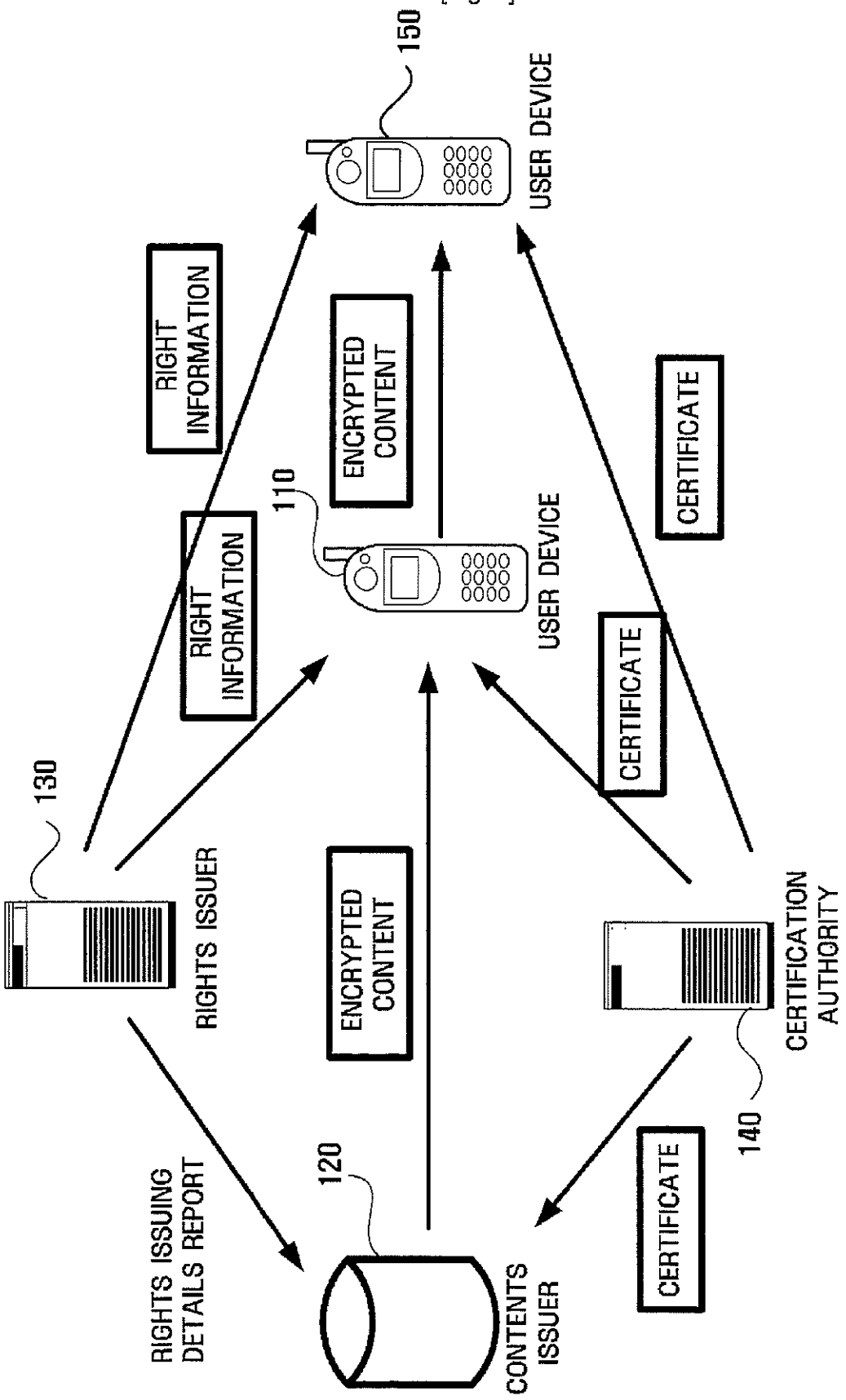
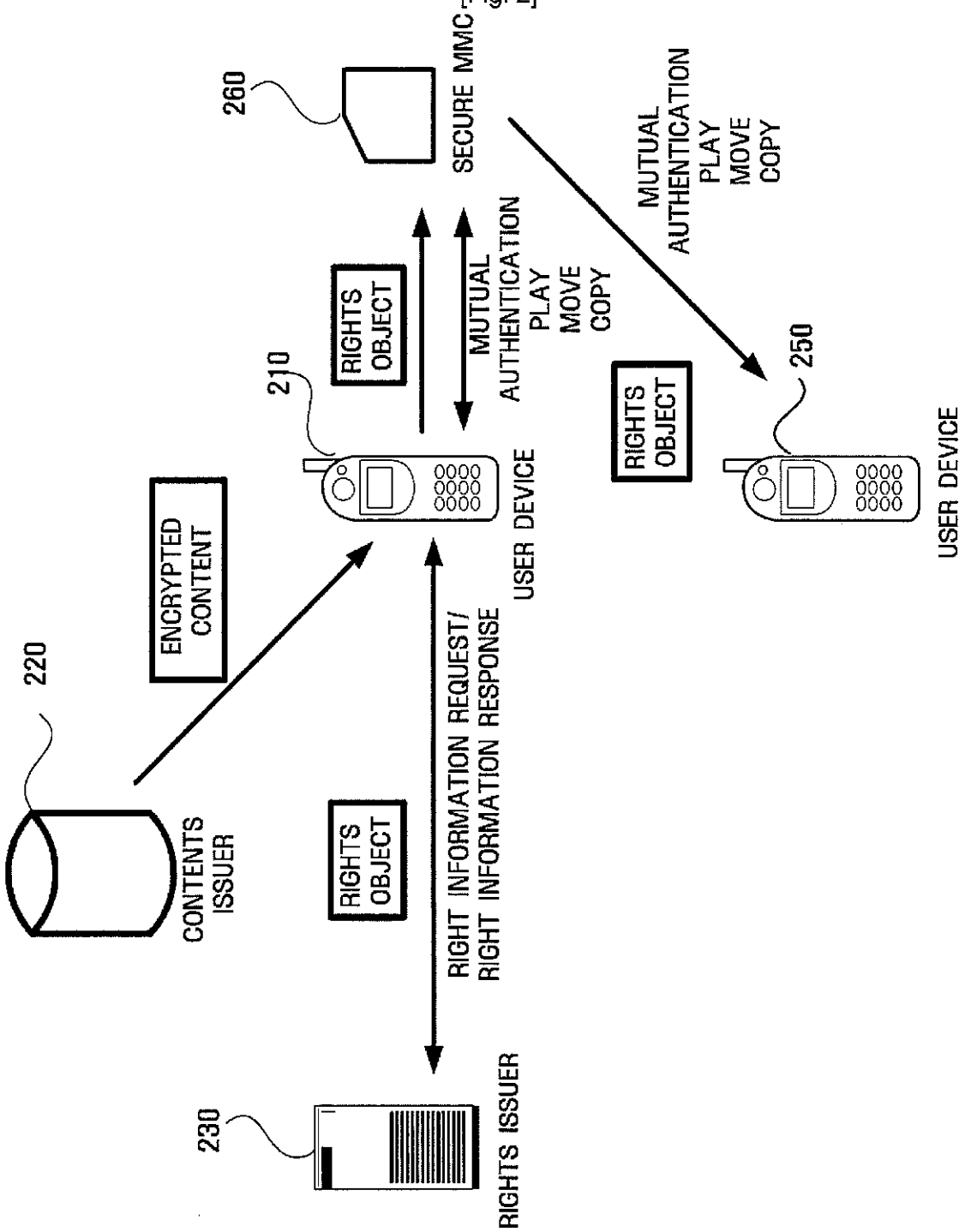
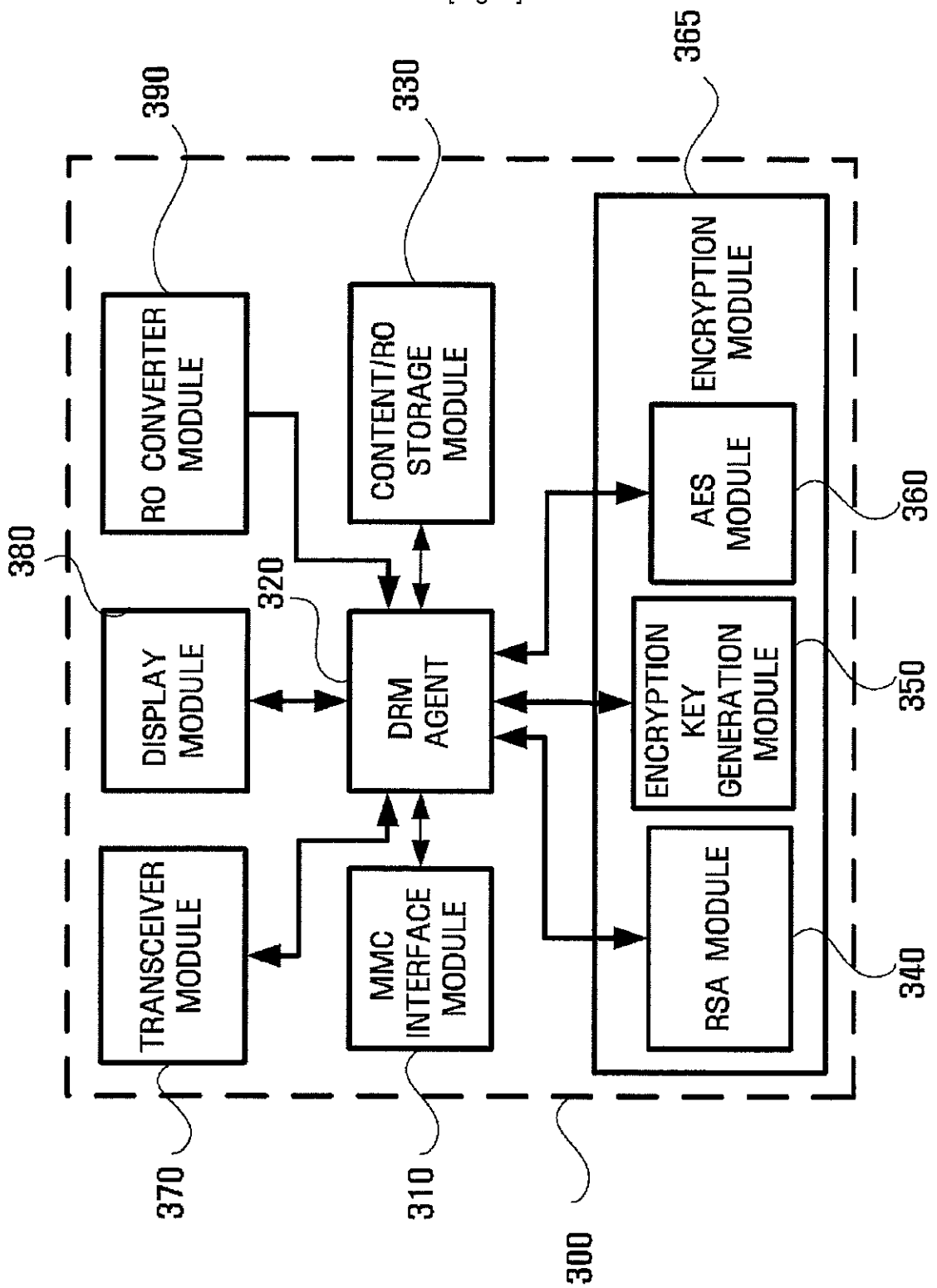
[Fig. 1]


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

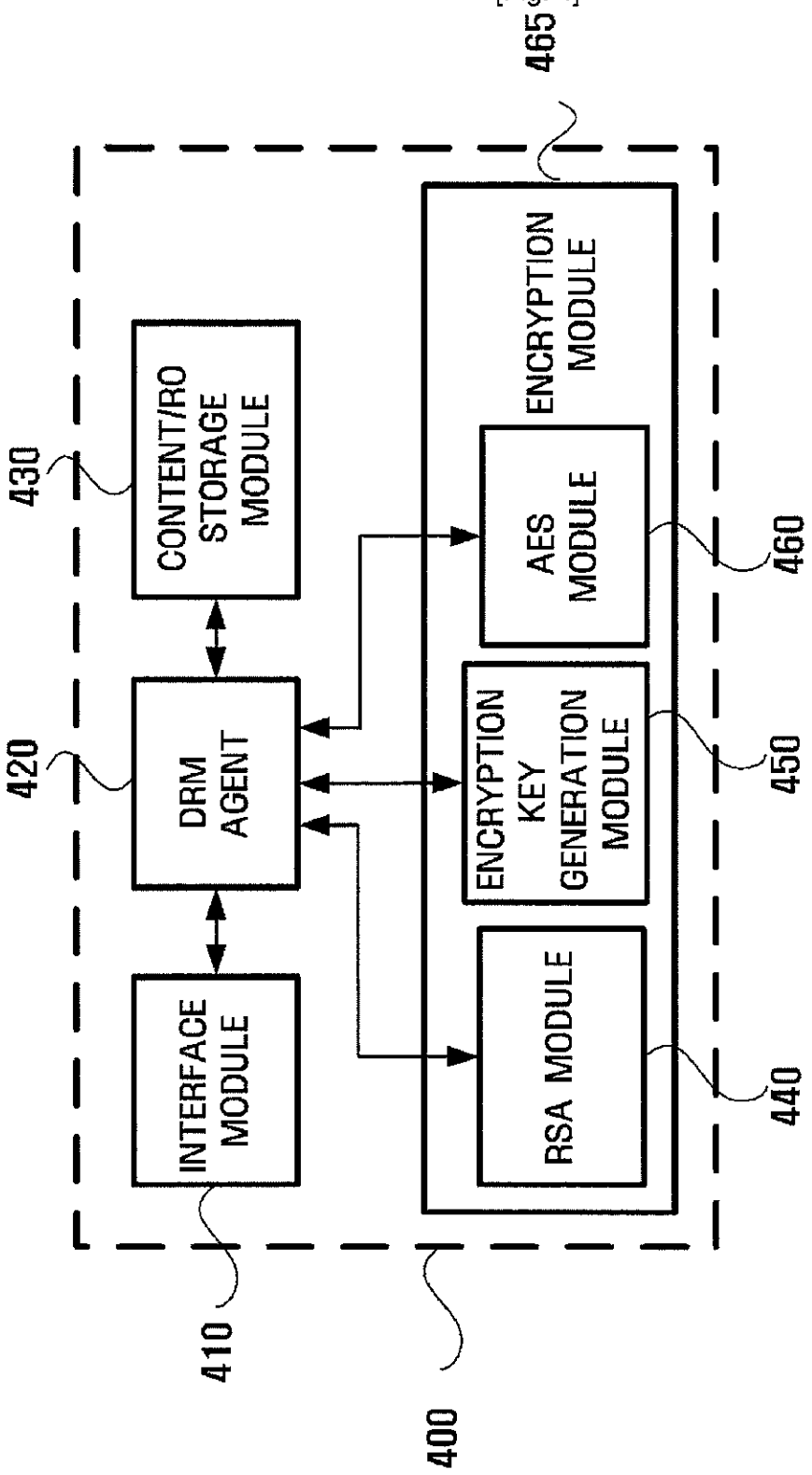
[Fig. 2]

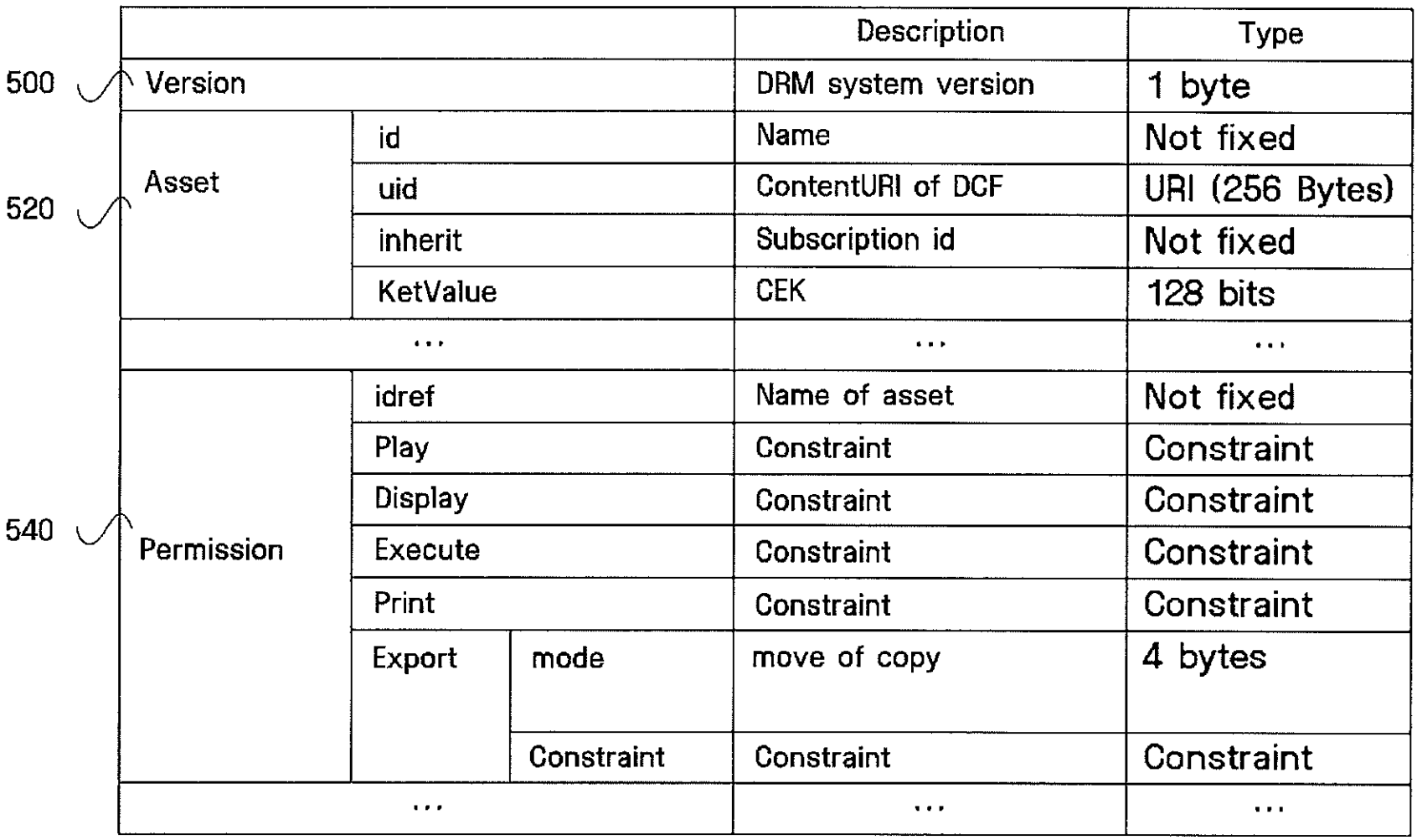

220
CONTENTS ISSUER
ENCRYPTED CONTENT
RIGHTS OBJECT
RIGHT INFORMATION REQUEST/
RIGHT INFORMATION RESPONSE
230
RIGHTS ISSUER
210
USER DEVICE
RIGHTS OBJECT
MUTUAL AUTHENTICATION
PLAY
MOVE
COPY
260
SECURE MMC
MUTUAL AUTHENTICATION
PLAY
MOVE
COPY
RIGHTS OBJECT
250
USER DEVICE

[Fig. 3]


390
330
365
RO CONVERTER MODULE
CONTENT/RO STORAGE MODULE
ENCRYPTION MODULE
380
320
DISPLAY MODULE
DRM AGENT
AES MODULE
360
ENCRYPTION KEY GENERATION MODULE
350
TRANSCEIVER MODULE
MMC INTERFACE MODULE
RSA MODULE
340
370
310
300

[Fig. 4]


400
410
420
430
440
450
460
465
INTERFACE MODULE
DRM AGENT
CONTENT/RO STORAGE MODULE
RSA MODULE
ENCRYPTION KEY GENERATION MODULE
AES MODULE
ENCRYPTION MODULE



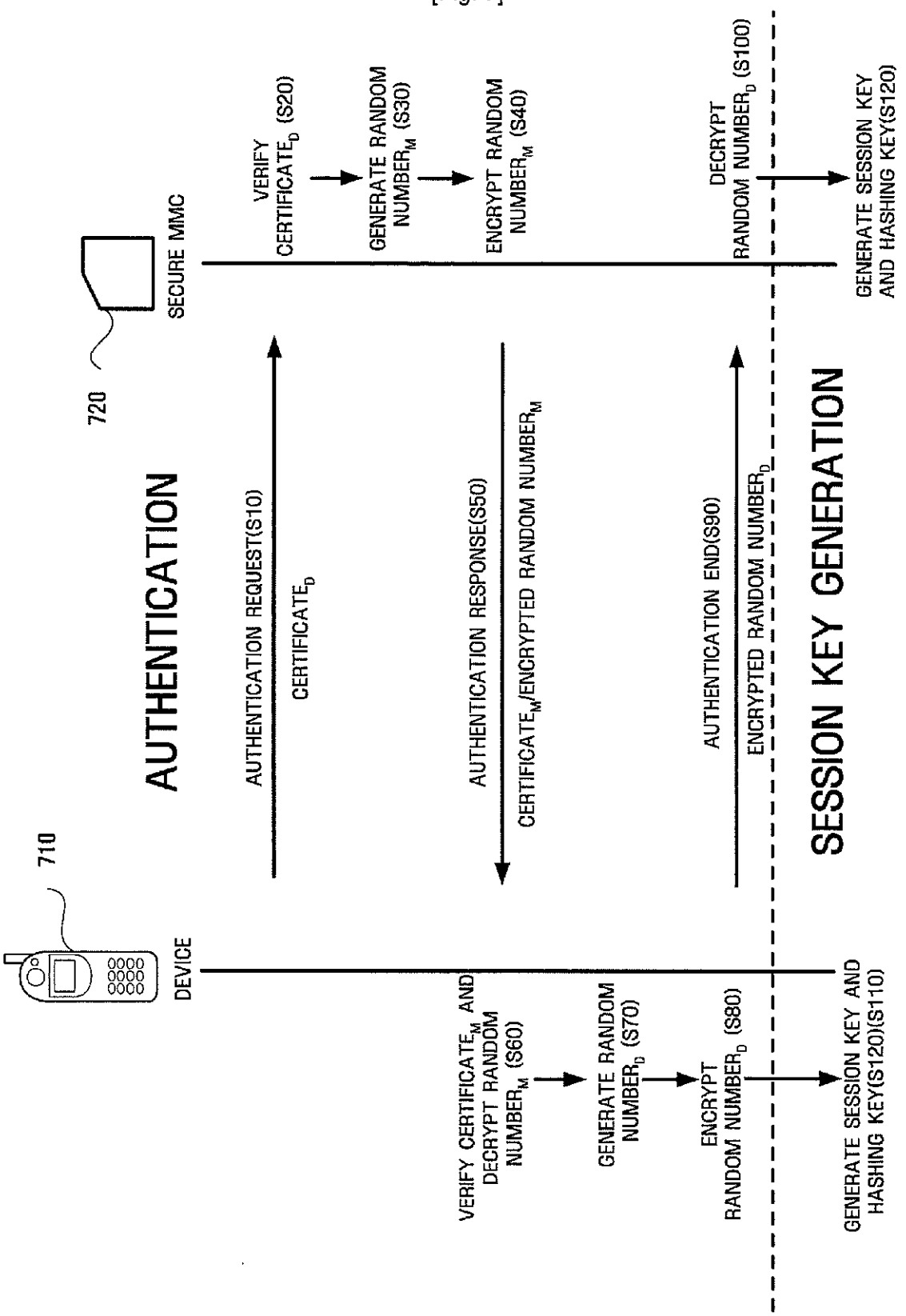
			Description	Type
500	Version		DRM system version	1 byte
520	Asset	id	Name	Not fixed
		uid	ContentURI of DCF	URI (256 Bytes)
		inherit	Subscription id	Not fixed
		KetValue	CEK	128 bits
	...		...	...
540	Permission	idref	Name of asset	Not fixed
		Play	Constraint	Constraint
		Display	Constraint	Constraint
		Execute	Constraint	Constraint
		Print	Constraint	Constraint
		Export mode	move of copy	4 bytes
		Export Constraint	Constraint	Constraint
	...		...	...

[Fig. 5]

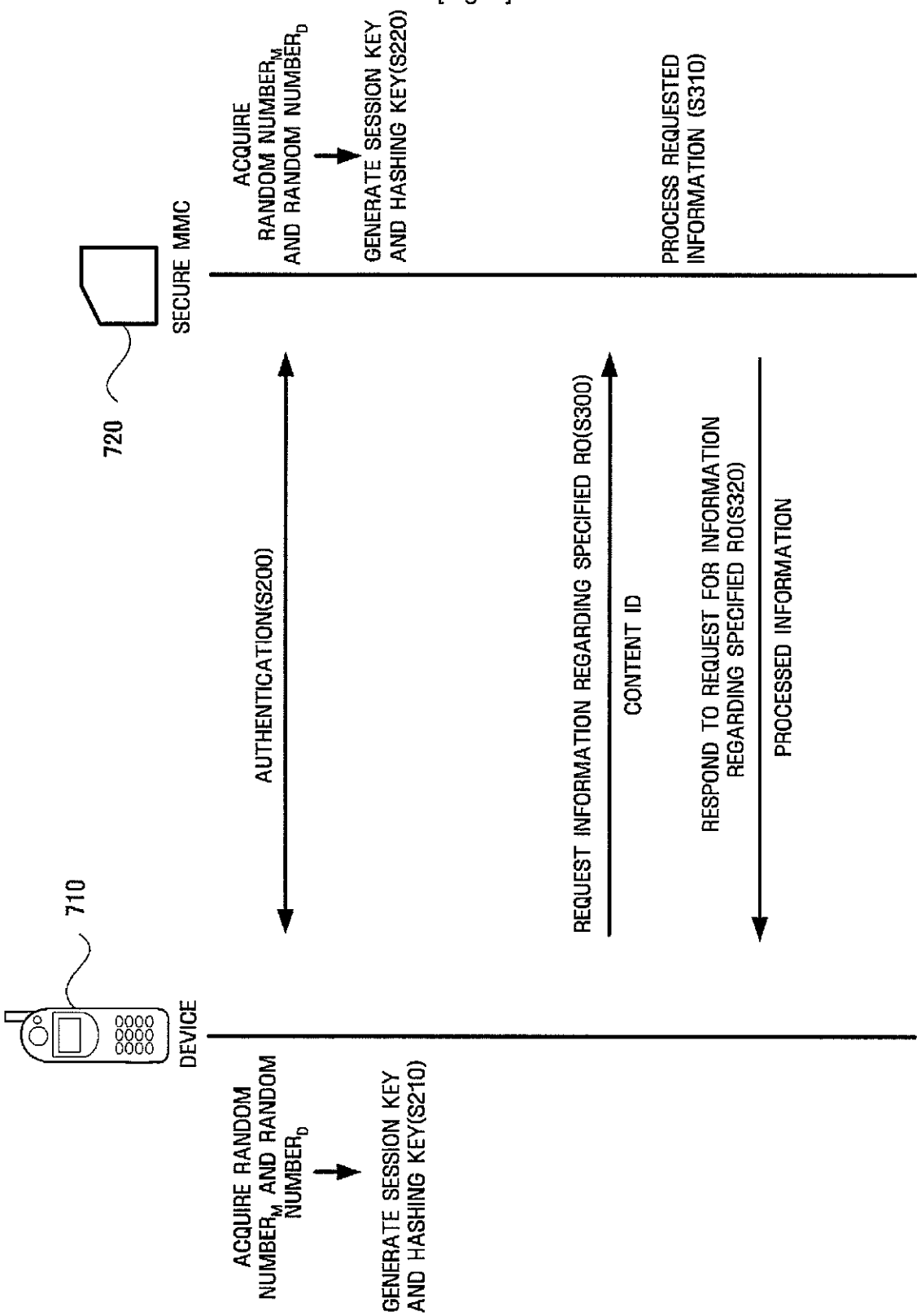
	Constraint		Description	Type
600	Count		Positive integer	1 byte
610	Datetime	start	CCYY-MM-DDThh:mm:ss	[ISO8601] (19 b)
		end	CCYY-MM-DDThh:mm:ss	[ISO8601] (19 b)
620	Interval	duration	PnDTnHnMnS	[ISO8601]
		start	CCYY-MM-DDThh:mm:ss	[ISO8601] (19 b)
		end	CCYY-MM-DDThh:mm:ss	[ISO8601] (19 b)
630	Accumulated		PnDTnHnMnS	[ISO8601] (19 b)
640	Individual		URI	15 bytes or 24 bytes
650	System	Version	Version of target DRM system	1 byte
		uid	Name of target DRM system	Not fixed

[Fig. 6]

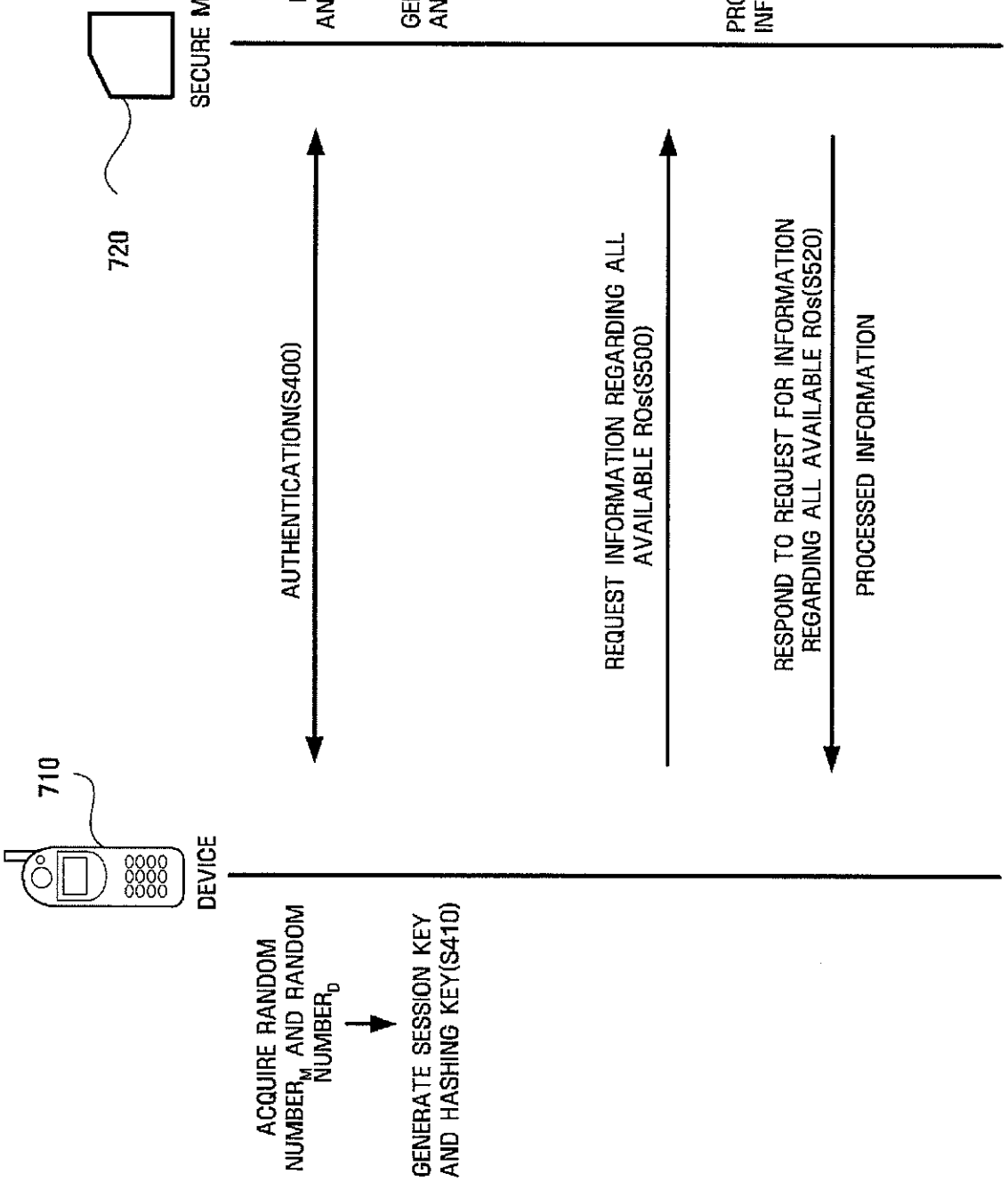
[Fig. 7]


710
DEVICE
720
SECURE MMC
AUTHENTICATION
SESSION KEY GENERATION
AUTHENTICATION REQUEST(S10)
CERTIFICATE$_D$
VERIFY CERTIFICATE$_D$ (S20)
GENERATE RANDOM NUMBER$_M$ (S30)
ENCRYPT RANDOM NUMBER$_M$ (S40)
AUTHENTICATION RESPONSE(S50)
CERTIFICATE$_M$/ENCRYPTED RANDOM NUMBER$_M$
VERIFY CERTIFICATE$_M$ AND DECRYPT RANDOM NUMBER$_M$ (S60)
GENERATE RANDOM NUMBER$_D$ (S70)
ENCRYPT RANDOM NUMBER$_D$ (S80)
AUTHENTICATION END(S90)
ENCRYPTED RANDOM NUMBER$_D$
DECRYPT RANDOM NUMBER$_D$ (S100)
GENERATE SESSION KEY AND HASHING KEY(S120)(S110)
GENERATE SESSION KEY AND HASHING KEY(S120)

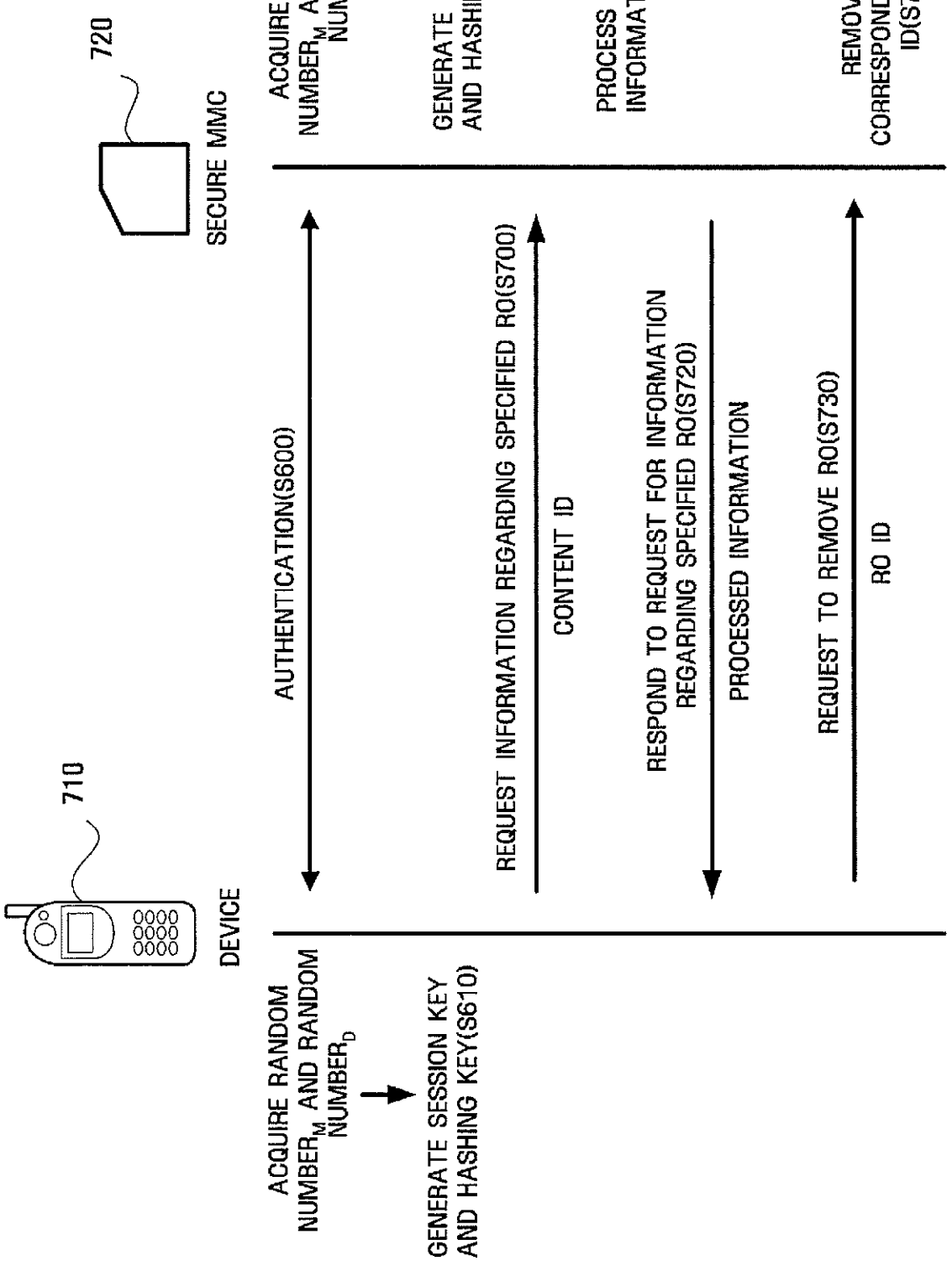
[Fig. 8]


710
DEVICE
720
SECURE MMC
ACQUIRE RANDOM NUMBER$_M$ AND RANDOM NUMBER$_D$
GENERATE SESSION KEY AND HASHING KEY(S210)
ACQUIRE RANDOM NUMBER$_M$ AND RANDOM NUMBER$_D$
GENERATE SESSION KEY AND HASHING KEY(S220)
AUTHENTICATION(S200)
REQUEST INFORMATION REGARDING SPECIFIED RO(S300)
CONTENT ID
RESPOND TO REQUEST FOR INFORMATION REGARDING SPECIFIED RO(S320)
PROCESSED INFORMATION
PROCESS REQUESTED INFORMATION (S310)

[Fig. 9]


710
DEVICE
720
SECURE MMC
ACQUIRE RANDOM NUMBER$_M$ AND RANDOM NUMBER$_D$
GENERATE SESSION KEY AND HASHING KEY(S410)
AUTHENTICATION(S400)
ACQUIRE RANDOM NUMBER$_M$ AND RANDOM NUMBER$_D$
GENERATE SESSION KEY AND HASHING KEY(S420)
REQUEST INFORMATION REGARDING ALL AVAILABLE ROs(S500)
PROCESS REQUESTED INFORMATION (S510)
RESPOND TO REQUEST FOR INFORMATION REGARDING ALL AVAILABLE ROs(S520)
PROCESSED INFORMATION

[Fig. 10]


710
DEVICE
720
SECURE MMC
ACQUIRE RANDOM NUMBER$_M$ AND RANDOM NUMBER$_D$
GENERATE SESSION KEY AND HASHING KEY(S610)
AUTHENTICATION(S600)
ACQUIRE RANDOM NUMBER$_M$ AND RANDOM NUMBER$_D$
GENERATE SESSION KEY AND HASHING KEY(S620)
REQUEST INFORMATION REGARDING SPECIFIED RO(S700)
CONTENT ID
PROCESS REQUESTED INFORMATION (S710)
RESPOND TO REQUEST FOR INFORMATION REGARDING SPECIFIED RO(S720)
PROCESSED INFORMATION
REQUEST TO REMOVE RO(S730)
RO ID
REMOVE RO CORRESPONDING TO RO ID(S740)

[Fig. 11]

- INSTRUCTION(1100)

CLA	INS	PI	P2	Lc	Data Field	Le
00	76	01	01	FF	TLV	00

[Fig. 12]

- INSTRUCTION PARAMETERS(1120)

P1	P2	Description
01	01	-P1:INSTRUCTION FOR ACQUIRING INFORMATION REGARDING RO -P2:SETTING OF CONTENT ID

[Fig. 13]

- INSTRUCTION PARAMETERS(1120)

		Description
Lc		FF
Date Field	T	0x76
	L	LENGTH OF V
	V	CONTENT ID OR PARENT RO ID
Le		00

[Fig. 14]

- OUTPUT RESPONSE(1140)

Data field	Description
T	None
L	None
V	None

[Fig. 15]

- OUTPUT RESPONSE(1140)

STATUS WORD		Description
SW1	SW2	
90	00	SUCCESSFUL EXECUTION OF INSTRUCTION
6D	00	UNKNOWN TAG
6B	00	WRONG PARAMETER IN V-FIELD
69	82	GENERAL AUTHENTICATION NEEDED
	85	AUTHENTICATION NEEDED
6A	83	CONTENT NOT EXIST
66	03	RO NOT EXIST

[Fig. 16]

- INSTRUCTION(1200)

CLA	INS	PI	P2	Lc	Data Field	Le
00	76	01	02	00	None	FF

[Fig. 17]

- INSTRUCTION PARAMETERS(1220)

P1	P2	Description
01	02	-P1:INSTRUCTION FOR ACQUIRING INFORMATION REGARDING RO -P2:ACQUIRING OF INFORMATION REGARDING RO

[Fig. 18]

- INSTRUCTION PARAMETERS(1220)

		Description
Lc		00
Date Field	T	None
	L	None
	V	None
Le		FF

[Fig. 19]

- OUTPUT RESPONSE(1240)

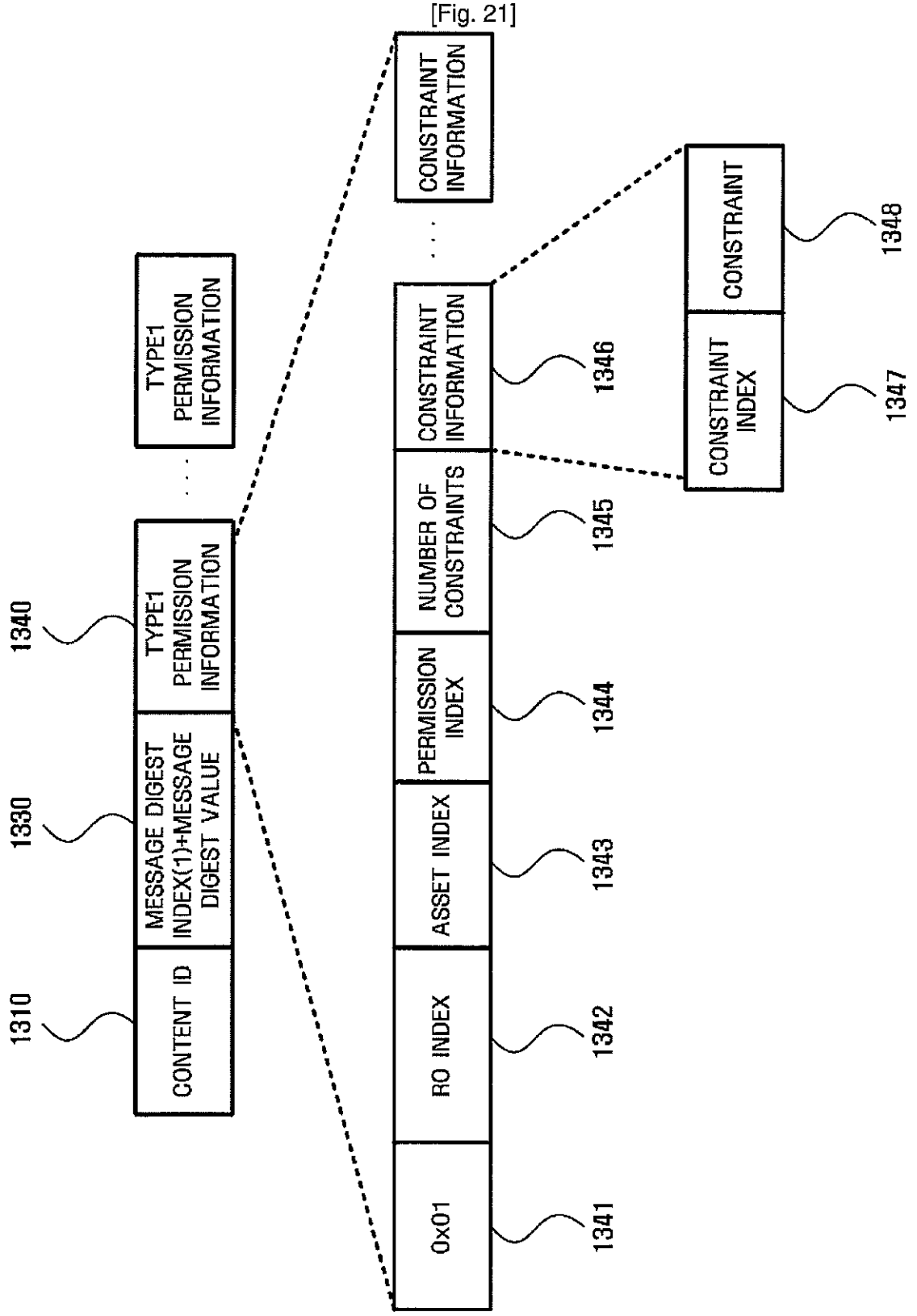
Data field	Description
T	0x76
L	LENGTH OF V
V	CPSF* ‖ H(K, CPSF*)

[Fig. 20]

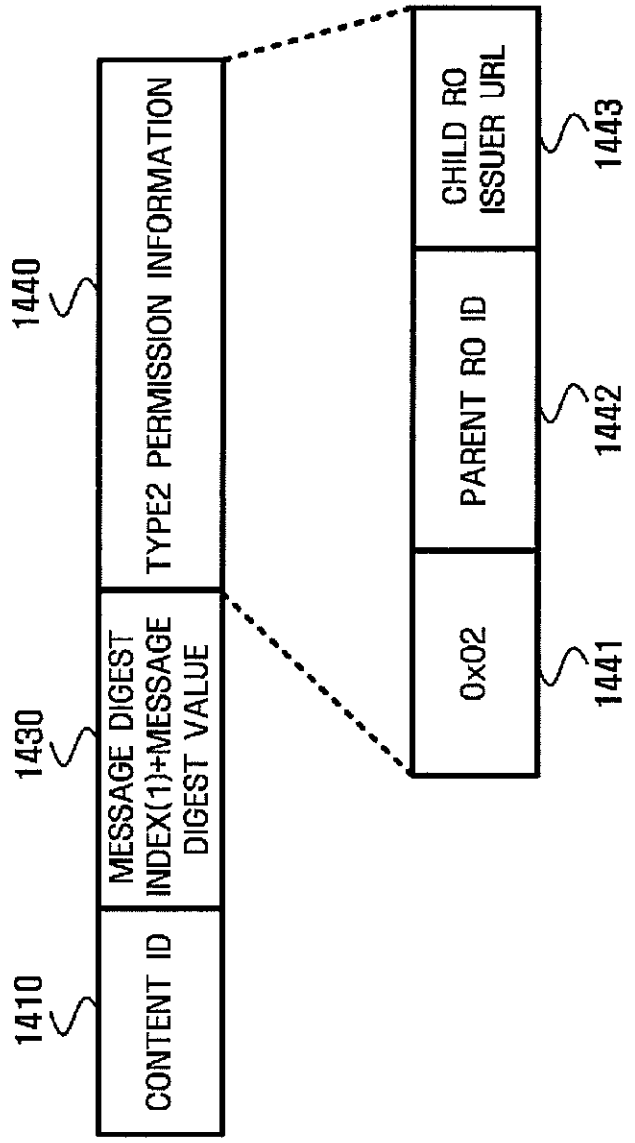
- OUTPUT RESPONSE(1240)

STATUS WORD		Description
SW1	SW2	
90	00	SUCCESSFUL EXECUTION OF INSTRUCTION
6D	00	UNKNOWN TAG
6B	00	WRONG PARAMETER IN V-FIELD
69	82	GENERAL AUTHENTICATION NEEDED
	85	AUTHENTICATION NEEDED

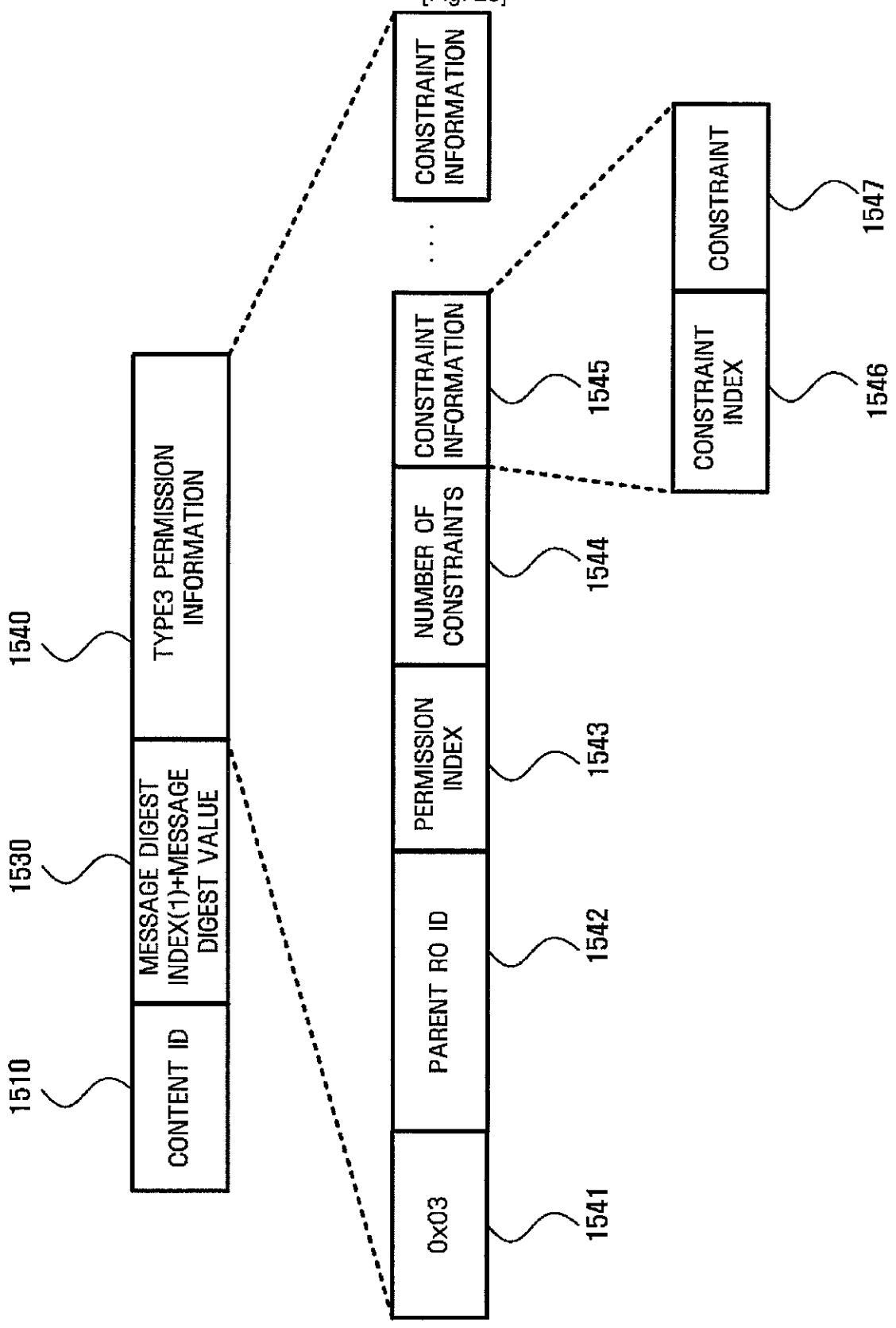
[Fig. 21]


1310
CONTENT ID
1330
MESSAGE DIGEST INDEX(1)+MESSAGE DIGEST VALUE
1340
TYPE1 PERMISSION INFORMATION
TYPE1 PERMISSION INFORMATION
0x01
1341
RO INDEX
1342
ASSET INDEX
1343
PERMISSION INDEX
1344
NUMBER OF CONSTRAINTS
1345
CONSTRAINT INFORMATION
1346
CONSTRAINT INFORMATION
CONSTRAINT INDEX
1347
CONSTRAINT
1348

[Fig. 22]


1410
CONTENT ID
1430
MESSAGE DIGEST INDEX(1)+MESSAGE DIGEST VALUE
1440
TYPE2 PERMISSION INFORMATION
1441
0x02
1442
PARENT RO ID
1443
CHILD RO ISSUER URL

[Fig. 23]


CONTENT ID
1510
MESSAGE DIGEST INDEX(1)+MESSAGE DIGEST VALUE
1530
TYPE3 PERMISSION INFORMATION
1540
0x03
1541
PARENT RO ID
1542
PERMISSION INDEX
1543
NUMBER OF CONSTRAINTS
1544
CONSTRAINT INFORMATION
1545
CONSTRAINT INDEX
1546
CONSTRAINT
1547
CONSTRAINT INFORMATION
. . .

[Fig. 24]

- INSTRUCTION(1600)

CLA	INS	PI	P2	Lc	Data Field	Le
00	76	02	01	00	None	FF

[Fig. 25]

- INSTRUCTION PARAMETERS(1620)

P1	P2	Description
02	01	-P1:INSTRUCTION FOR ACQUIRING INFORMATION OF RO LIST -P2:ACQUIRING OF INFORMATION REGARDING ALL AVAILABLE ROs

[Fig. 26]

- INSTRUCTION PARAMETERS(1620)

		Description
Lc		00
Date Field	T	None
	L	None
	V	None
Le		FF

[Fig. 27]

- OUTPUT RESPONSE(1640)

Data field	Description
T	0x76
L	LENGTH OF V
V	ADDITIONAL INFORMATION :: RO LIST INFORMATION :: H(K,RO LIST INFORMATION)

[Fig. 28]

- OUTPUT RESPONSE(1640)

STATUS WORD		Description
SW1	SW2	
90	00	SUCCESSFUL EXECUTION OF INSTRUCTION
6D	00	UNKNOWN TAG
6B	00	WRONG PARAMETER IN V-FIELD
69	82	GENERAL AUTHENTICATION NEEDED
	85	AUTHENTICATION NEEDED

[Fig. 29]

INSTRUCTION

CLA	INS	P1	P2	Lc	Data Field	Le
00	76	03	01	FF	TLV	00

[Fig. 30]

INSTRUCTION PARAMETERS

P1	P2	Description
03	01	-P1:INSTRUCTION FOR REMOVING RO -P2:REMOVING OF ONE RO

[Fig. 31]

INSTRUCTION PARAMETERS

		Description
Lc		FF
Data Field	T	0x76
	L	The length of field V
	V	E(K,RID)
Le		00

[Fig. 32]

OUTPUT RESPONSE

Data Field	Description
T	None
L	None
V	None

[Fig. 33]

OUTPUT RESPONSE

Status Word		Description
SW1	SW1	
90	00	SUCCESSFUL EXECUTION OF INSTRUCTION
6D	00	UNKNOWN TAG
6B	00	WRONG PARAMETER IN V-FIELD
69	82	GENERAL AUTHENTICATION NEEDED
	85	AUTHENTICATION NEEDED