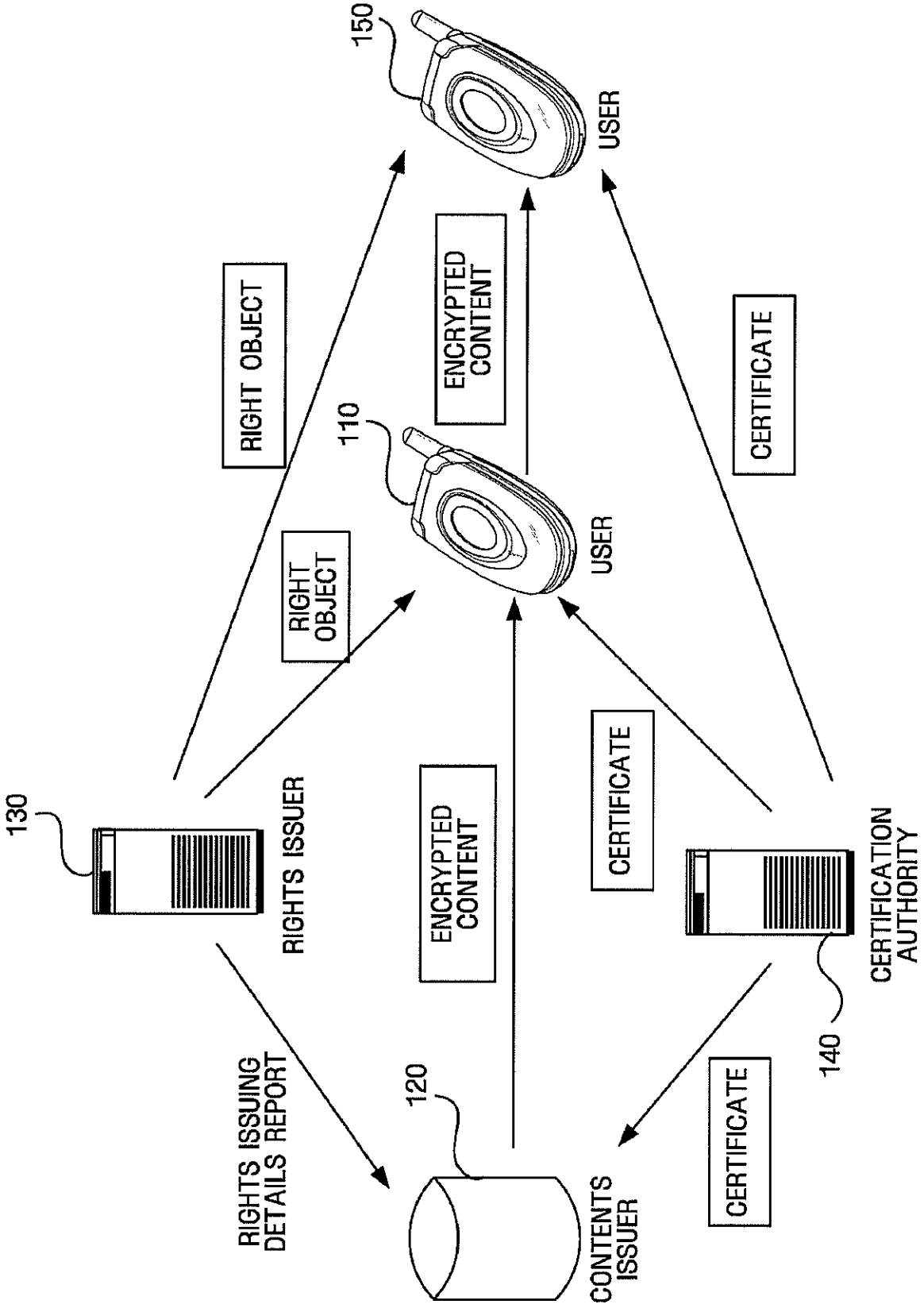
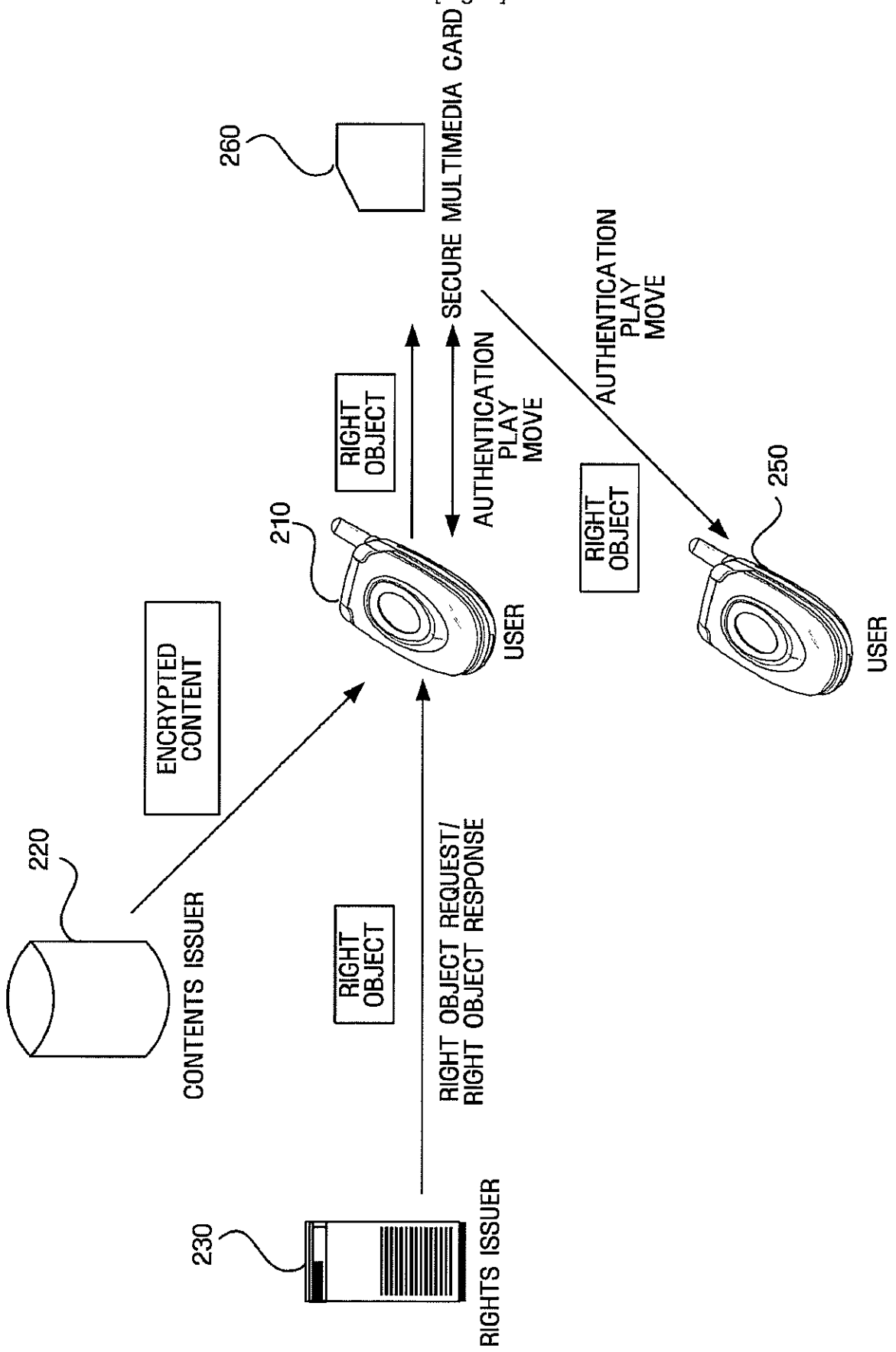
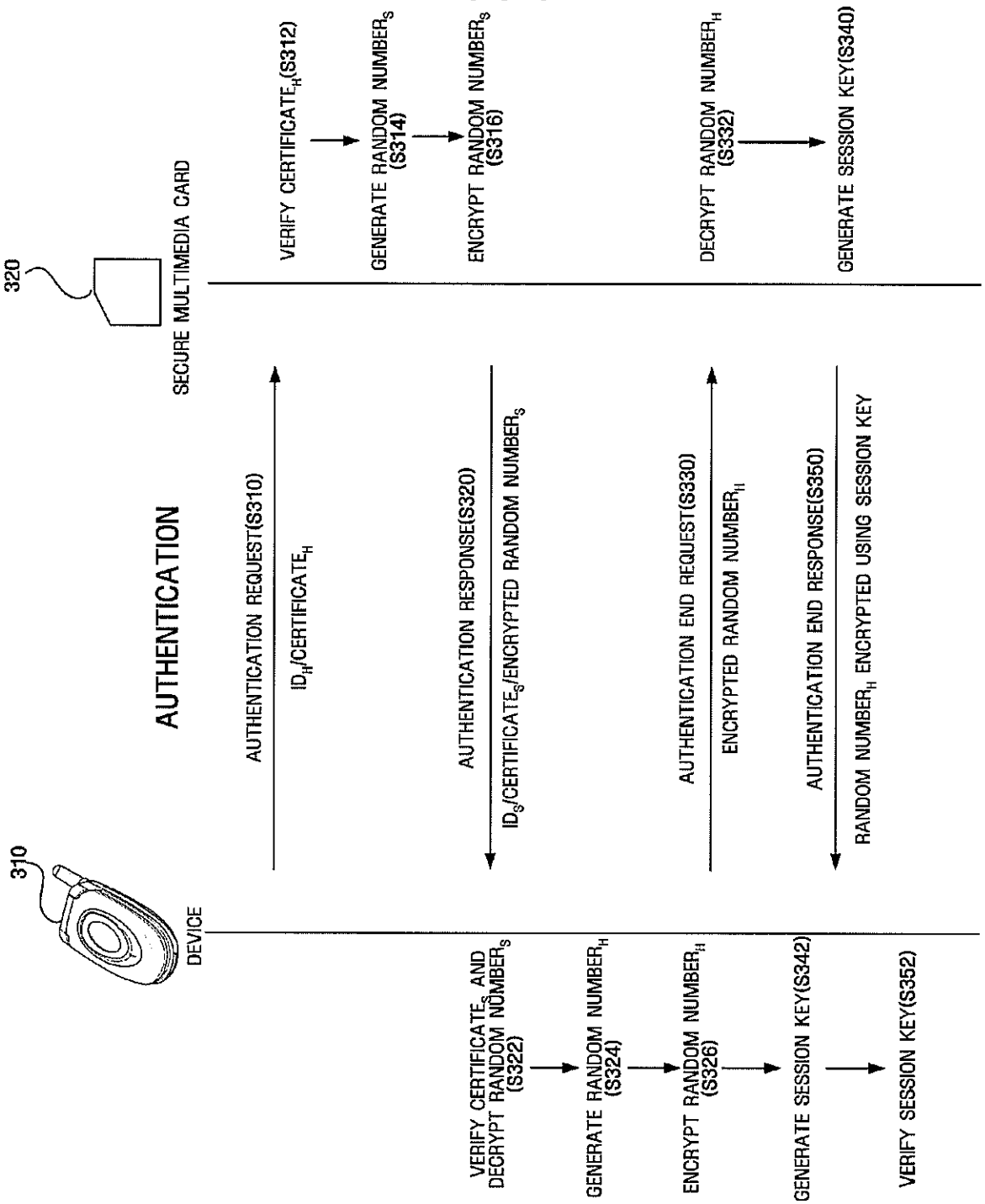
[Fig. 1]


150
USER
RIGHT OBJECT
ENCRYPTED CONTENT
CERTIFICATE
110
USER
RIGHT OBJECT
130
RIGHTS ISSUER
ENCRYPTED CONTENT
CERTIFICATE
CERTIFICATION AUTHORITY
140
RIGHTS ISSUING DETAILS REPORT
120
CONTENTS ISSUER
CERTIFICATE

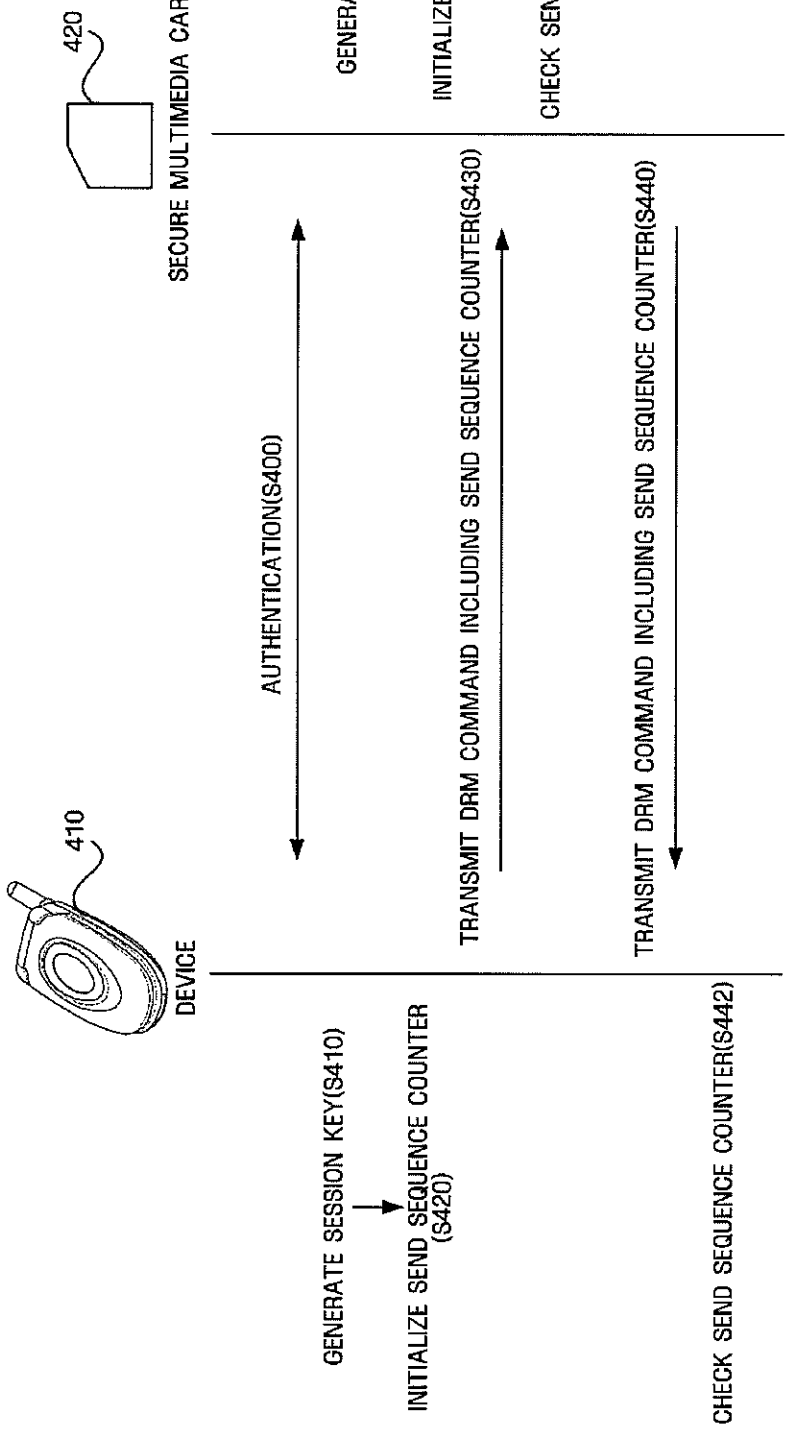
[Fig. 2]


260
SECURE MULTIMEDIA CARD
AUTHENTICATION
PLAY
MOVE
RIGHT
OBJECT
210
USER
AUTHENTICATION
PLAY
MOVE
RIGHT
OBJECT
250
USER
ENCRYPTED
CONTENT
220
CONTENTS ISSUER
RIGHT
OBJECT
RIGHT OBJECT REQUEST/
RIGHT OBJECT RESPONSE
230
RIGHTS ISSUER

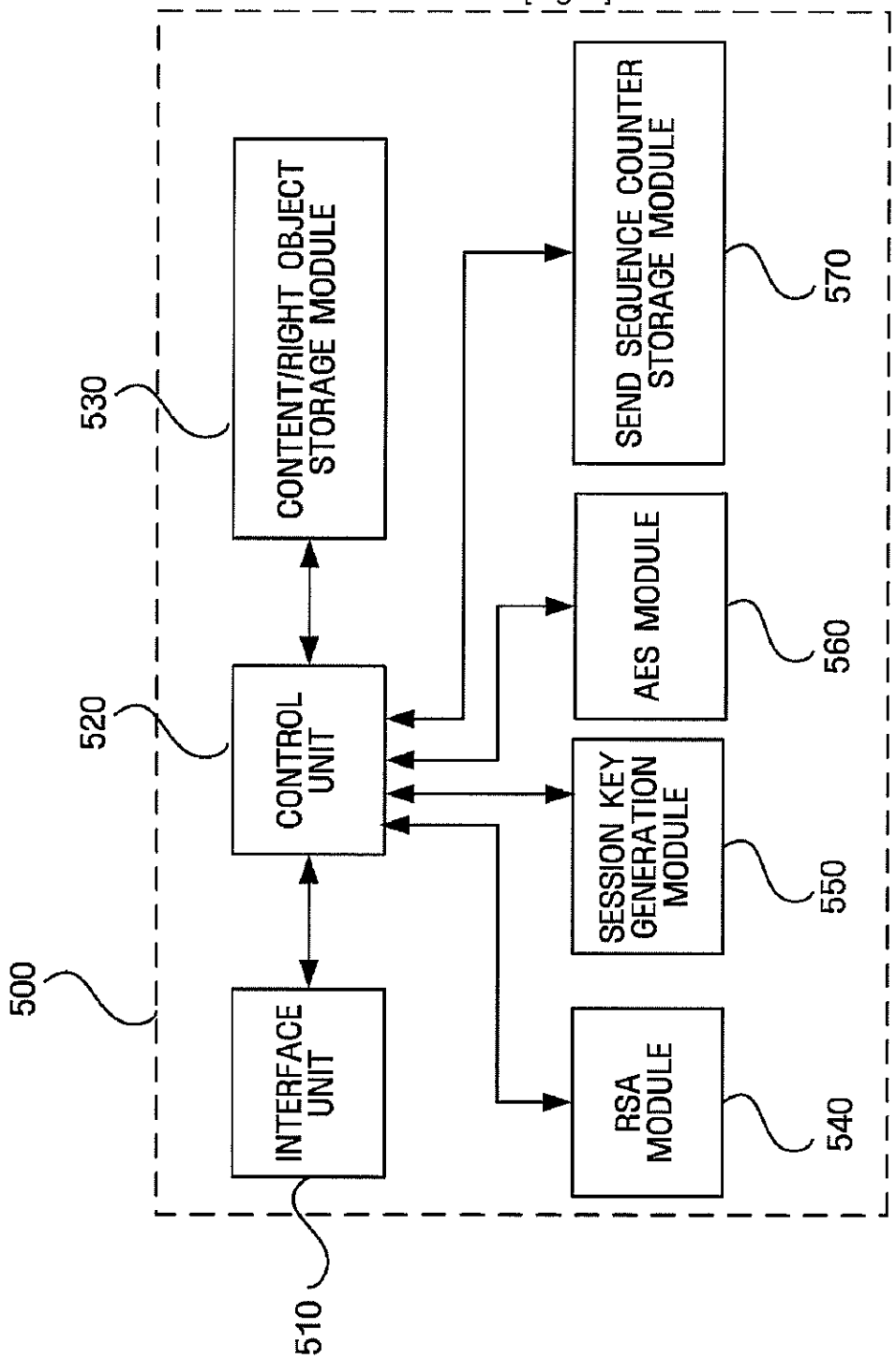
[Fig. 3]


320
SECURE MULTIMEDIA CARD
AUTHENTICATION
310
DEVICE
AUTHENTICATION REQUEST(S310)
ID_H/CERTIFICATE$_H$
AUTHENTICATION RESPONSE(S320)
ID_S/CERTIFICATE$_S$/ENCRYPTED RANDOM NUMBER$_S$
AUTHENTICATION END REQUEST(S330)
ENCRYPTED RANDOM NUMBER$_H$
AUTHENTICATION END RESPONSE(S350)
RANDOM NUMBER$_H$ ENCRYPTED USING SESSION KEY
VERIFY CERTIFICATE$_H$(S312)
GENERATE RANDOM NUMBER$_S$ (S314)
ENCRYPT RANDOM NUMBER$_S$ (S316)
DECRYPT RANDOM NUMBER$_H$ (S332)
GENERATE SESSION KEY(S340)
VERIFY CERTIFICATE$_S$ AND DECRYPT RANDOM NUMBER$_S$ (S322)
GENERATE RANDOM NUMBER$_H$ (S324)
ENCRYPT RANDOM NUMBER$_H$ (S326)
GENERATE SESSION KEY(S342)
VERIFY SESSION KEY(S352)

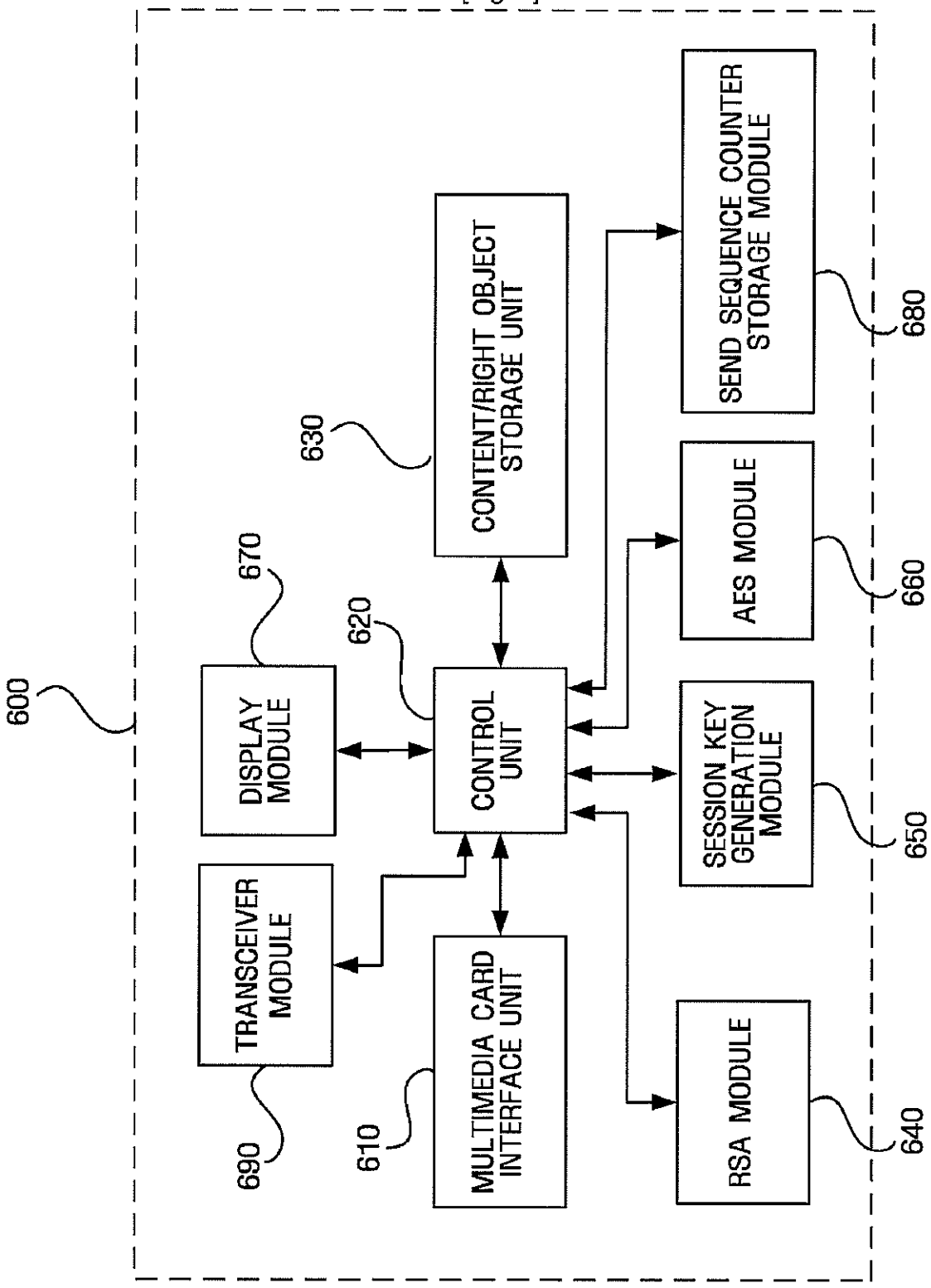
[Fig. 4]


410
DEVICE
420
SECURE MULTIMEDIA CARD
GENERATE SESSION KEY(S410)
INITIALIZE SEND SEQUENCE COUNTER (S420)
GENERATE SESSION KEY(S412)
INITIALIZE SEND SEQUENCE COUNTER (S422)
AUTHENTICATION(S400)
TRANSMIT DRM COMMAND INCLUDING SEND SEQUENCE COUNTER(S430)
CHECK SEND SEQUENCE COUNTER(S432)
TRANSMIT DRM COMMAND INCLUDING SEND SEQUENCE COUNTER(S440)
CHECK SEND SEQUENCE COUNTER(S442)

[Fig. 5]


500
510
INTERFACE UNIT
520
CONTROL UNIT
530
CONTENT/RIGHT OBJECT STORAGE MODULE
540
RSA MODULE
550
SESSION KEY GENERATION MODULE
560
AES MODULE
570
SEND SEQUENCE COUNTER STORAGE MODULE

[Fig. 6]


600
CONTROL UNIT
620
DISPLAY MODULE
670
TRANSCEIVER MODULE
690
MULTIMEDIA CARD INTERFACE UNIT
610
CONTENT/RIGHT OBJECT STORAGE UNIT
630
SEND SEQUENCE COUNTER STORAGE MODULE
680
AES MODULE
660
SESSION KEY GENERATION MODULE
650
RSA MODULE
640