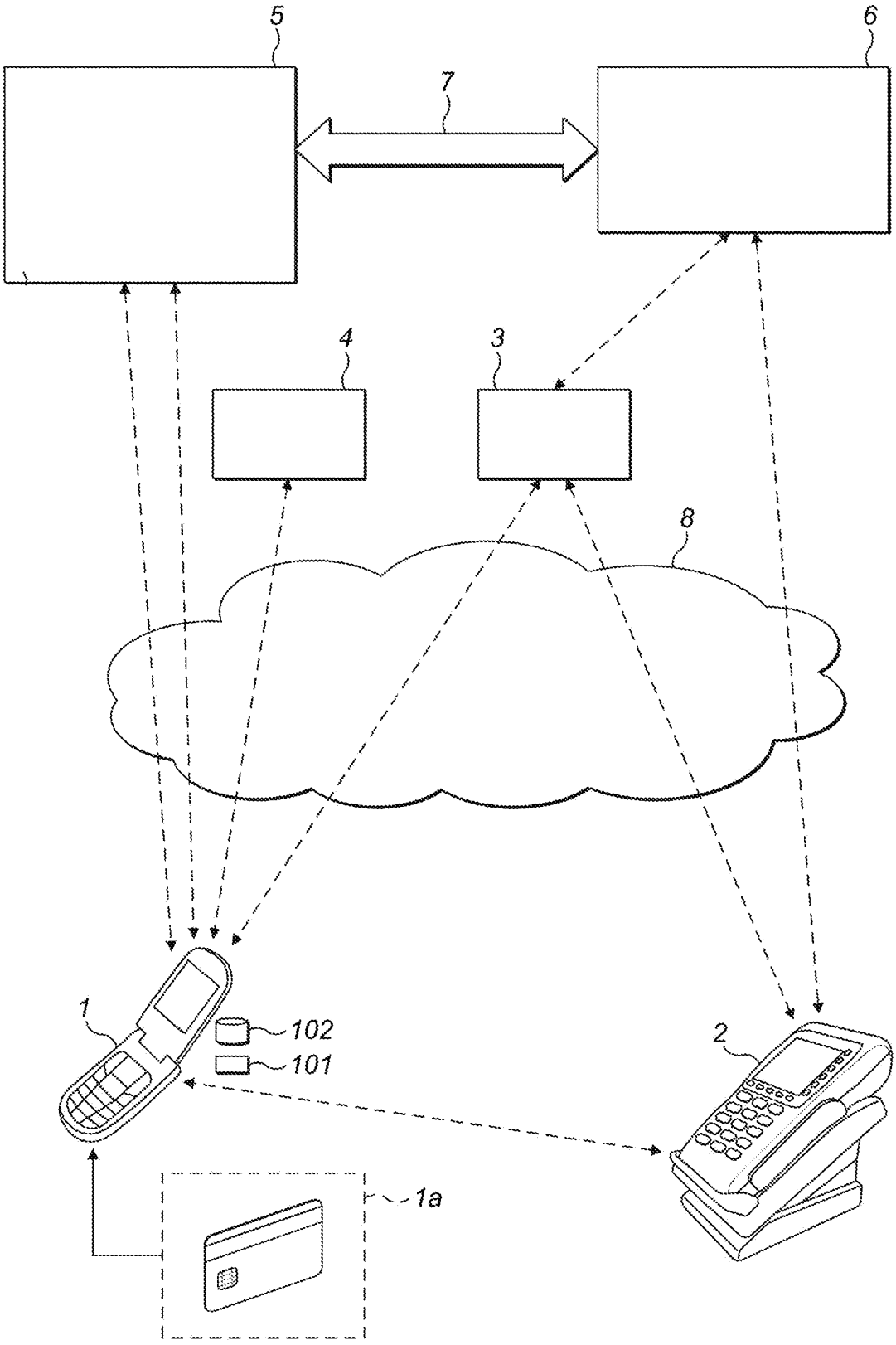


FIG.1

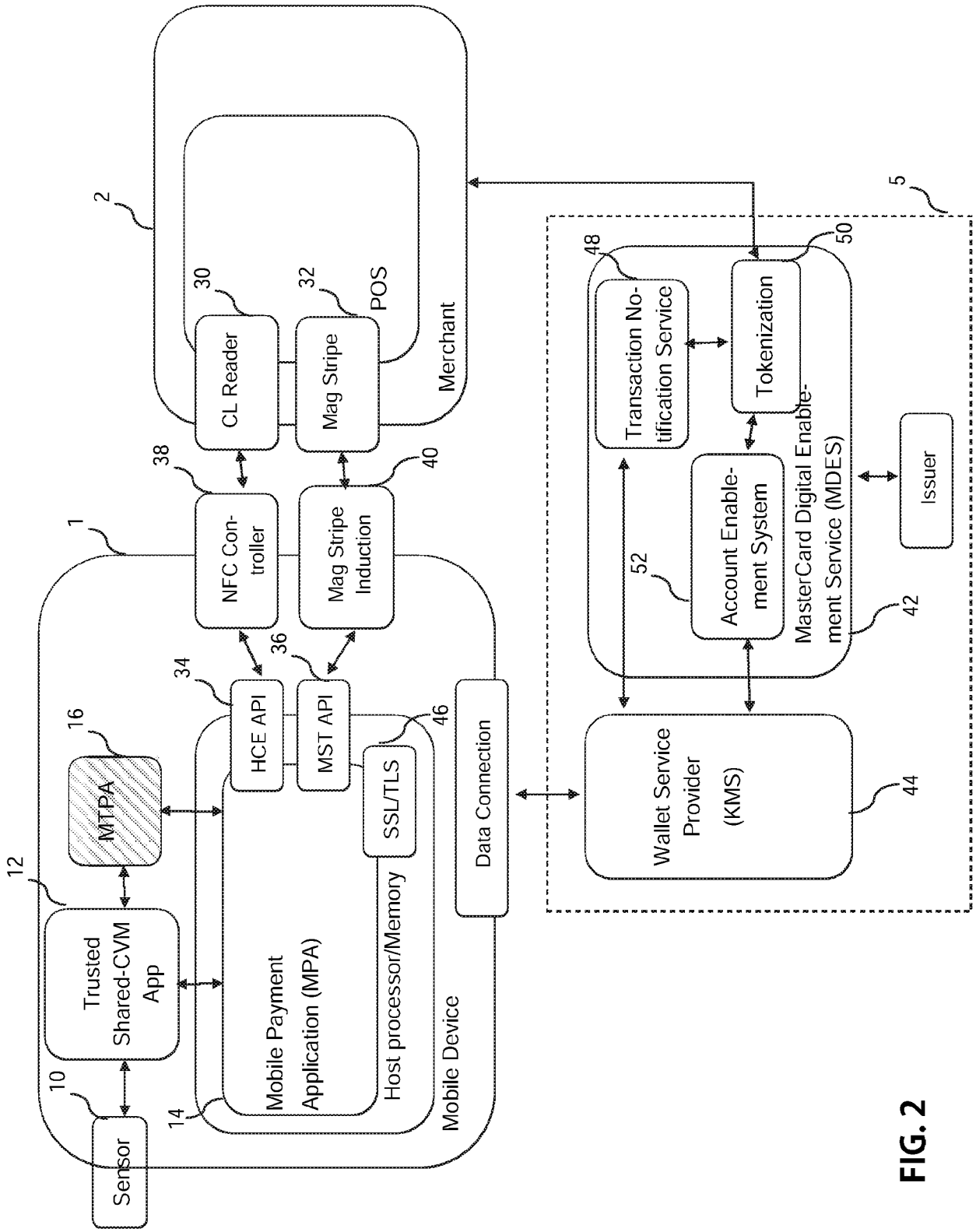

Sensor
10
12
Trusted Shared-CVM App
MTPA
16
Mobile Payment Application (MPA)
14
HCE API
34
MST API
36
SSL/TLS
46
Host processor/Memory
Mobile Device
1
NFC Con-troller
38
Mag Stripe Induction
40
Data Connection
CL Reader
30
Mag Stripe
32
POS
Merchant
2
Wallet Service Provider (KMS)
44
Transaction No-tification Service
48
Tokenization
50
Account Enable-ment System
52
MasterCard Digital Enable-ment Service (MDES)
42
Issuer
5

FIG. 2

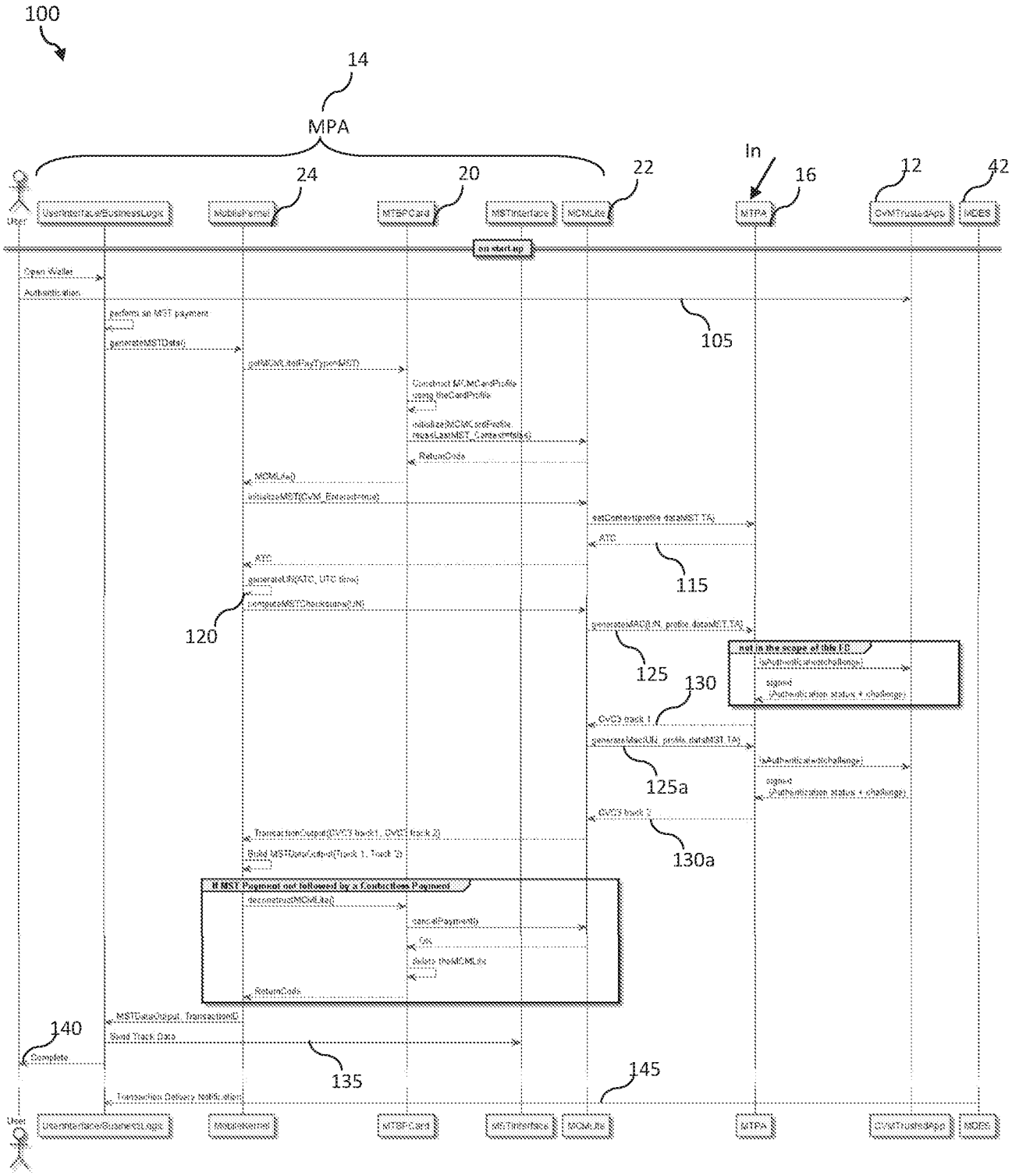

100
14
MPA
In
16
12
42
24
20
22
User
UserInterface/BusinessLogic
MobileKernel
MTBPCard
MSTInterface
MCMLite
MTPA
CVMTrustedApp
MDES
on startup
Open Wallet
Authentication
perform an MST payment
generateMSTData()
105
getMCMLitePayType=MST()
Construct MCMCardProfile
using theCardProfile
initialize(MCMCardProfile
resetLastMST_ContextMsg())
ReturnCode
MCMLite()
initializeMST(CVM_Enforcement)
setContextprofile dataMST.TA)
ATC
ATC
115
generateUN(ATC, UTC time)
120
computeMSTCheckcurve(UN)
generateMAC(UN, profile dataMST.TA)
125
not in the scope of this I.D.
isAuthenticate(challenge)
signed
(Authentication status + challenge)
130
CVC3 track 1
generateIdentUN, profile, dataMST.TA)
125a
isAuthenticate(challenge)
signed
(Authentication status + challenge)
CVC3 track 2
130a
TransactionOutput(CVC3 track1, CVC3 track 2)
Build MSTDataOutput(Track 1, Track 2)
If MST Payment not followed by a Contactless Payment
deconstructMCMLite()
cancelPayment()
OK
delete theMCMLite
ReturnCode
MSTDataOutput, transactionID
140
Send Track Data
135
Complete
145
Transaction Delivery Notification

FIG. 3

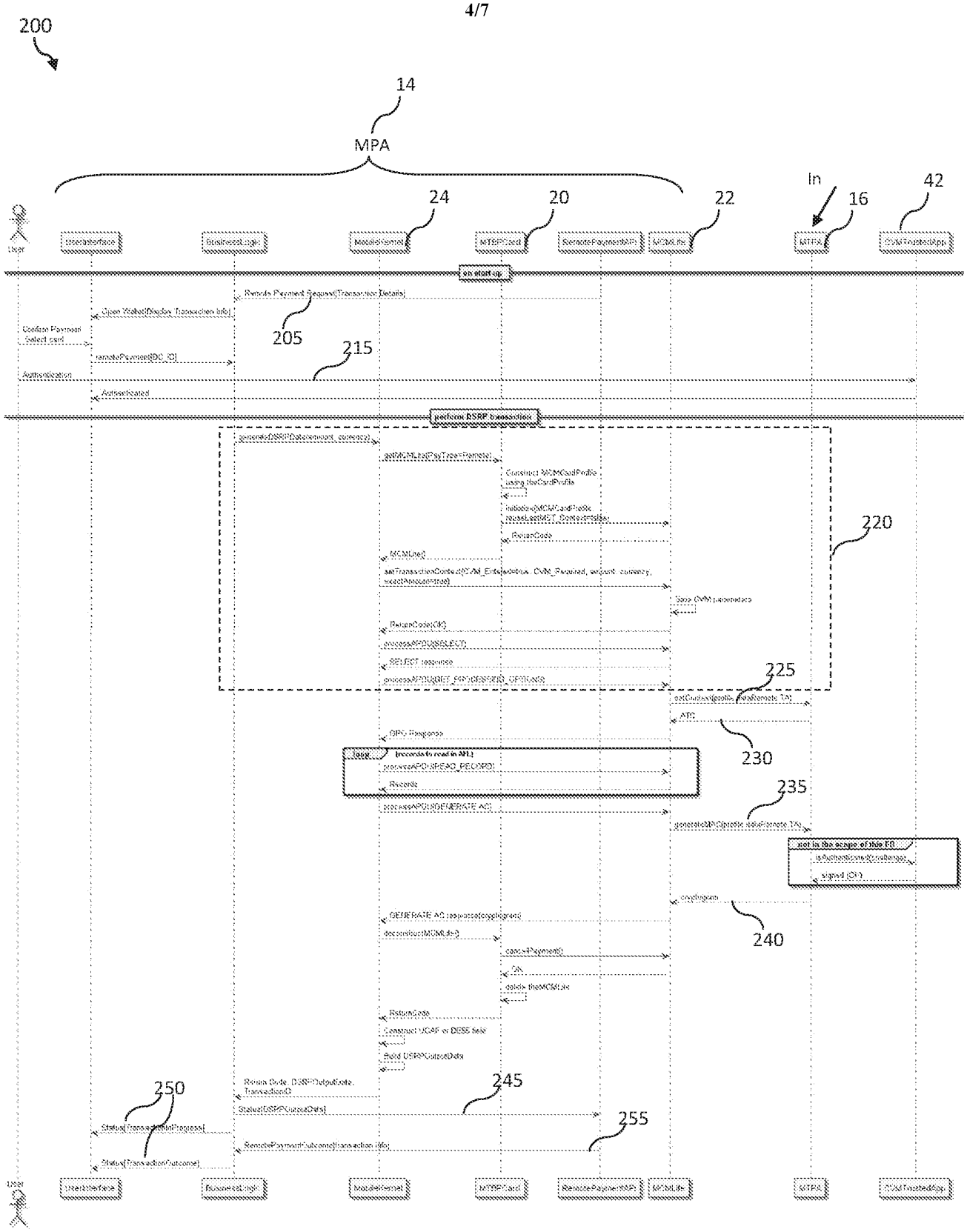


FIG. 4

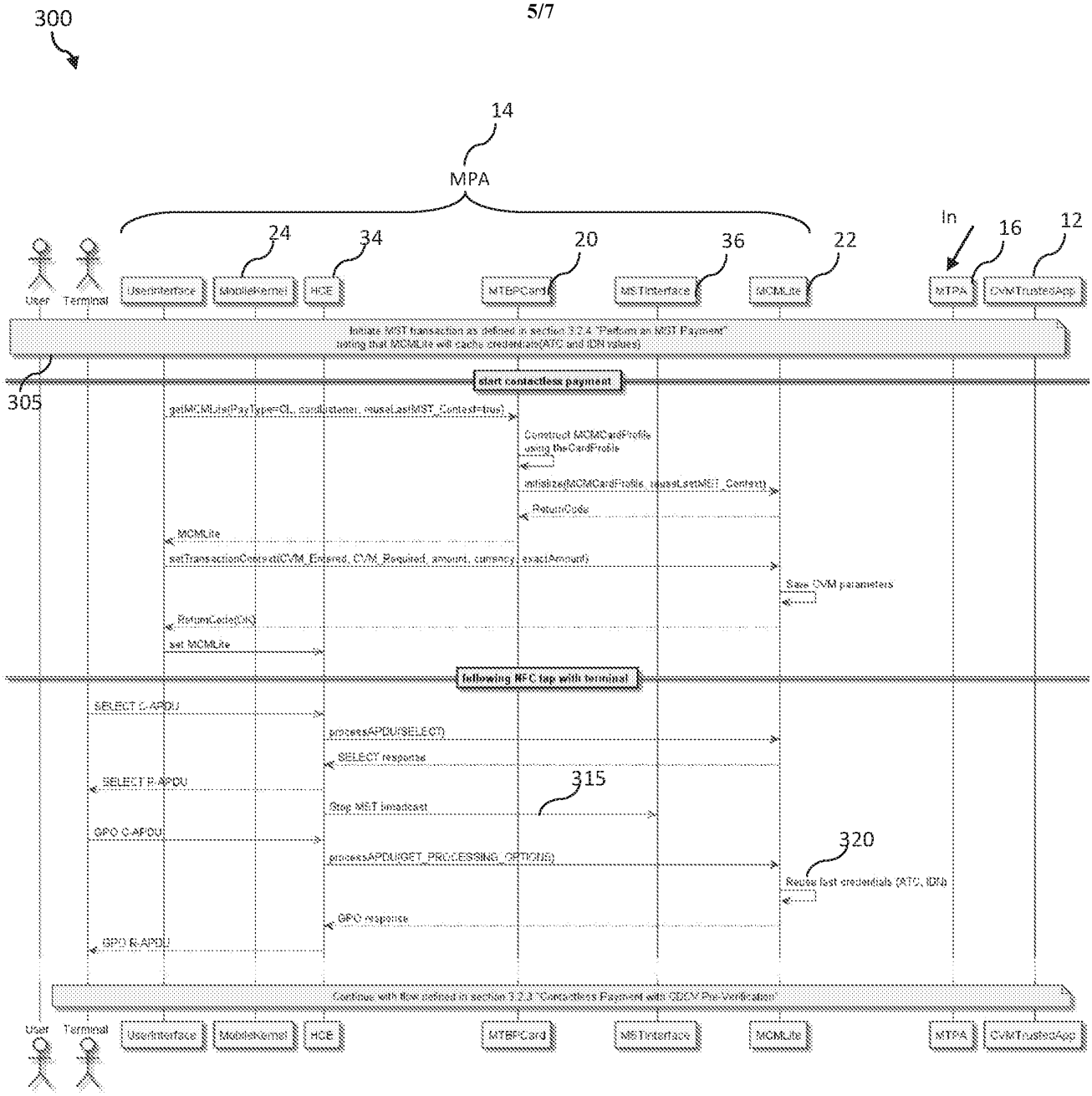

300
14
MPA
24
34
20
36
22
In
16
12
User
Terminal
UserInterface
MobileKernel
HCE
MTBPCard
MSTInterface
MCMLite
MTPA
CVMTrustedApp
Initiate MST transaction as defined in section 3.2.4 "Perform an MST Payment"
noting that MCMLite will cache credentials(ATC and IDN values)
305
start contactless payment
getMCMLite(PayType=CL, cardListener, reuseLastMST_Context=true)
Construct MCMCardProfile
using theCardProfile
initialize(MCMCardProfile, reuseLastMST_Context)
ReturnCode
MCMLite
setTransactionContext(CVM_Entered, CVM_Required, amount, currency, exactAmount)
Save CVM parameters
ReturnCode(OK)
set MCMLite
following NFC tap with terminal
SELECT C-APDU
processAPDU(SELECT)
SELECT response
SELECT R-APDU
315
Stop MST broadcast
GPO C-APDU
320
processAPDU(GET_PROCESSING_OPTIONS)
Reuse fast credentials (ATC, IDN)
GPO response
GPO R-APDU
Continue with flow defined in section 3.2.3 "Contactless Payment with CDCVM Pre-Verification"

FIG. 5

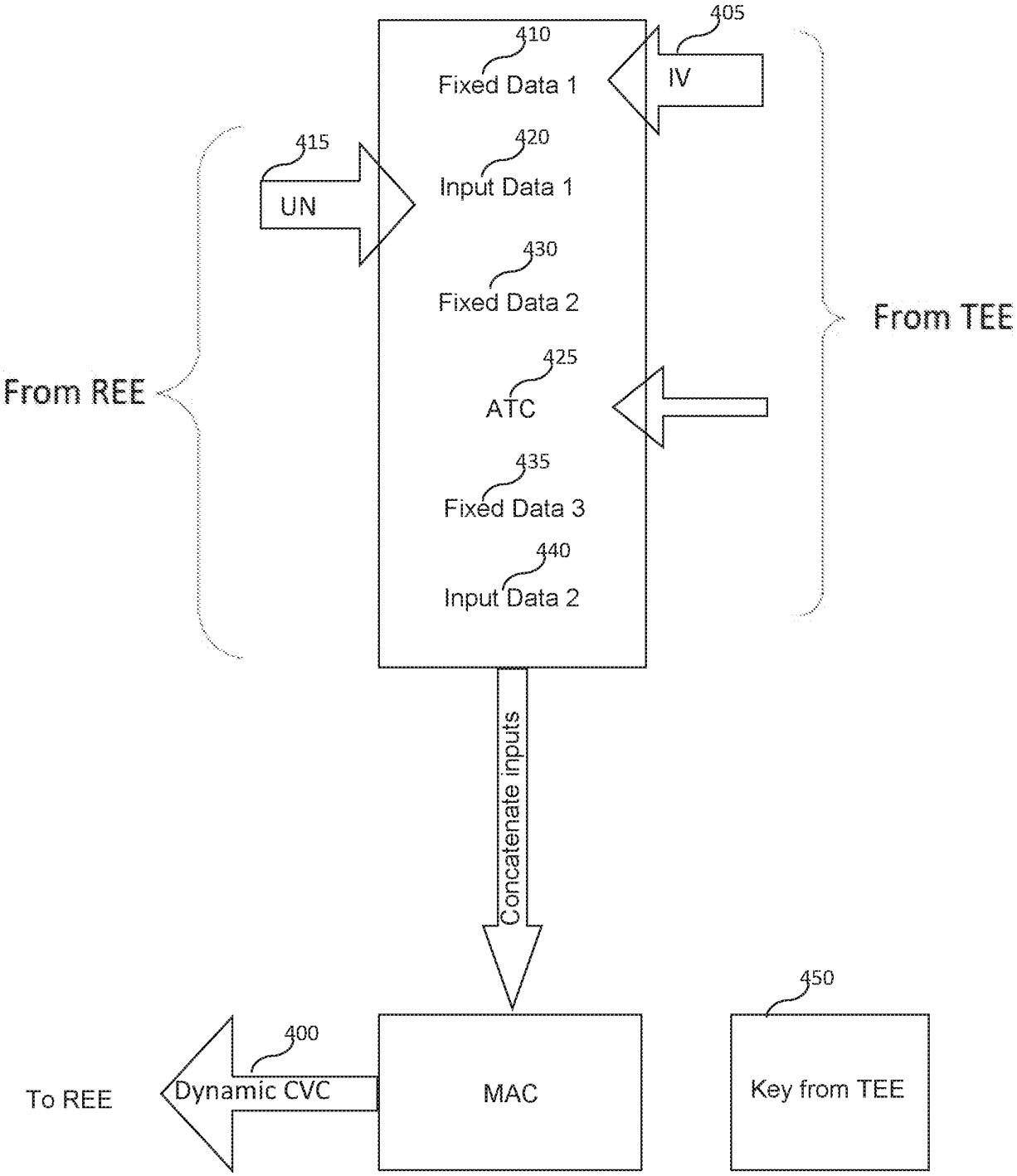

405
410
Fixed Data 1
IV
415
420
UN
Input Data 1
430
Fixed Data 2
From TEE
From REE
425
ATC
435
Fixed Data 3
440
Input Data 2
Concatenate inputs
450
400
To REE
Dynamic CVC
MAC
Key from TEE

FIG. 6

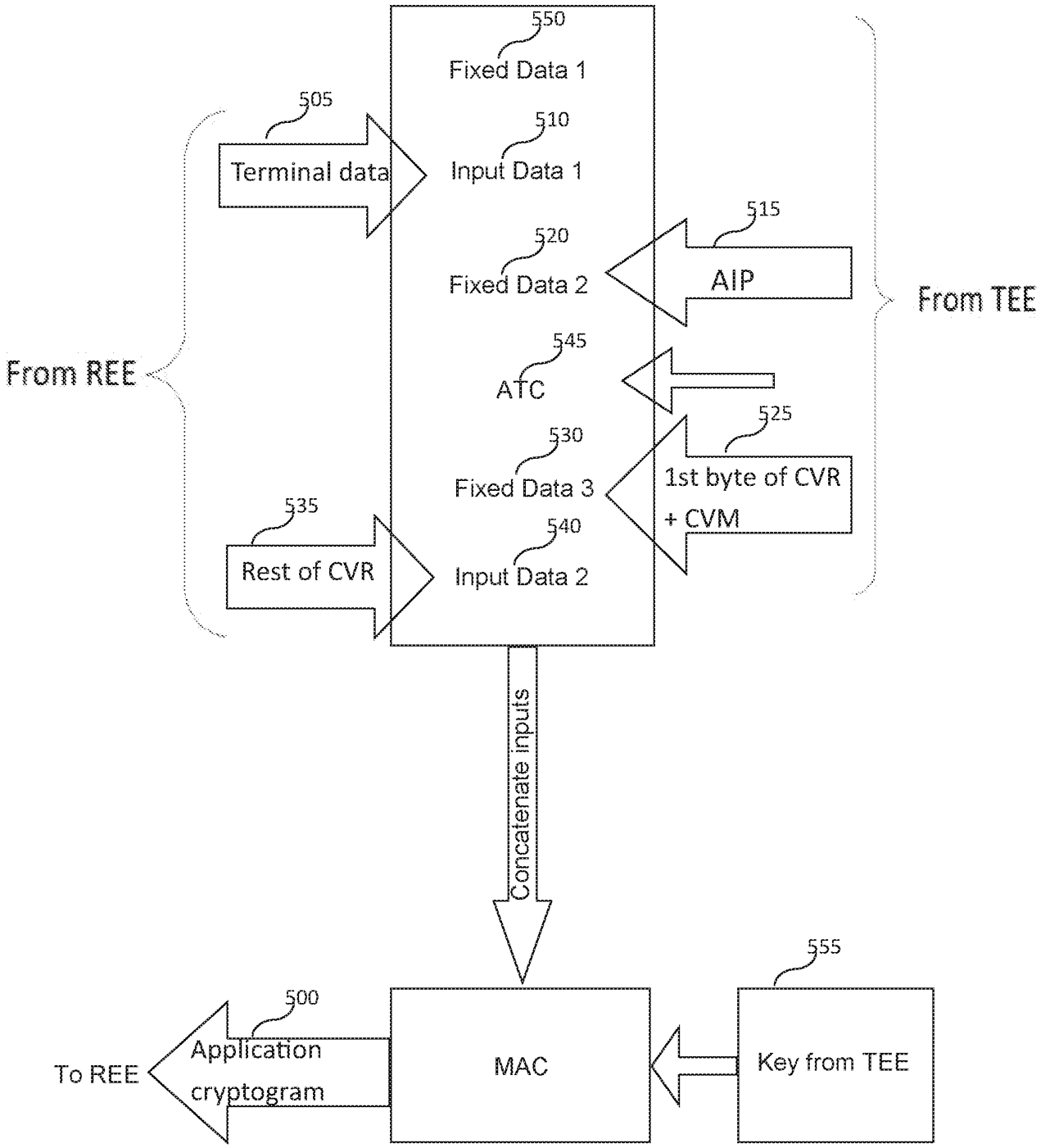

550
Fixed Data 1
505
Terminal data
510
Input Data 1
515
AIP
520
Fixed Data 2
From TEE
From REE
545
ATC
525
530
Fixed Data 3
1st byte of CVR
+ CVM
535
Rest of CVR
540
Input Data 2
Concatenate inputs
555
500
To REE
Application
cryptogram
MAC
Key from TEE

FIG. 7