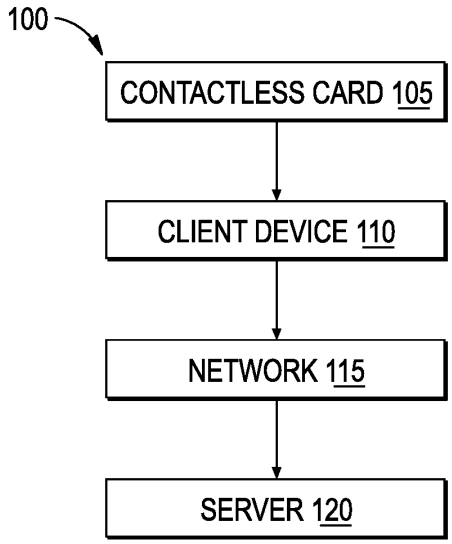

100
CONTACTLESS CARD 105
CLIENT DEVICE 110
NETWORK 115
SERVER 120

FIG. 1A

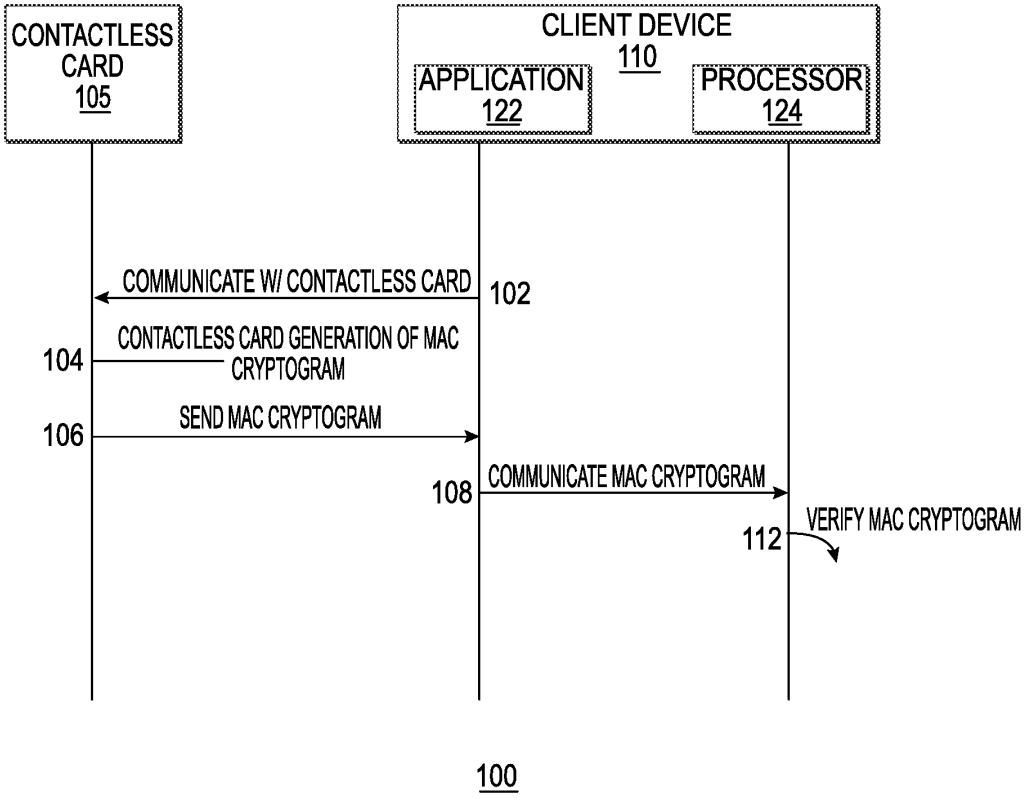

CONTACTLESS CARD 105
CLIENT DEVICE 110
APPLICATION 122
PROCESSOR 124
COMMUNICATE W/ CONTACTLESS CARD
102
CONTACTLESS CARD GENERATION OF MAC CRYPTOGRAM
104
SEND MAC CRYPTOGRAM
106
COMMUNICATE MAC CRYPTOGRAM
108
VERIFY MAC CRYPTOGRAM
112
100

FIG. 1B

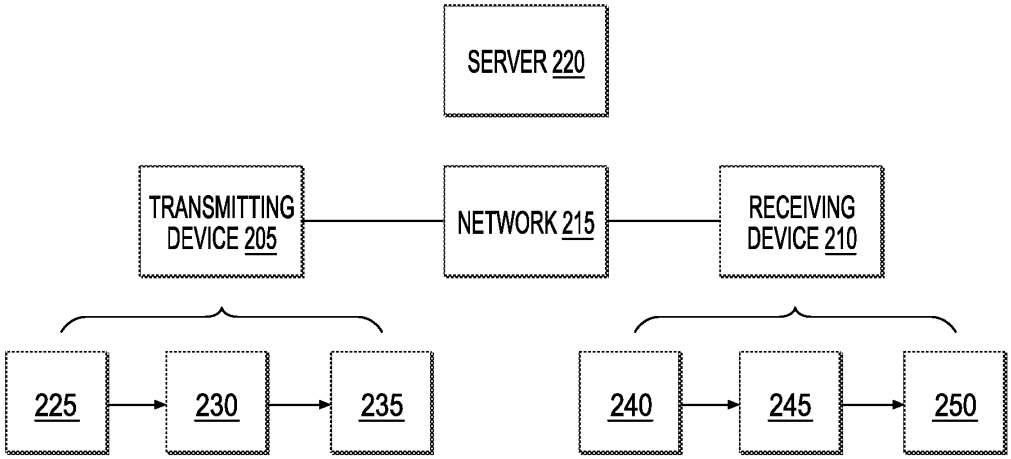

SERVER 220
TRANSMITTING DEVICE 205
NETWORK 215
RECEIVING DEVICE 210
225
230
235
240
245
250
200

FIG. 2

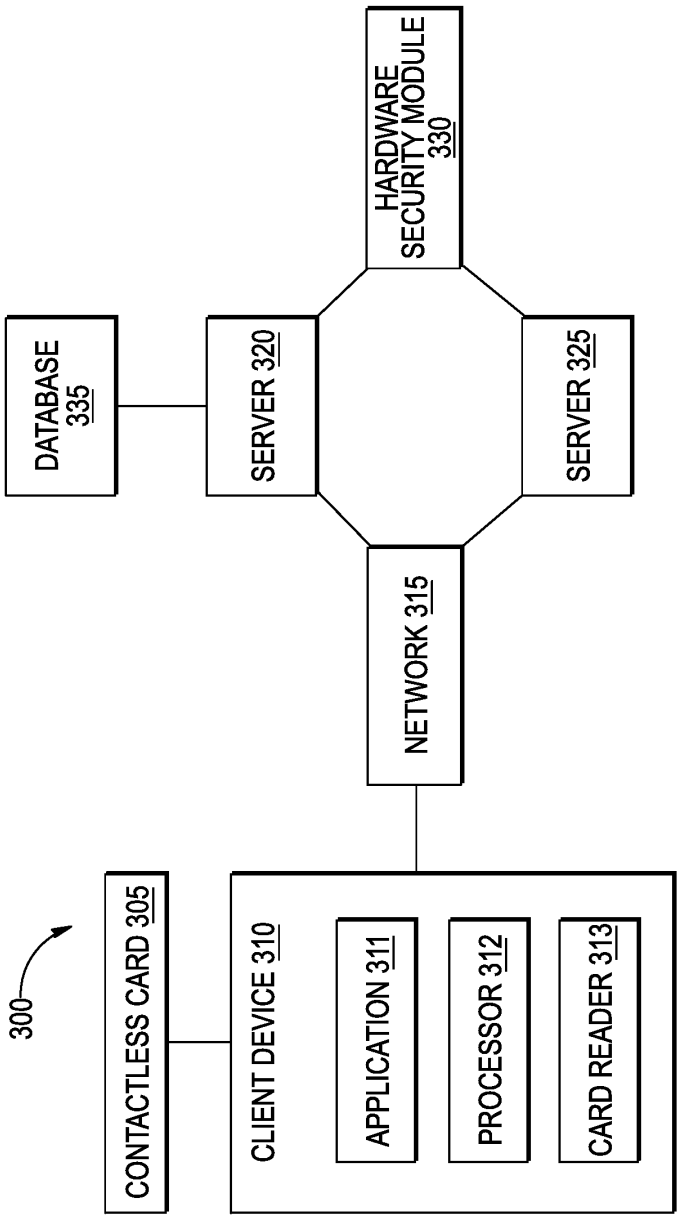
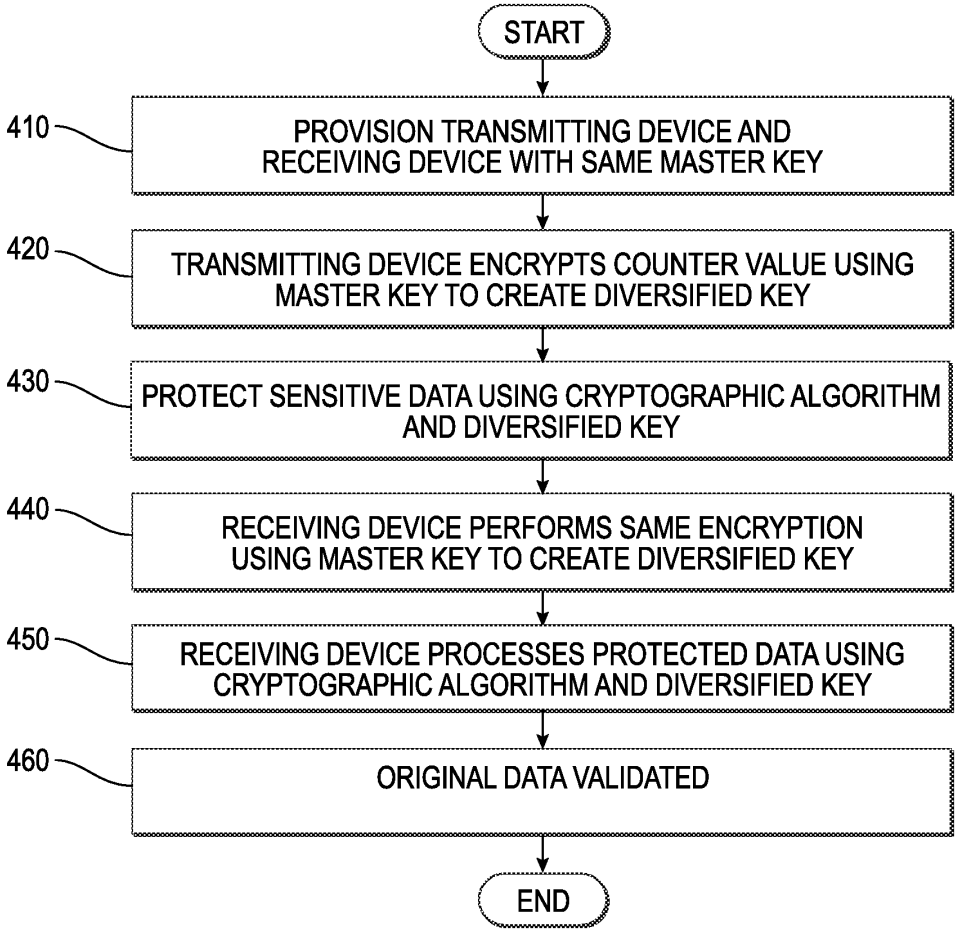

HARDWARE SECURITY MODULE 330
DATABASE 335
SERVER 320
SERVER 325
NETWORK 315
300
CONTACTLESS CARD 305
CLIENT DEVICE 310
APPLICATION 311
PROCESSOR 312
CARD READER 313

FIG. 3


START
410
PROVISION TRANSMITTING DEVICE AND RECEIVING DEVICE WITH SAME MASTER KEY
420
TRANSMITTING DEVICE ENCRYPTS COUNTER VALUE USING MASTER KEY TO CREATE DIVERSIFIED KEY
430
PROTECT SENSITIVE DATA USING CRYPTOGRAPHIC ALGORITHM AND DIVERSIFIED KEY
440
RECEIVING DEVICE PERFORMS SAME ENCRYPTION USING MASTER KEY TO CREATE DIVERSIFIED KEY
450
RECEIVING DEVICE PROCESSES PROTECTED DATA USING CRYPTOGRAPHIC ALGORITHM AND DIVERSIFIED KEY
460
ORIGINAL DATA VALIDATED
END

400

FIG. 4

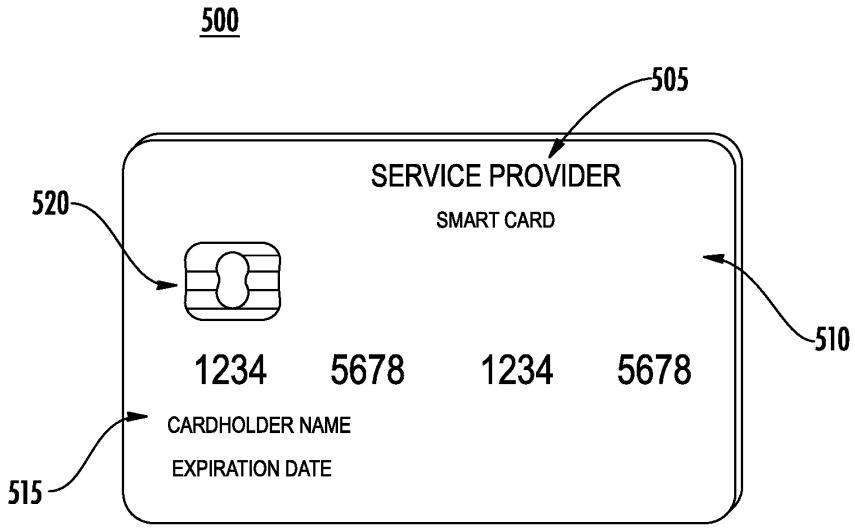

500
505
SERVICE PROVIDER
SMART CARD
520
510
1234 5678 1234 5678
CARDHOLDER NAME
EXPIRATION DATE
515

FIG. 5A

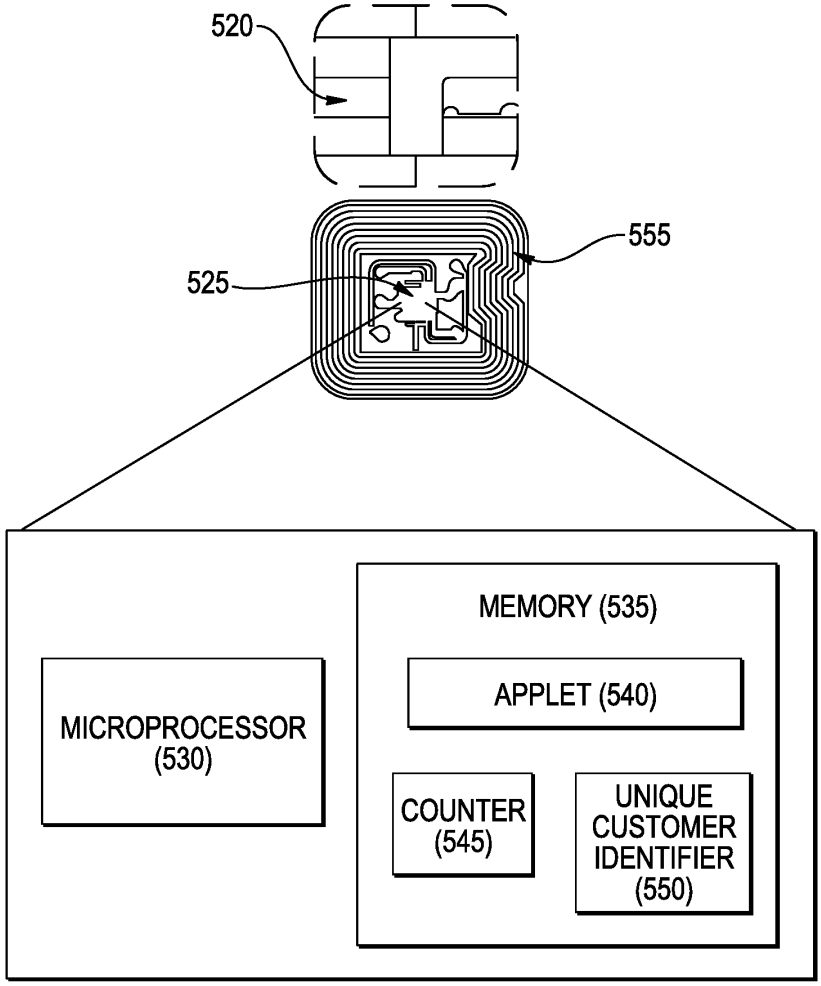
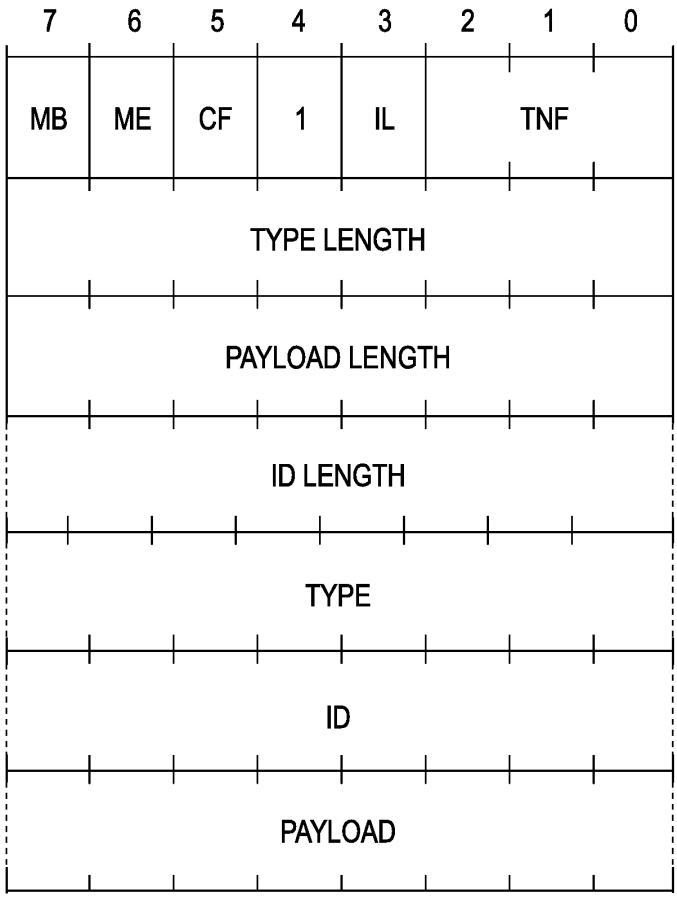

520
555
525
MEMORY (535)
APPLET (540)
MICROPROCESSOR (530)
COUNTER (545)
UNIQUE CUSTOMER IDENTIFIER (550)

FIG. 5B


7
6
5
4
3
2
1
0
MB
ME
CF
1
IL
TNF
TYPE LENGTH
PAYLOAD LENGTH
ID LENGTH
TYPE
ID
PAYLOAD

600

FIG. 6

00 D1 (Message Begin, Message End, Short Record, noID length) 01 (well known type) 01 01 Text type
02 <Payload Length including recordID and "EN", or contentlength+3) = 45+3 = 48 (DEC)
03 54 ('T')
04 02 record ID
05 65 6E (language length, 'en')
07 43 01 00 76 a6 62 7b 67 a8 cf bb <eight mac bytes>
D101305402656E 43010076A6627B67A8CFBB <eight mac bytes>

710

VERSION	pUID (8)	pATC	ENCYPHERED CRYPTOGRAM(16)	
0100	0015399555360061	00000050	7D28B8B9D8666E5143153AC9C944E5A6	
DECRYPTED CRYPTOGRAM				
RANDOM (8)	MAC (8)			
4838FB7DC171B89E	CF3F3B8C56DA0BF1			
	MAC(T=[pVERSION (2 BYTES) | | pUID (8 BYTES) | | pATC (4 BYTES) | | pSHSEC (4 BYTES) | | '80' | | '00 00 00 00 00'])			

720

FIG. 7

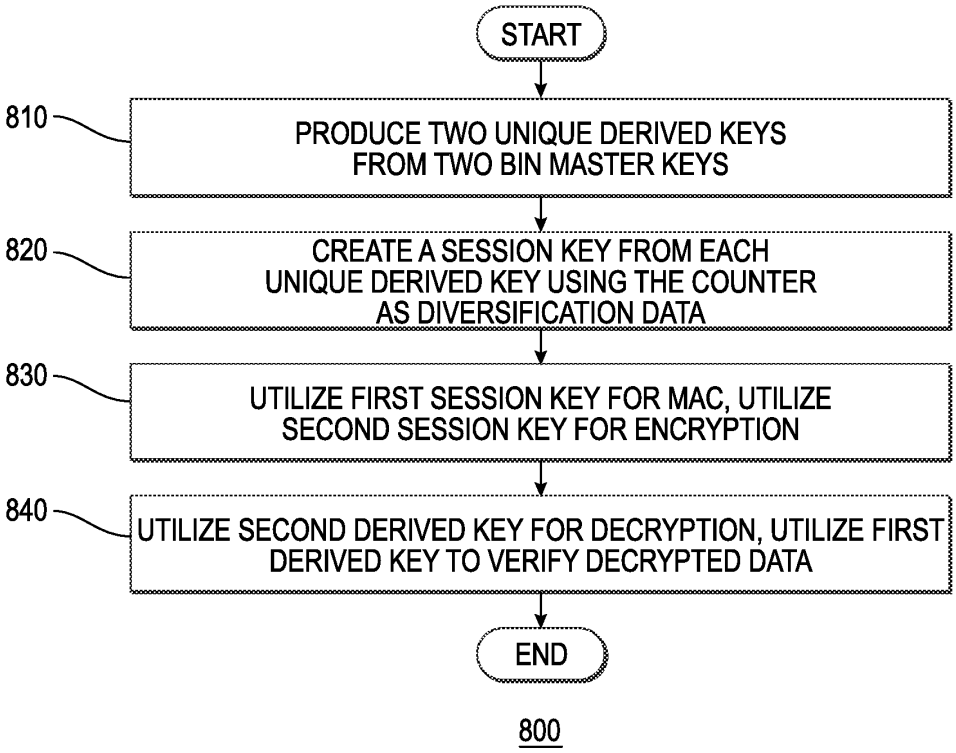

START
810
PRODUCE TWO UNIQUE DERIVED KEYS FROM TWO BIN MASTER KEYS
820
CREATE A SESSION KEY FROM EACH UNIQUE DERIVED KEY USING THE COUNTER AS DIVERSIFICATION DATA
830
UTILIZE FIRST SESSION KEY FOR MAC, UTILIZE SECOND SESSION KEY FOR ENCRYPTION
840
UTILIZE SECOND DERIVED KEY FOR DECRYPTION, UTILIZE FIRST DERIVED KEY TO VERIFY DECRYPTED DATA
END
800

FIG. 8

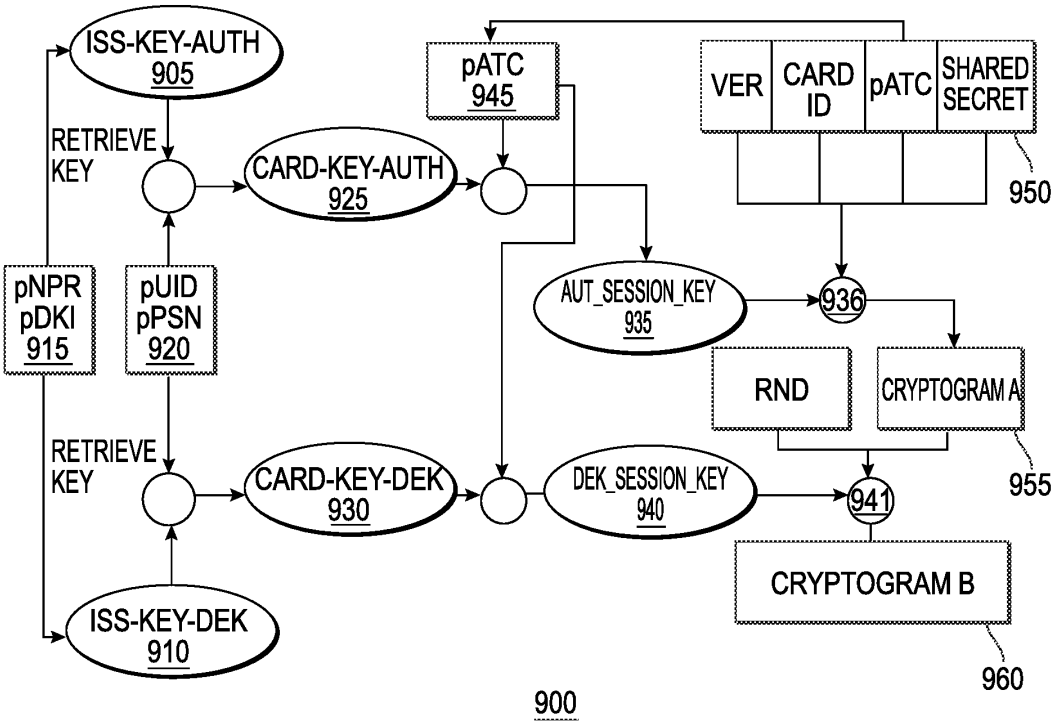

ISS-KEY-AUTH
905
RETRIEVE
KEY
CARD-KEY-AUTH
925
pATC
945
VER
CARD
ID
pATC
SHARED
SECRET
950
pNPR
pDKI
915
pUID
pPSN
920
AUT_SESSION_KEY
935
936
RND
CRYPTOGRAM A
955
RETRIEVE
KEY
CARD-KEY-DEK
930
DEK_SESSION_KEY
940
941
CRYPTOGRAM B
960
ISS-KEY-DEK
910
900

FIG. 9

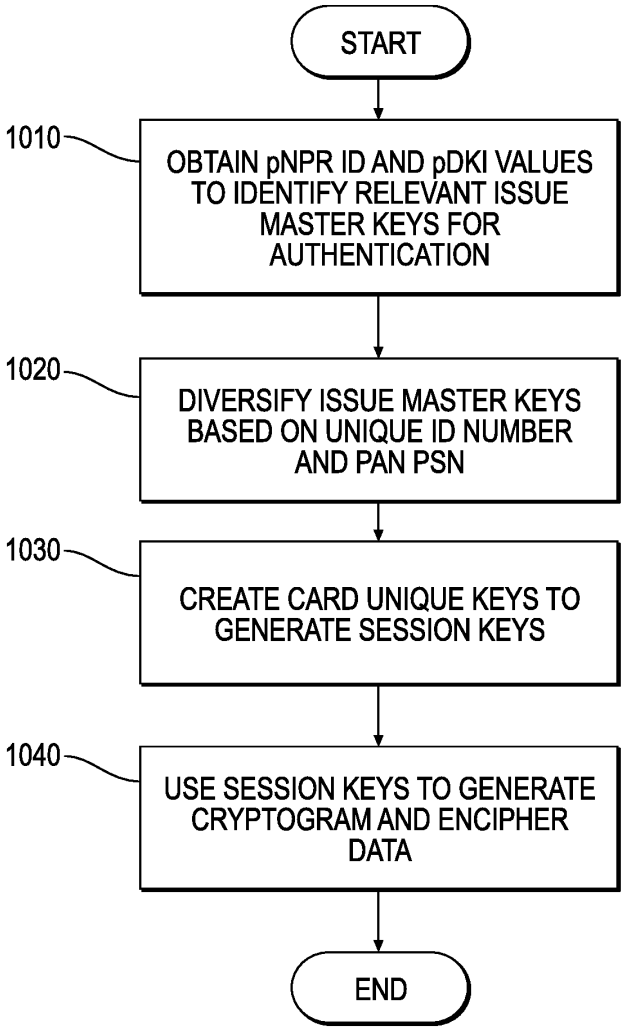

START
1010
OBTAIN pNPR ID AND pDKI VALUES TO IDENTIFY RELEVANT ISSUE MASTER KEYS FOR AUTHENTICATION
1020
DIVERSIFY ISSUE MASTER KEYS BASED ON UNIQUE ID NUMBER AND PAN PSN
1030
CREATE CARD UNIQUE KEYS TO GENERATE SESSION KEYS
1040
USE SESSION KEYS TO GENERATE CRYPTOGRAM AND ENCIPHER DATA
END
1000

FIG. 10

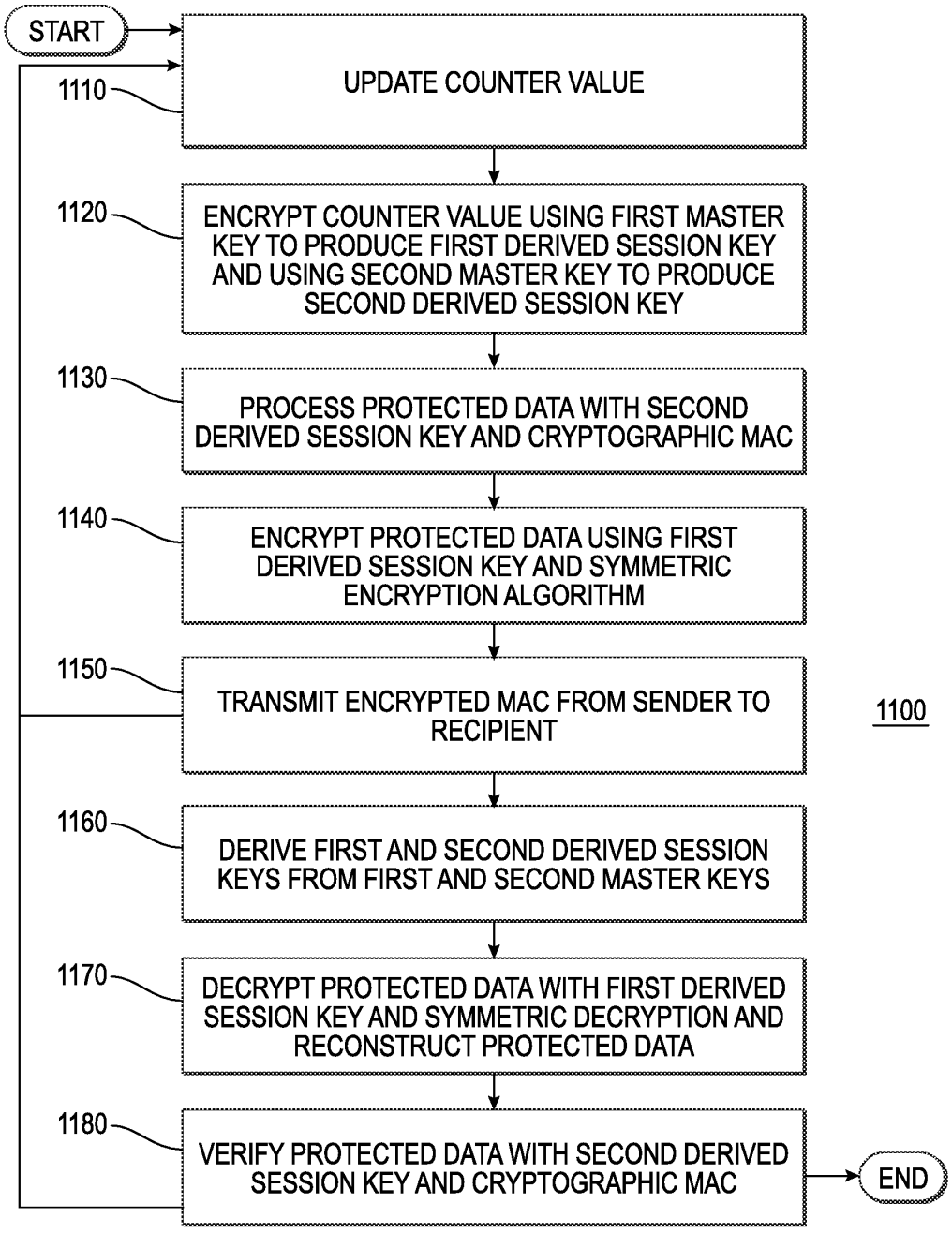

START
1110
UPDATE COUNTER VALUE
1120
ENCRYPT COUNTER VALUE USING FIRST MASTER KEY TO PRODUCE FIRST DERIVED SESSION KEY AND USING SECOND MASTER KEY TO PRODUCE SECOND DERIVED SESSION KEY
1130
PROCESS PROTECTED DATA WITH SECOND DERIVED SESSION KEY AND CRYPTOGRAPHIC MAC
1140
ENCRYPT PROTECTED DATA USING FIRST DERIVED SESSION KEY AND SYMMETRIC ENCRYPTION ALGORITHM
1150
TRANSMIT ENCRYPTED MAC FROM SENDER TO RECIPIENT
1100
1160
DERIVE FIRST AND SECOND DERIVED SESSION KEYS FROM FIRST AND SECOND MASTER KEYS
1170
DECRYPT PROTECTED DATA WITH FIRST DERIVED SESSION KEY AND SYMMETRIC DECRYPTION AND RECONSTRUCT PROTECTED DATA
1180
VERIFY PROTECTED DATA WITH SECOND DERIVED SESSION KEY AND CRYPTOGRAPHIC MAC
END

FIG. 11

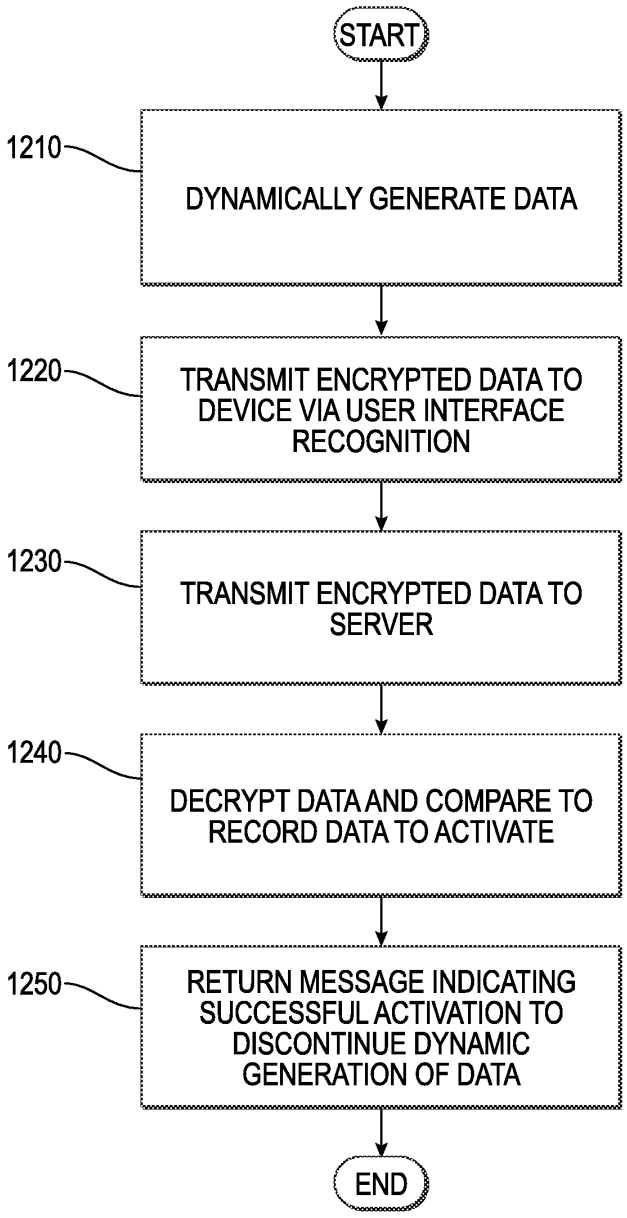
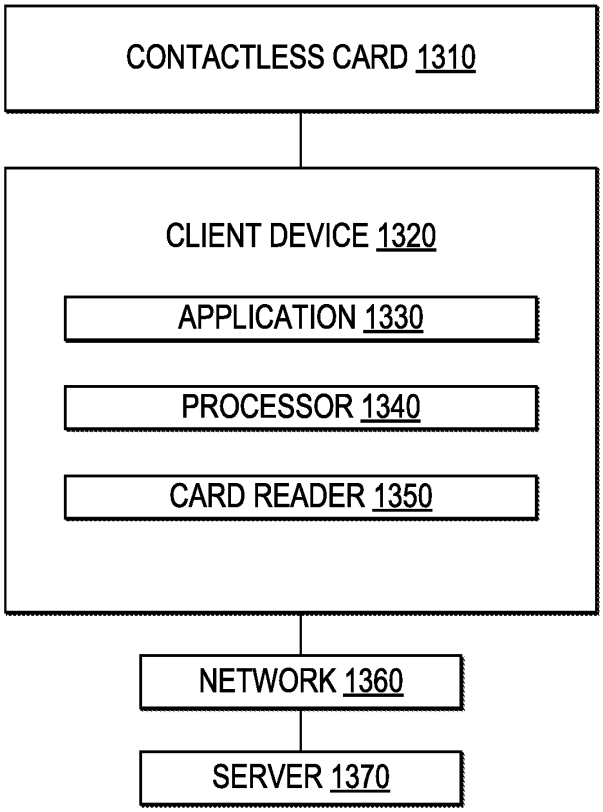
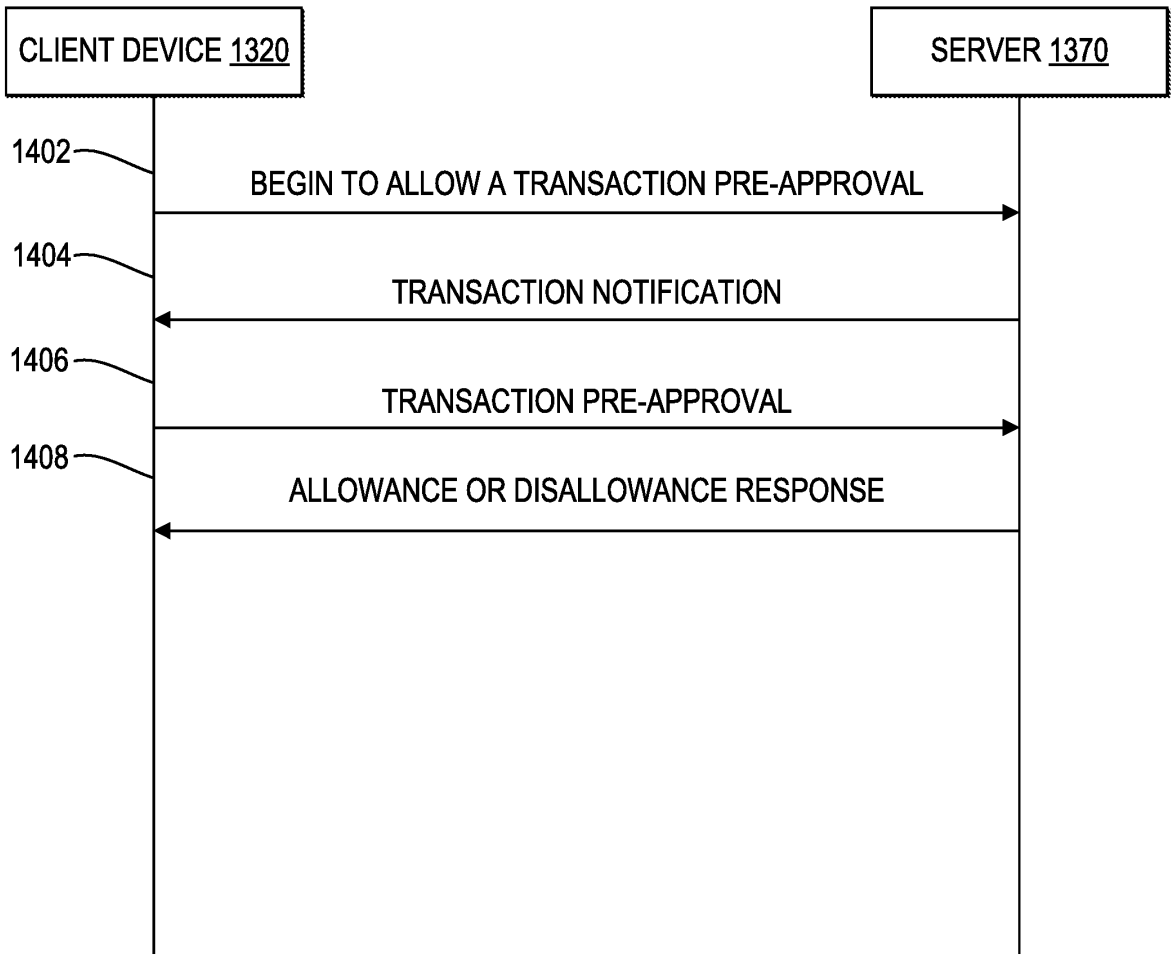

START
1210
DYNAMICALLY GENERATE DATA
1220
TRANSMIT ENCRYPTED DATA TO DEVICE VIA USER INTERFACE RECOGNITION
1230
TRANSMIT ENCRYPTED DATA TO SERVER
1240
DECRYPT DATA AND COMPARE TO RECORD DATA TO ACTIVATE
1250
RETURN MESSAGE INDICATING SUCCESSFUL ACTIVATION TO DISCONTINUE DYNAMIC GENERATION OF DATA
END
1200

FIG. 12


CONTACTLESS CARD 1310
CLIENT DEVICE 1320
APPLICATION 1330
PROCESSOR 1340
CARD READER 1350
NETWORK 1360
SERVER 1370

1300

FIG. 13


CLIENT DEVICE 1320
SERVER 1370
1402
BEGIN TO ALLOW A TRANSACTION PRE-APPROVAL
1404
TRANSACTION NOTIFICATION
1406
TRANSACTION PRE-APPROVAL
1408
ALLOWANCE OR DISALLOWANCE RESPONSE

1400

FIG. 14