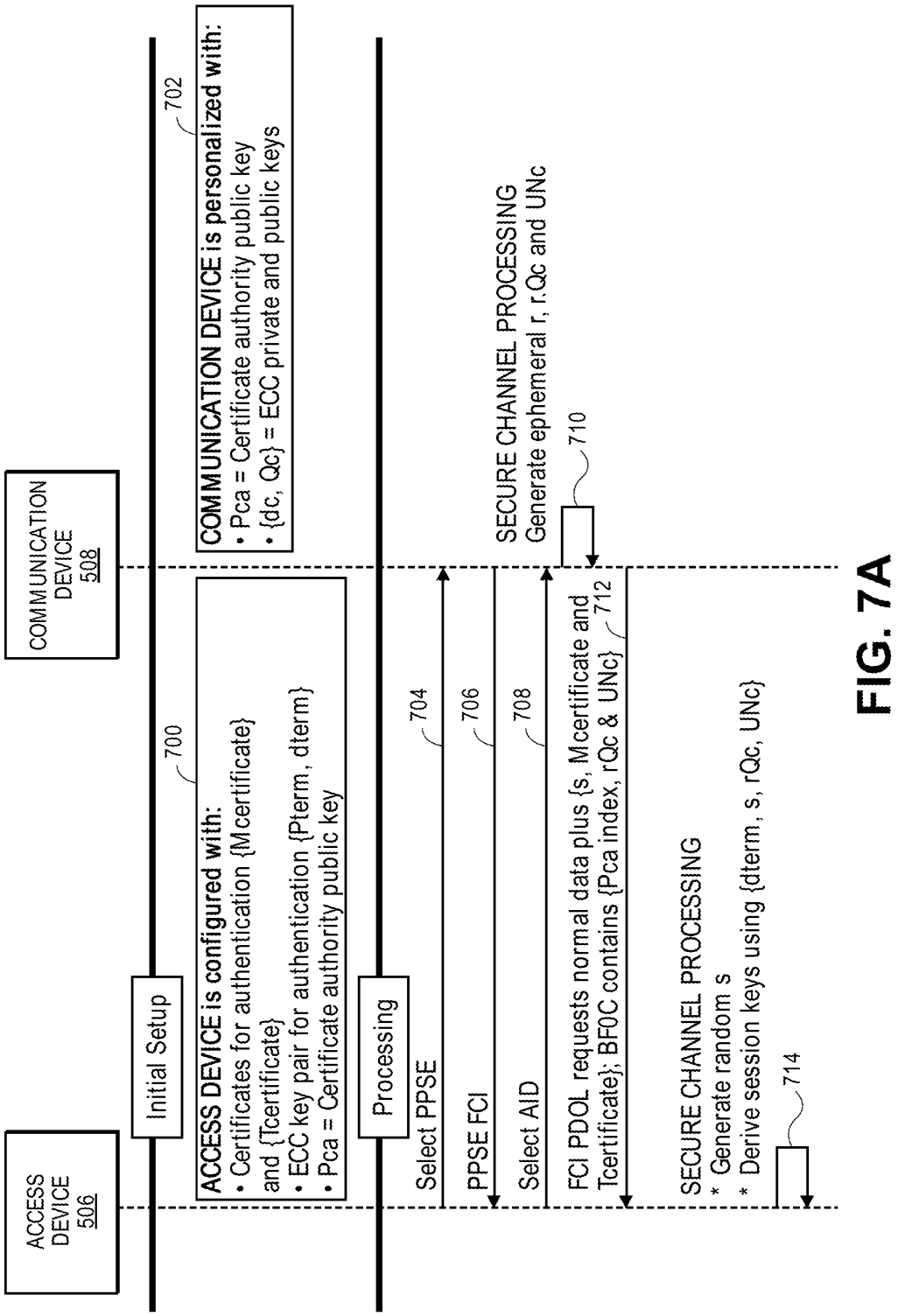
ACCESS DEVICE 506
COMMUNICATION DEVICE 508
Initial Setup
700
ACCESS DEVICE is configured with:
• Certificates for authentication {Mcertificate} and {Tcertificate}
• ECC key pair for authentication {Pterm, dterm}
• Pca = Certificate authority public key
702
COMMUNICATION DEVICE is personalized with:
• Pca = Certificate authority public key
• {dc, Qc} = ECC private and public keys
Processing
704
Select PPSE
706
PPSE FCI
708
Select AID
710
SECURE CHANNEL PROCESSING
Generate ephemeral r, r.Qc and UNc
712
FCI PDOL requests normal data plus {s, Mcertificate and Tcertificate}; BF0C contains {Pca index, rQc & UNc}
SECURE CHANNEL PROCESSING
* Generate random s
* Derive session keys using {dterm, s, rQc, UNc}
714

FIG. 7A

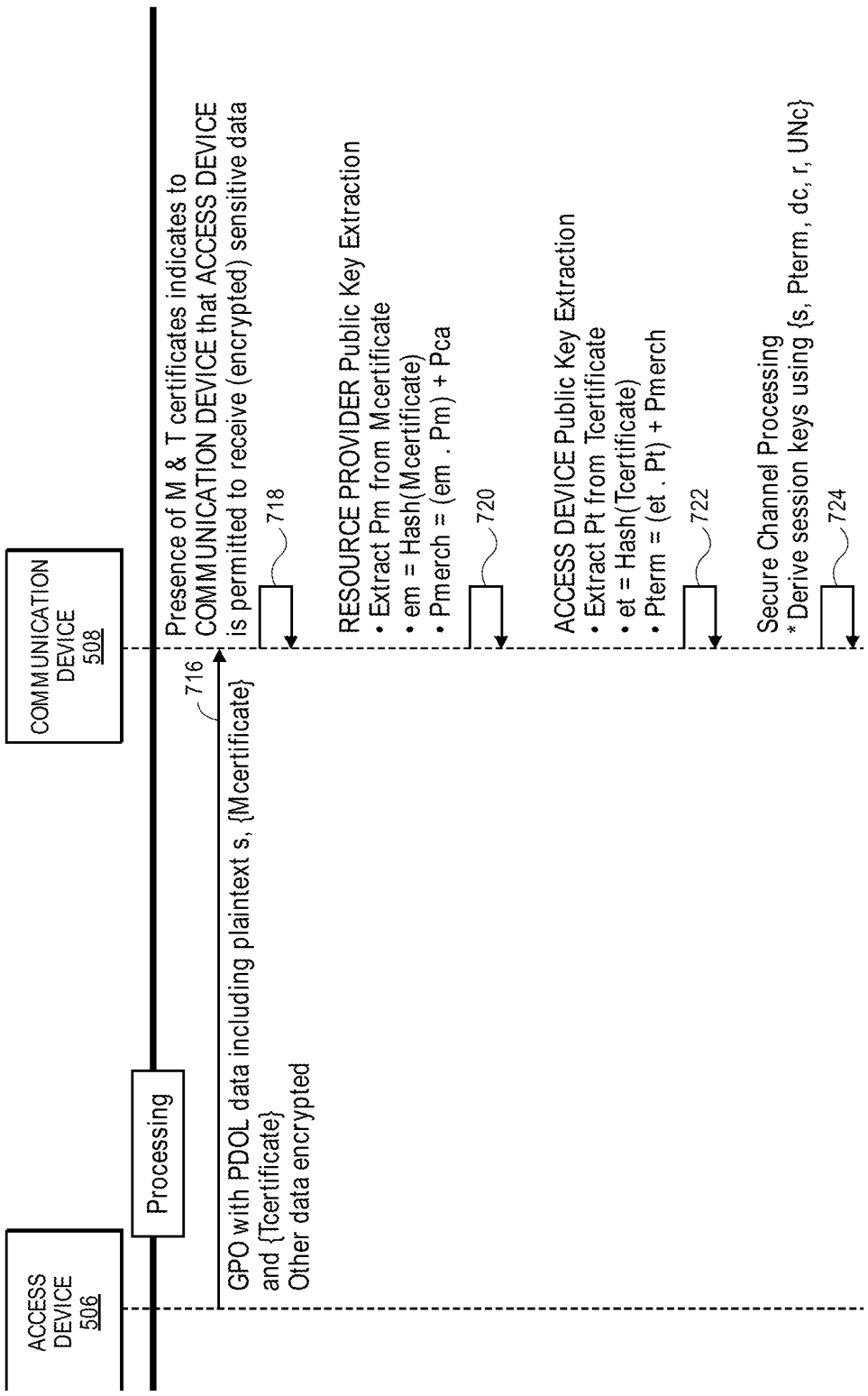
ACCESS DEVICE 506
Processing
COMMUNICATION DEVICE 508
716
GPO with PDOL data including plaintext s, {Mcertificate} and {Tcertificate}
Other data encrypted
Presence of M & T certificates indicates to COMMUNICATION DEVICE that ACCESS DEVICE is permitted to receive (encrypted) sensitive data
718
RESOURCE PROVIDER Public Key Extraction
• Extract Pm from Mcertificate
• em = Hash(Mcertificate)
• Pmerch = (em . Pm) + Pca
720
ACCESS DEVICE Public Key Extraction
• Extract Pt from Tcertificate
• et = Hash(Tcertificate)
• Pterm = (et . Pt) + Pmerch
722
Secure Channel Processing
* Derive session keys using {s, Pterm, dc, r, UNc}
724

FIG. 7B

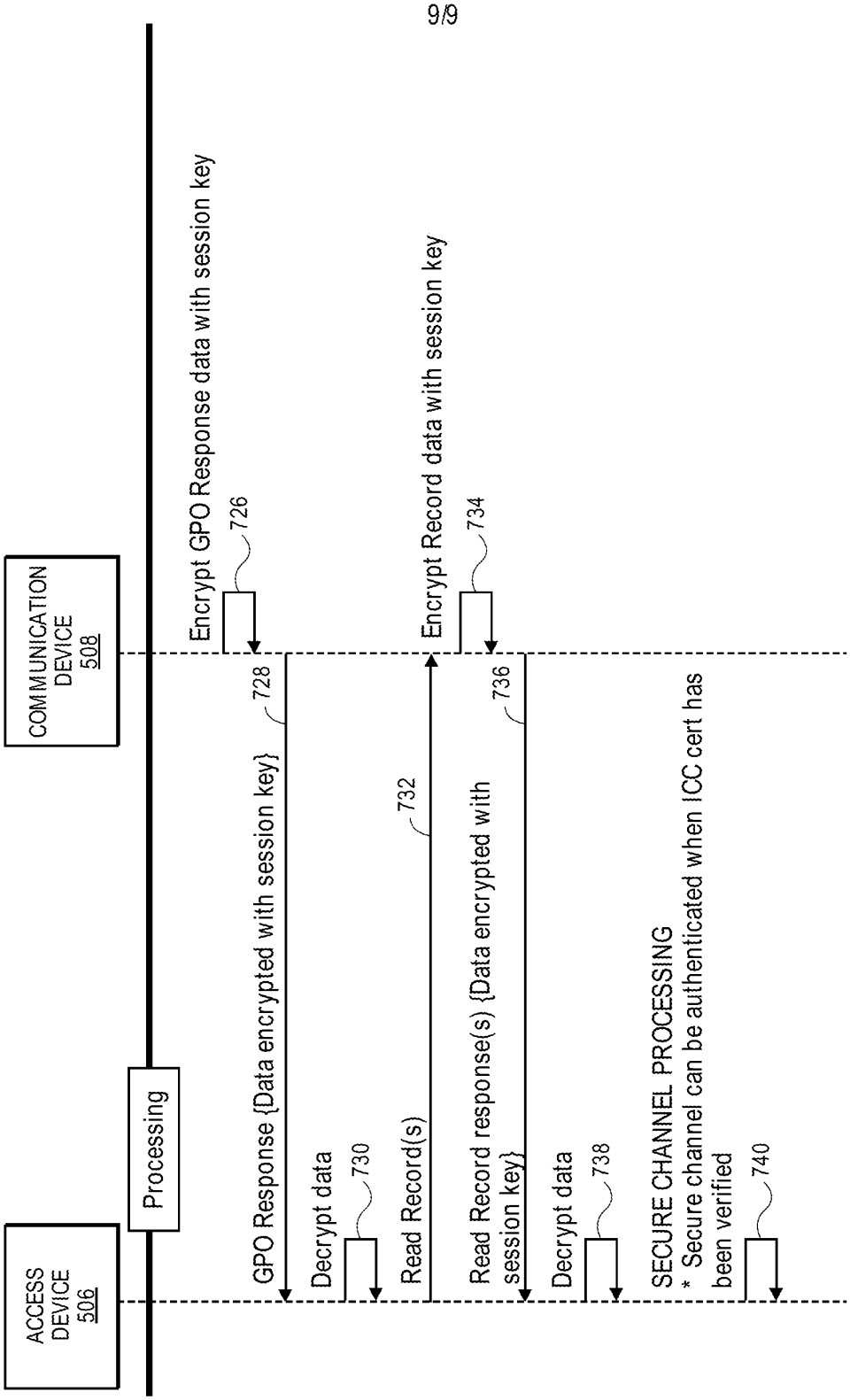
ACCESS DEVICE 506
Processing
COMMUNICATION DEVICE 508
Encrypt GPO Response data with session key
726
GPO Response {Data encrypted with session key}
728
Decrypt data
730
Read Record(s)
732
Encrypt Record data with session key
734
Read Record response(s) {Data encrypted with session key}
736
Decrypt data
738
SECURE CHANNEL PROCESSING
* Secure channel can be authenticated when ICC cert has been verified
740

FIG. 7C