

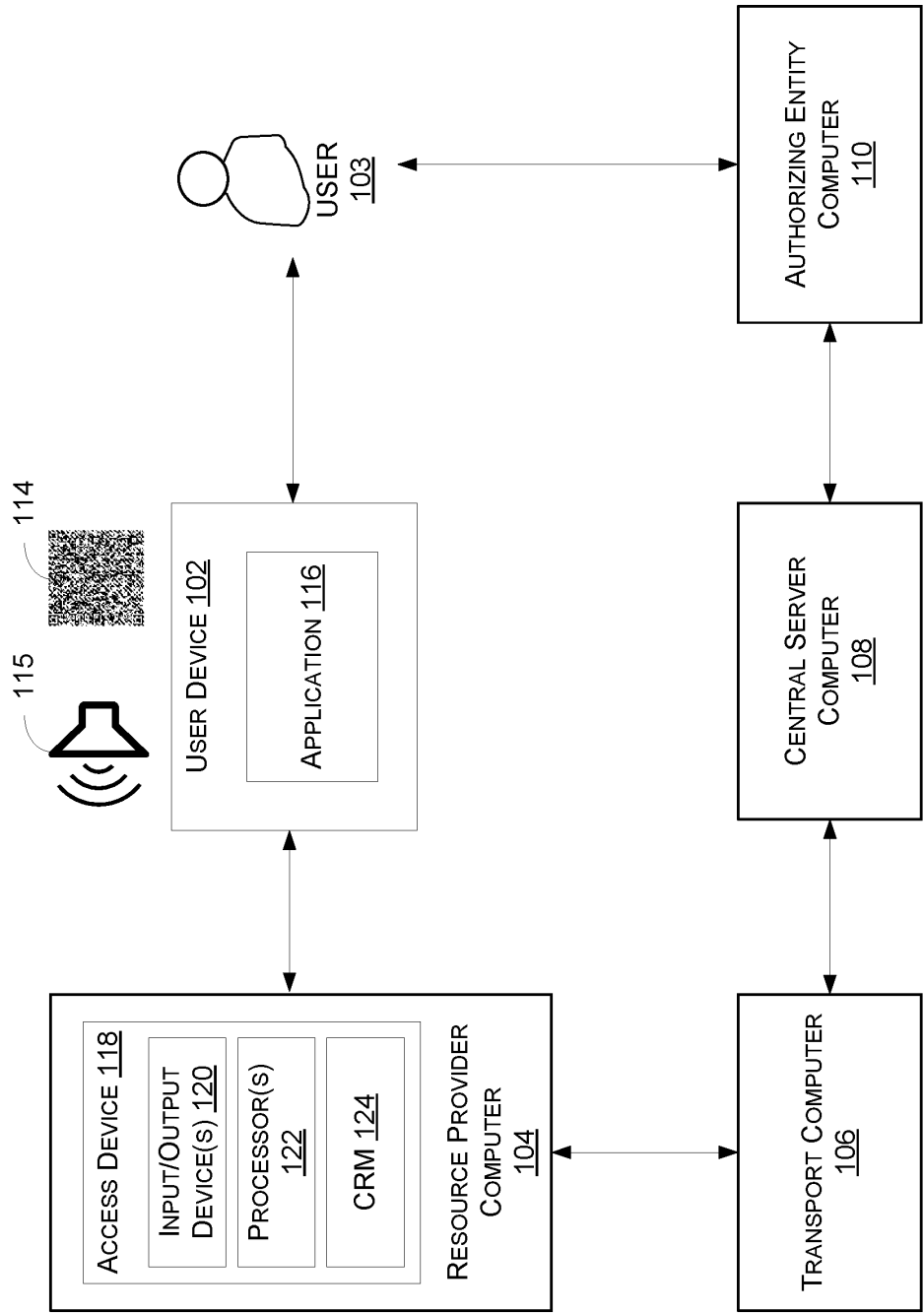


FIG. 1

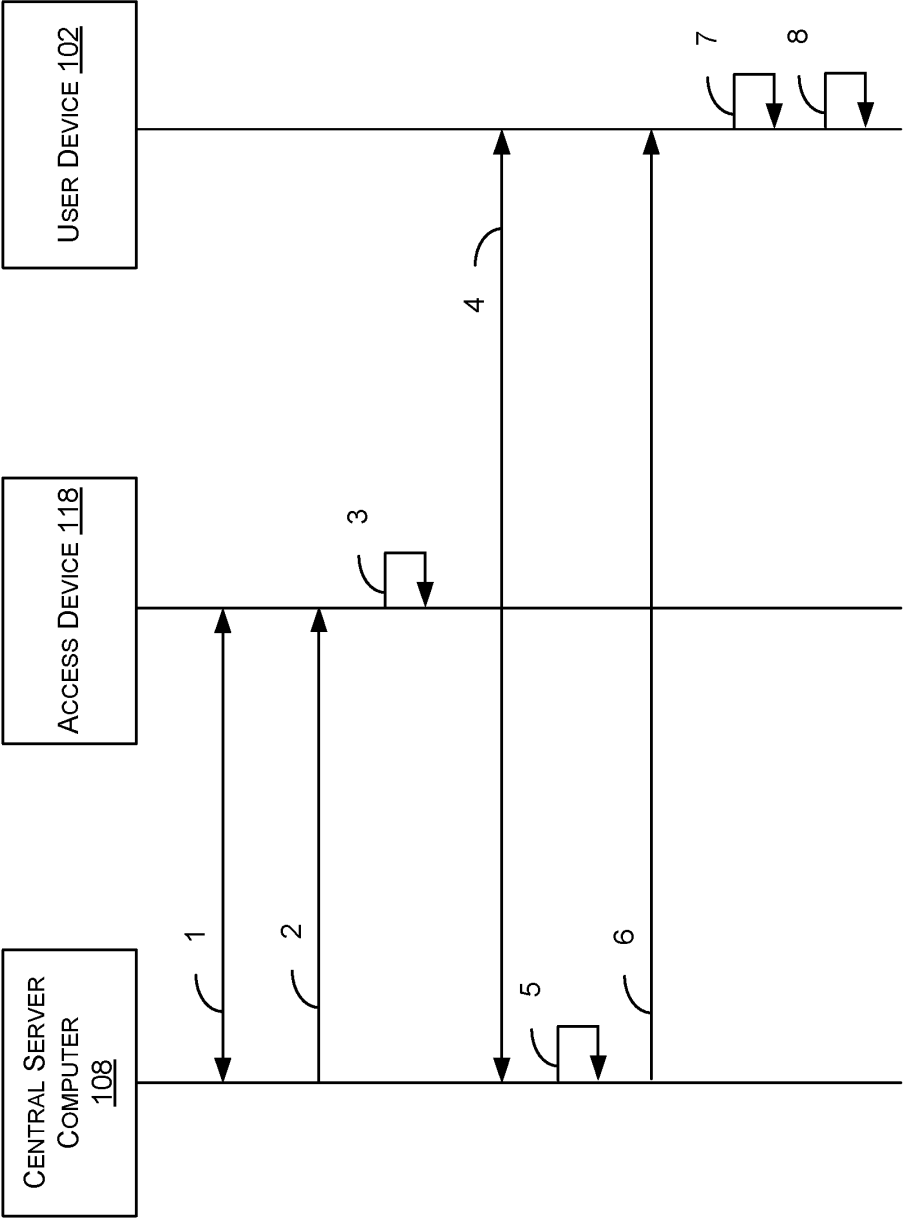


FIG. 2

	NAME	DESCRIPTION	LENGTH (BYTES)
1	CERTIFICATE FORMAT	'14'	1
2	CERTIFICATE ENCODING	'00'	1
3	SUITE INDICATOR	IDENTIFIES THE ALGORITHM SUITE TO BE USED WITH THE CERTIFIED DEVICE PUBLIC KEY	1
4	CERTIFICATE EXPIRY DATE	YYYYMMDD, UTC	4
5	CERTIFICATE EXPIRY TIME	HHMM, UTC	2
6	CERTIFICATE SERIAL NUMBER	IDENTIFIER UNIQUE TO THE CA KEY THAT CREATES THE DEVICE CERTIFICATE	6
7	DEVICE PUBLIC KEY	REPRESENTATION OF THE DEVICE PUBLIC KEY (E.G., X- COORDINATE OF THE PUBLIC KEY POINT) ON THE CURVE IDENTIFIED BY THE SUITE INDICATOR DATA FIELD	NFIELD
8	PUBLIC KEY CERTIFICATE SIGNATURE	DIGITAL SIGNATURE ON THE DATA FIELDS 1-7 . VERIFIABLE USING THE PUBLIC KEY OF THE CERTIFICATE AUTHORITY AND THE ALGORITHM ASSOCIATED WITH THE SUITE INDICATOR	VARIES

FIG. 3

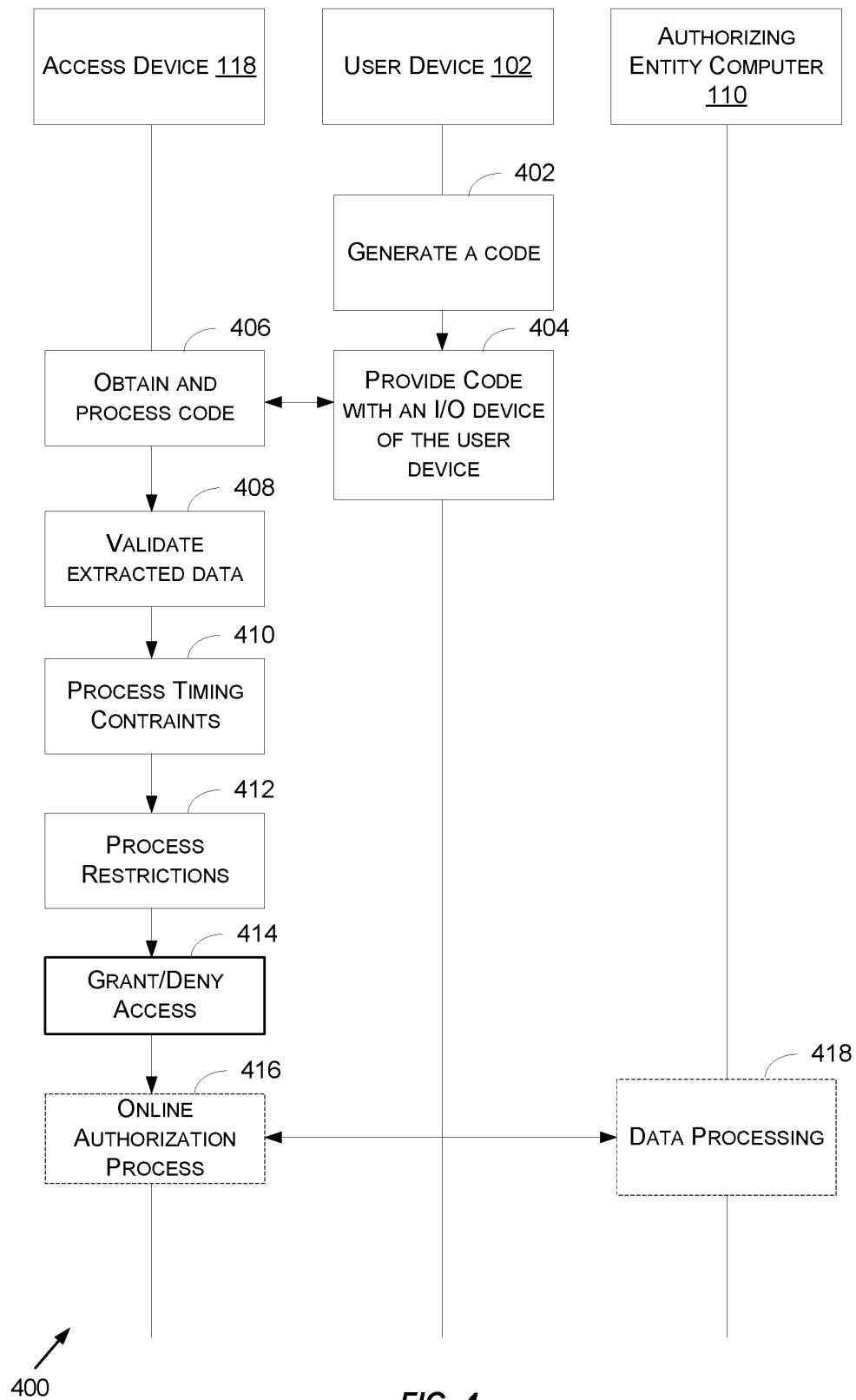
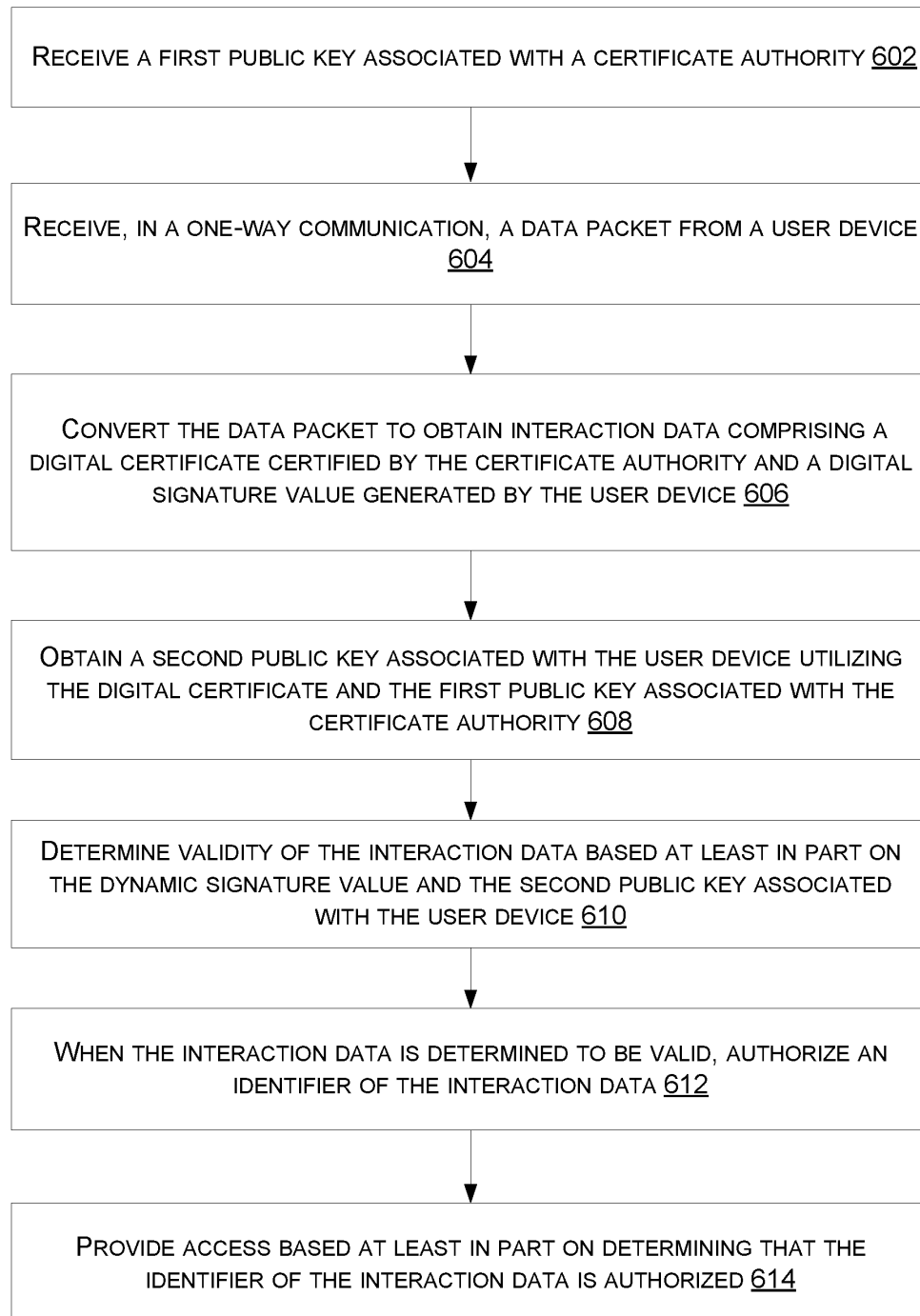


FIG. 4

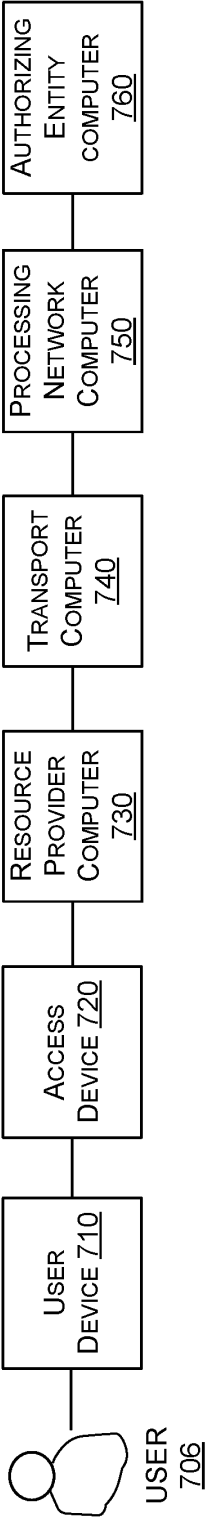
Tag	Data Object	Length (Bytes)	Content
85	PAYLOAD FORMAT INDICATOR	5	DEFINES VERSION OF THE GENERATED CODE (E.G., "CPV01")
61	APPLICATION TEMPLATE	VARIES	TEMPLATE CONTAINING APPLICATION SPECIFIC DATA
	4F ADF NAME	5-16	IDENTIFIES AN APPLICATION.
62	COMMON DATA TEMPLATE	VARIES	TEMPLATE CONTAINING APPLICATION DATA THAT IS COMMON ACROSS APPLICATIONS
	57 TRACK 2 EQUIVALENT DATA	VARIES UP TO 19	CONTAINS THE EQUIVALENT OF TRACK 2 DATA AS DEFINED IN ISO 7813
	82 APPLICATION INTERCHANGE PROFILE	2	CONTAINS DATA FOR TRANSITION TO AUTHORIZING ENTITY AND/OR CENTRAL SERVER COMPUTER
	9F10 APPLICATION DATA	VARIES UP TO 32	CONTAINS DATA FOR TRANSITION TO AUTHORIZING ENTITY AND/OR CENTRAL SERVER COMPUTER
	9F26 APPLICATION CRYPTOGRAM	8	CRYPTOGRAM GENERATED BY THE APPLICATION
	9F36 TIMESTAMP P1	2	TIMESTAMP OF WHEN QR CODE WAS GENERATED, PART 1
	9F27 TIMESTAMP P2	4	TIMESTAMP OF WHEN QR CODE WAS GENERATED, PART 2
	8F CERTIFICATE AUTHORITY PUBLIC KEY INDEX	1	IDENTIFIES THE CERTIFICATE AUTHORITY PUBLIC KEY FOR USE WITH OFFLINE DATA AUTHENTICATION
	9F46 PUBLIC KEY CERTIFICATE	VARIES	PUBLIC KEY CERTIFICATE, CERTIFIED BY THE CERTIFICATE AUTHORITY
	9F4B DIGITAL SIGNATURE	VARIES	DIGITAL SIGNATURE OF SOME PORTION OF THE DATA FIELDS ABOVE

FIG. 5



600

FIG. 6



700 ↗

FIG. 7

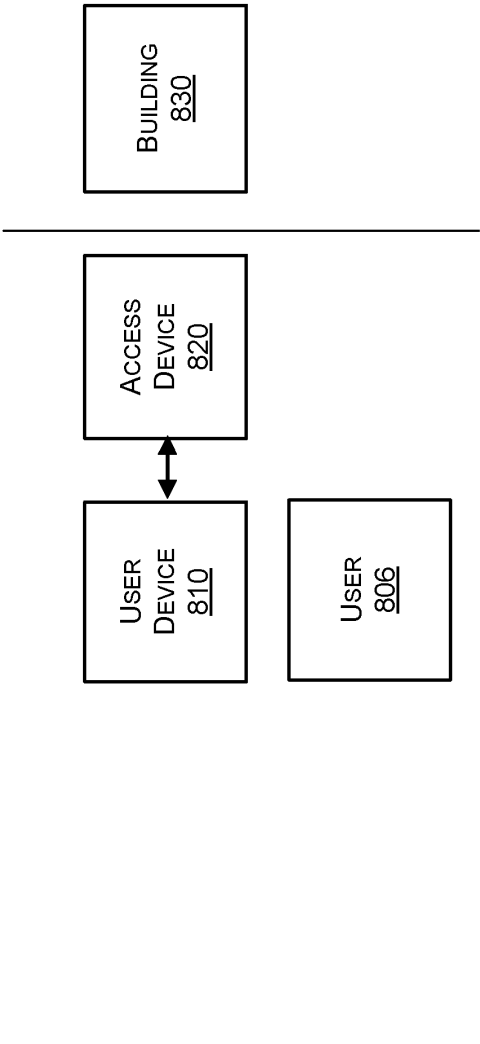


FIG. 8