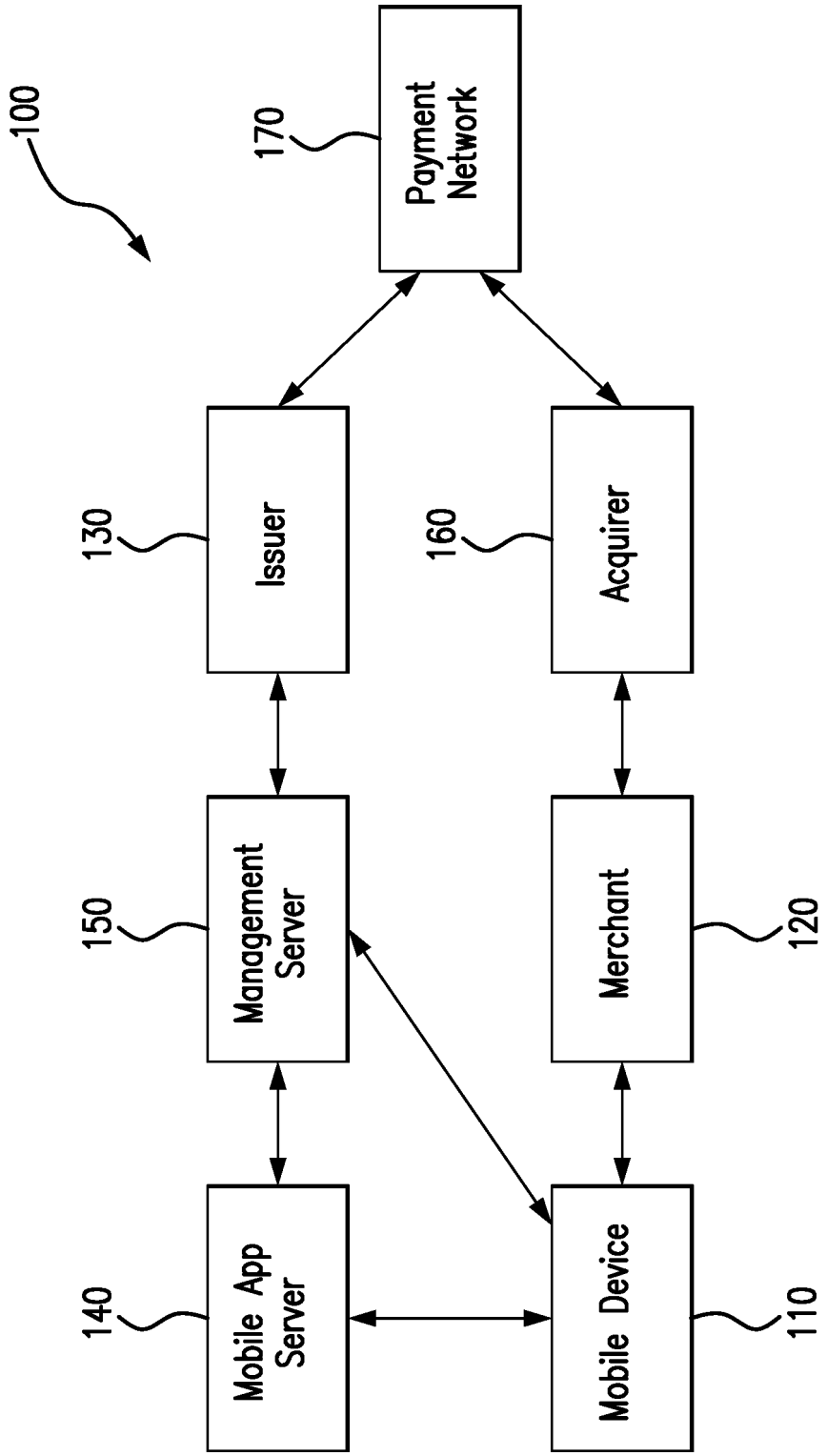

100
170
Payment Network
130
Issuer
160
Acquirer
150
Management Server
Merchant
120
140
Mobile App Server
Mobile Device
110

FIG. 1

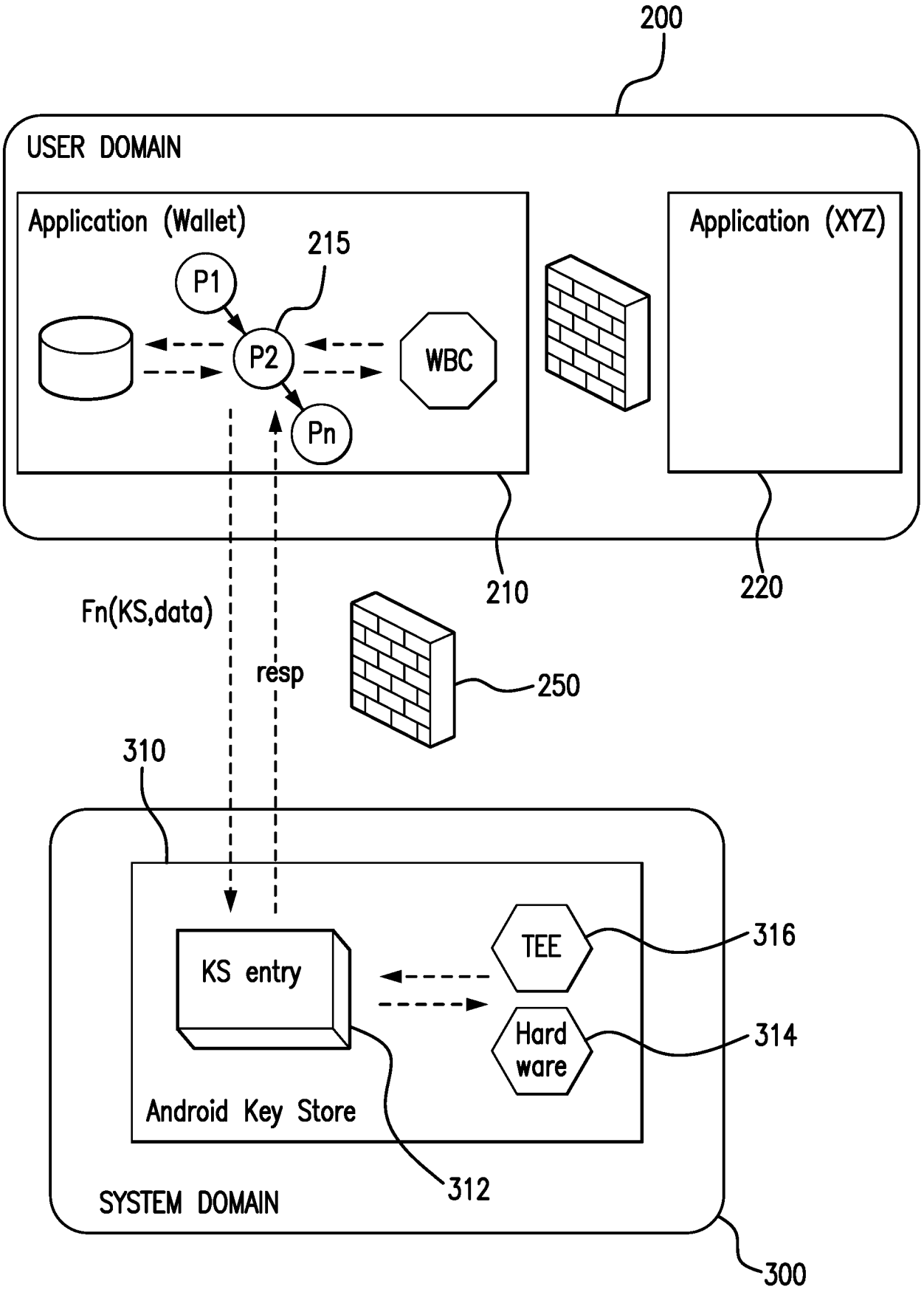

200
USER DOMAIN
Application (Wallet)
215
P1
P2
Pn
WBC
Application (XYZ)
210
220
Fn(KS,data)
resp
250
310
KS entry
TEE
316
Hard ware
314
Android Key Store
312
SYSTEM DOMAIN
300

FIG. 2

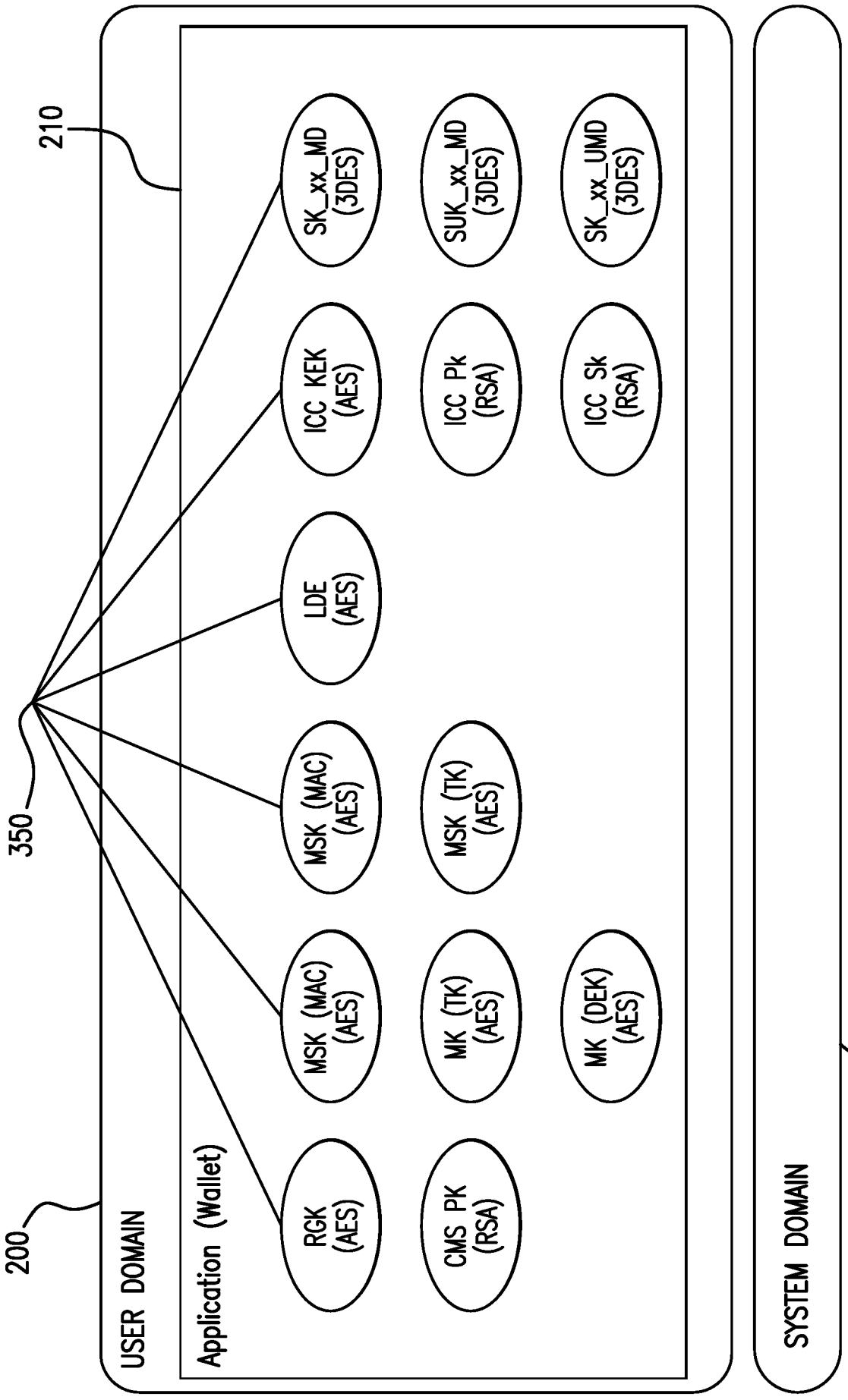

200
USER DOMAIN
210
Application (Wallet)
350
RGK (AES)
MSK (MAC) (AES)
LDE (AES)
ICC KEK (AES)
SK_xx_MD (3DES)
CMS PK (RSA)
MK (TK) (AES)
MSK (TK) (AES)
ICC Pk (RSA)
SUK_xx_MD (3DES)
MK (DEK) (AES)
ICC Sk (RSA)
SK_xx_UMD (3DES)
SYSTEM DOMAIN
300

FIG. 3

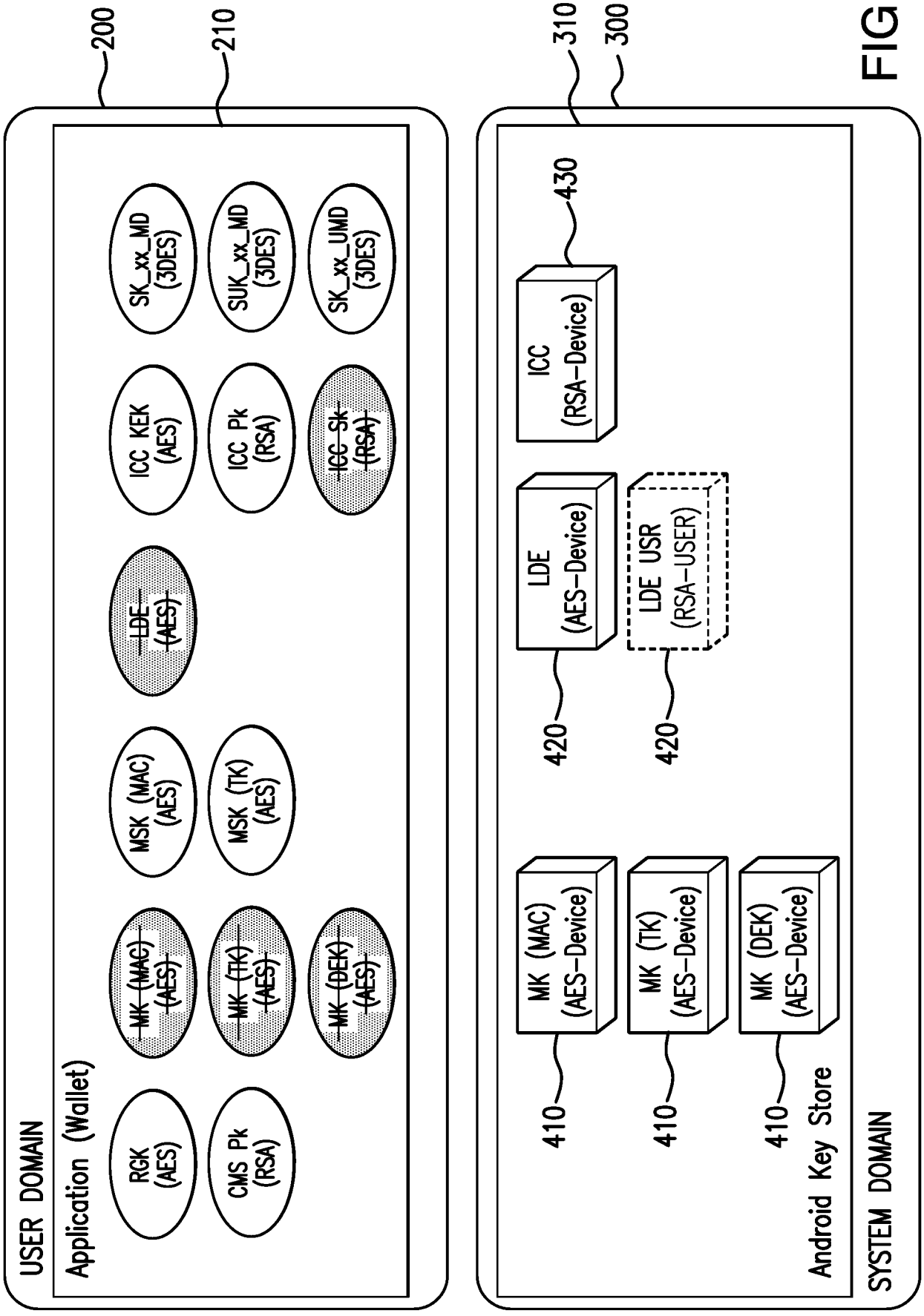

200
210
310
300
USER DOMAIN
Application (Wallet)
RGK (AES)
CMS Pk (RSA)
MK (MAC) (AES)
MK (TK) (AES)
MK (DEK) (AES)
MSK (MAC) (AES)
MSK (TK) (AES)
LDE (AES)
ICC KEK (AES)
ICC Pk (RSA)
ICC Sk (RSA)
SK_xx_MD (3DES)
SUK_xx_MD (3DES)
SK_xx_UMD (3DES)
SYSTEM DOMAIN
Android Key Store
MK (MAC) (AES-Device)
MK (TK) (AES-Device)
MK (DEK) (AES-Device)
LDE (AES-Device)
LDE USR (RSA-USER)
ICC (RSA-Device)
410
420
430

FIG. 4

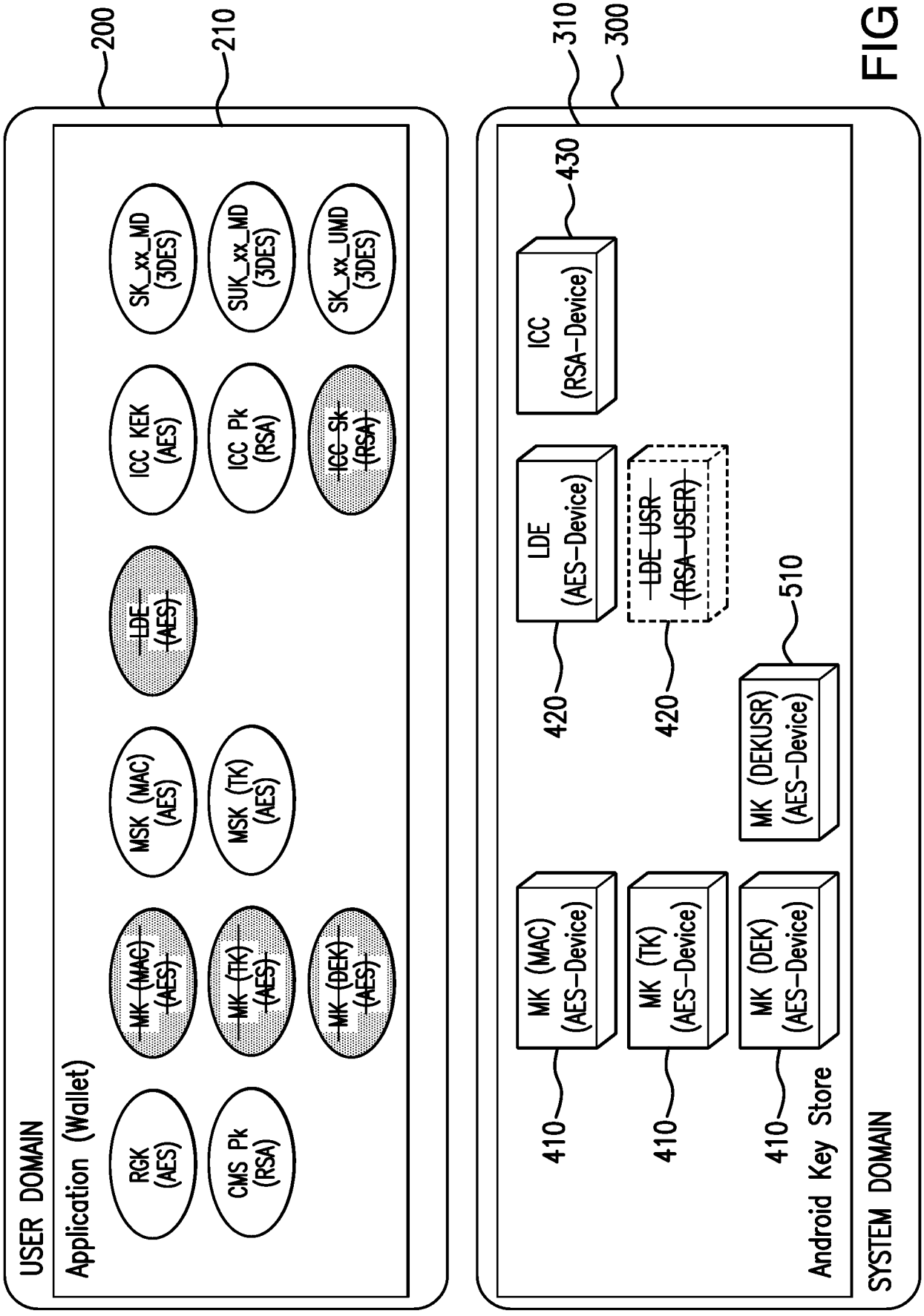

200
210
USER DOMAIN
Application (Wallet)
RGK (AES)
CMS Pk (RSA)
MK (MAC) (AES)
MK (TK) (AES)
MK (DEK) (AES)
MSK (MAC) (AES)
MSK (TK) (AES)
LDE (AES)
ICC KEK (AES)
ICC Pk (RSA)
ICC Sk (RSA)
SK_xx_MD (3DES)
SUK_xx_MD (3DES)
SK_xx_UMD (3DES)
310
300
430
ICC (RSA-Device)
LDE (AES-Device)
LDE USR (RSA USER)
420
420
510
MK (DEKUSR) (AES-Device)
MK (MAC) (AES-Device)
MK (TK) (AES-Device)
MK (DEK) (AES-Device)
410
410
410
Android Key Store
SYSTEM DOMAIN

FIG. 5

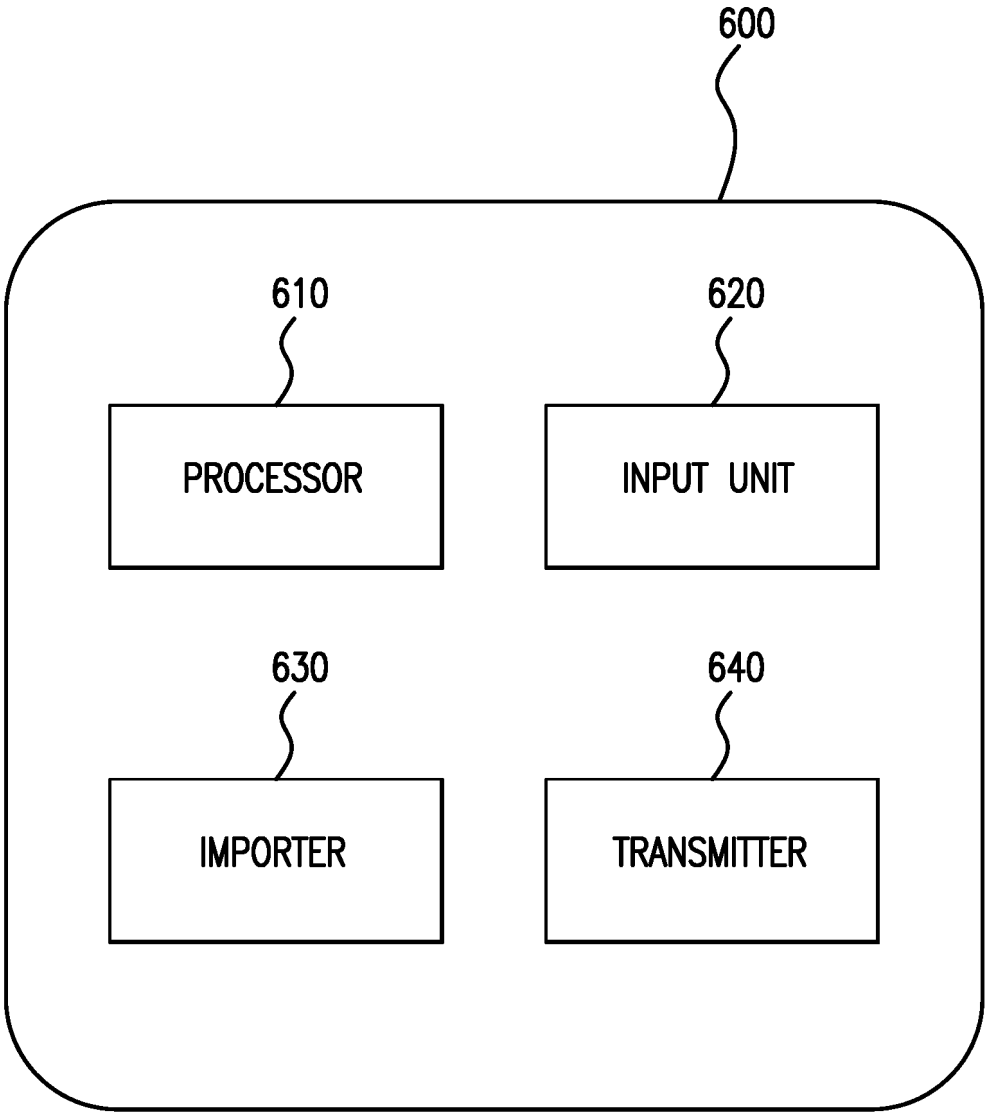

600
610
PROCESSOR
620
INPUT UNIT
630
IMPORTER
640
TRANSMITTER

FIG. 6

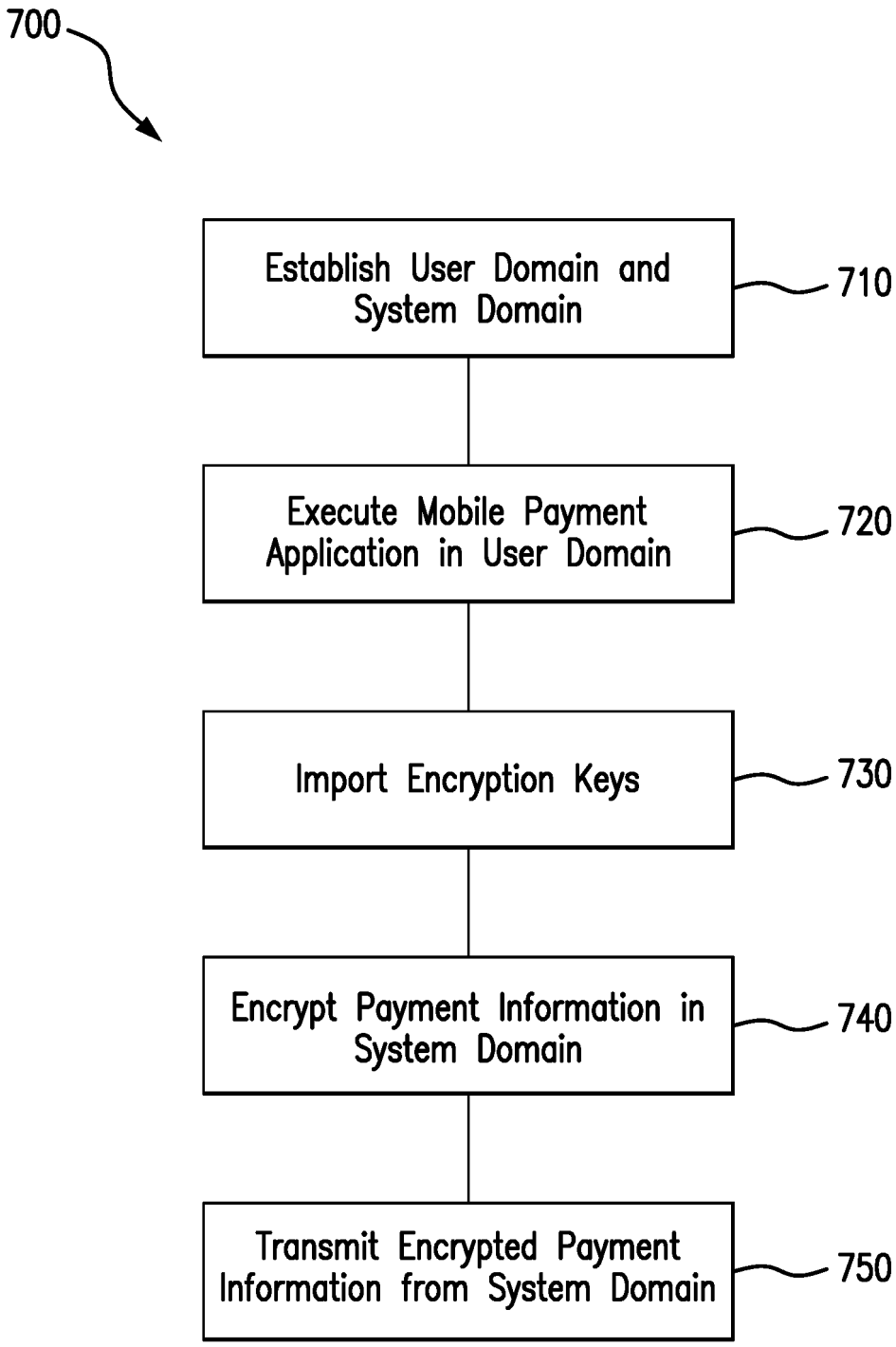

700
Establish User Domain and System Domain
710
Execute Mobile Payment Application in User Domain
720
Import Encryption Keys
730
Encrypt Payment Information in System Domain
740
Transmit Encrypted Payment Information from System Domain
750

FIG. 7