

1/8

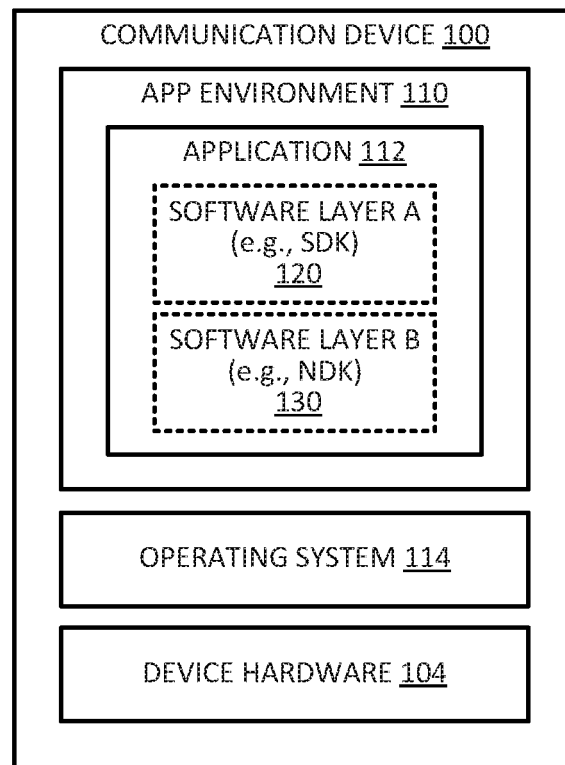


FIG. 1

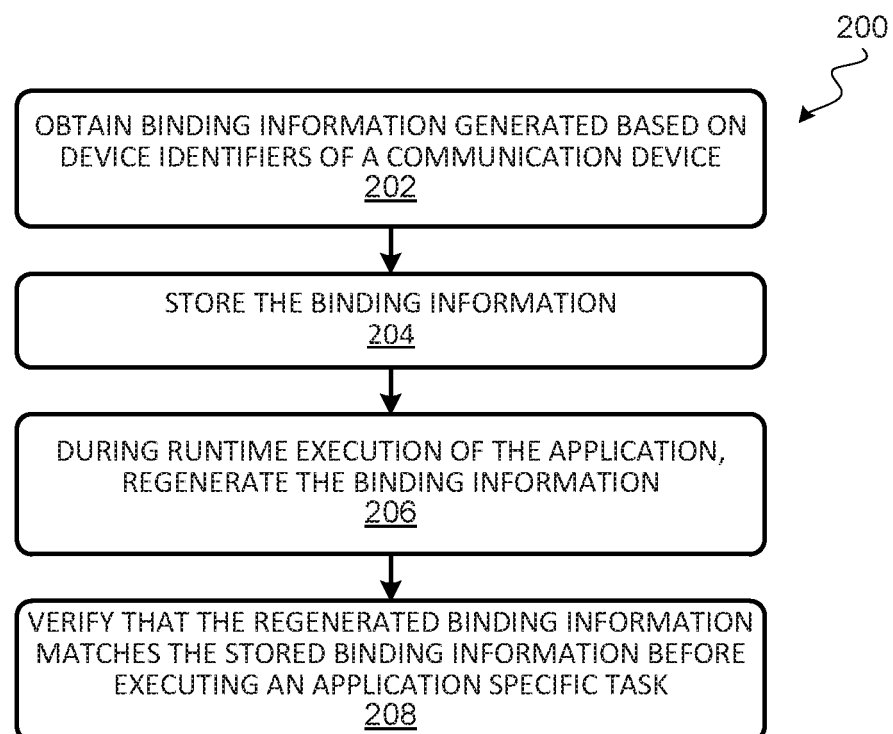


FIG. 2

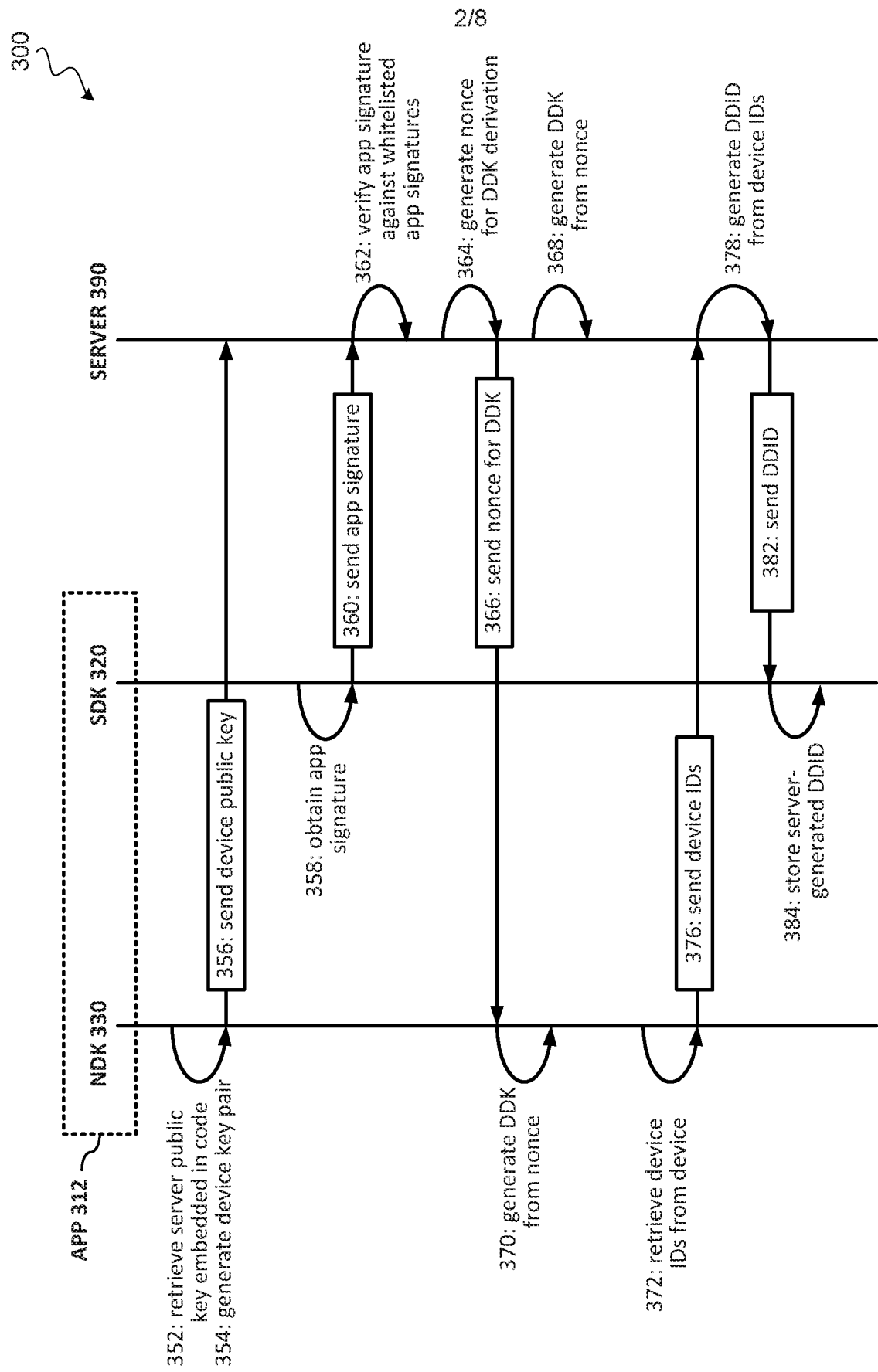


FIG. 3

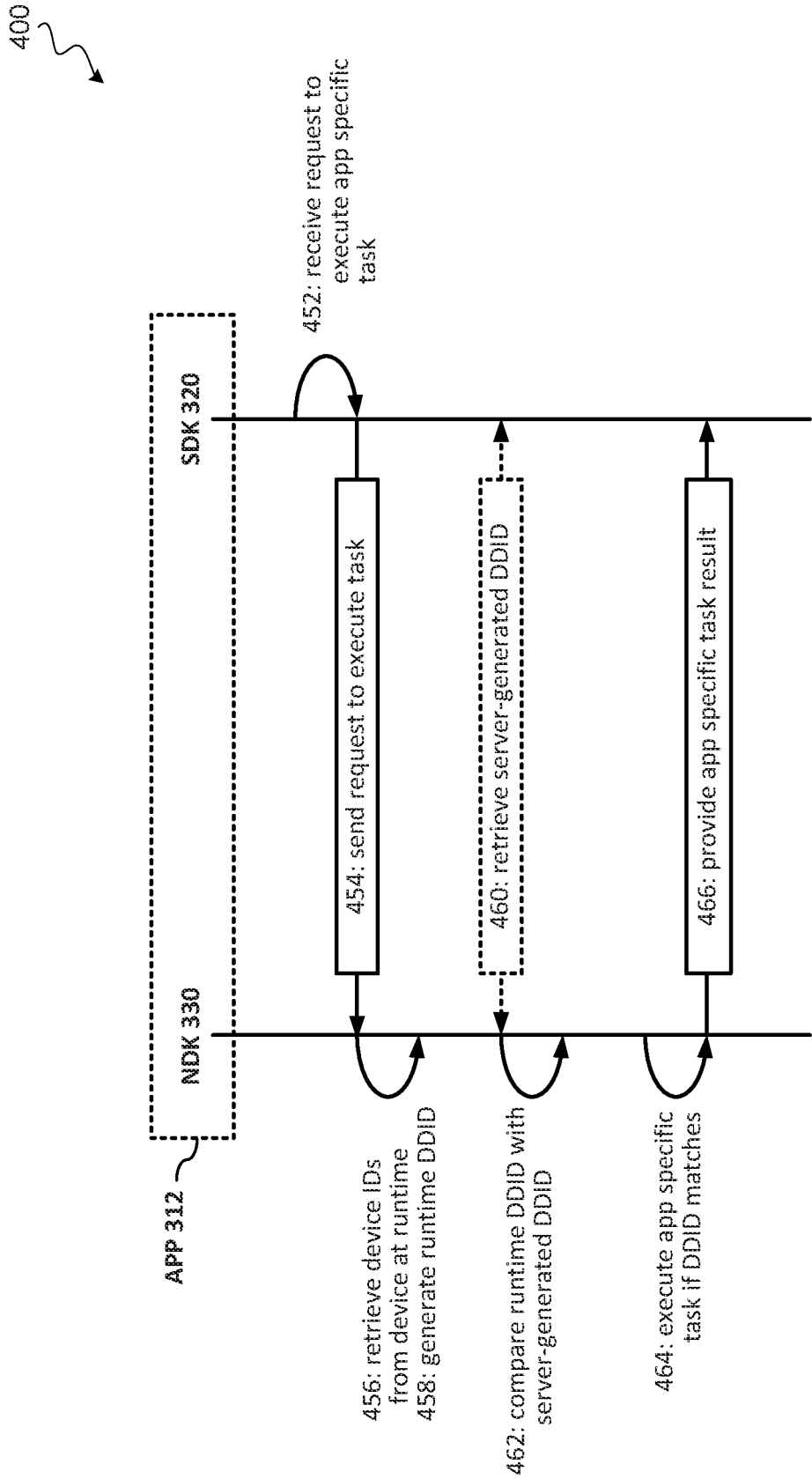


FIG. 4

4/8

500

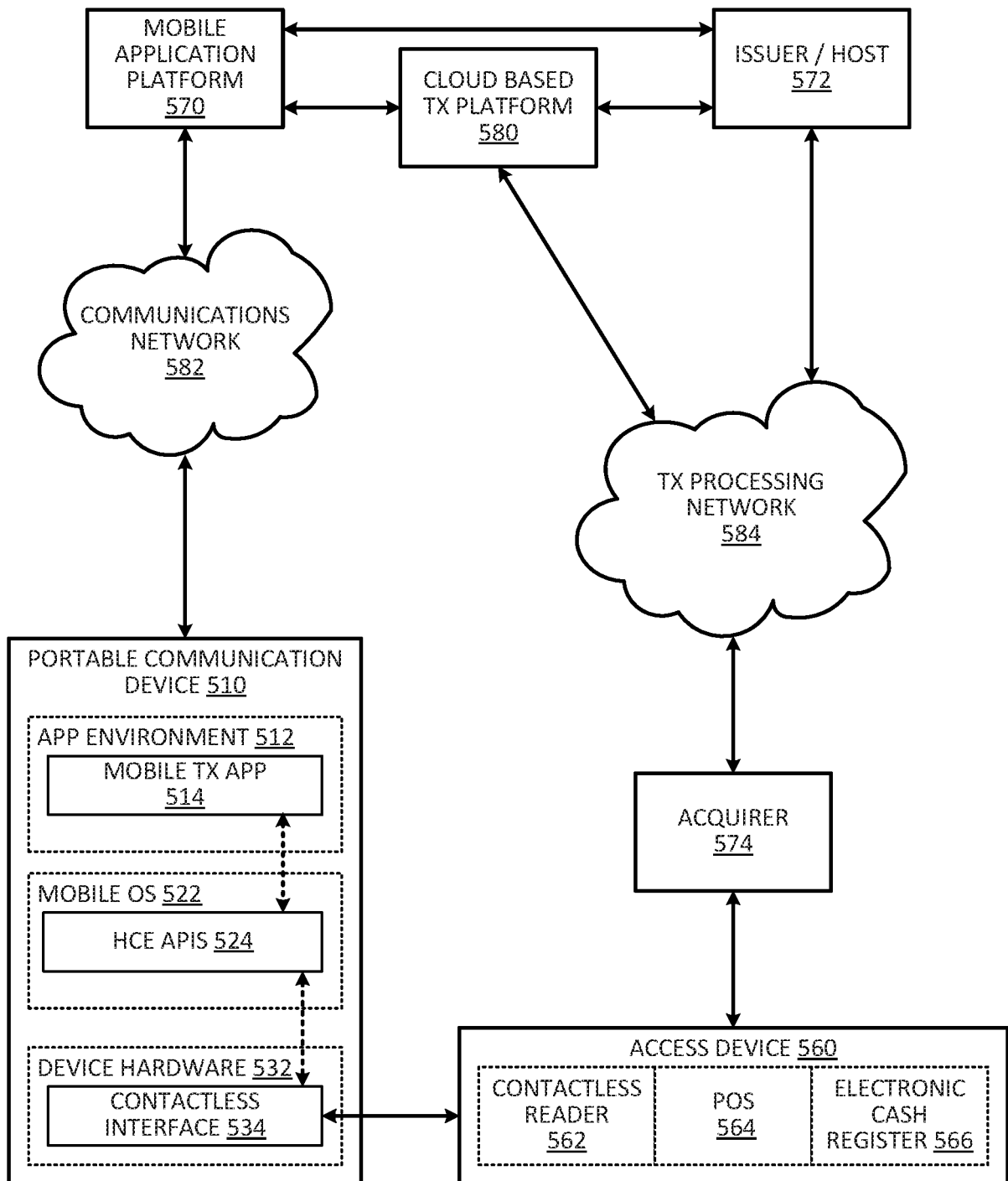


FIG. 5

5/8

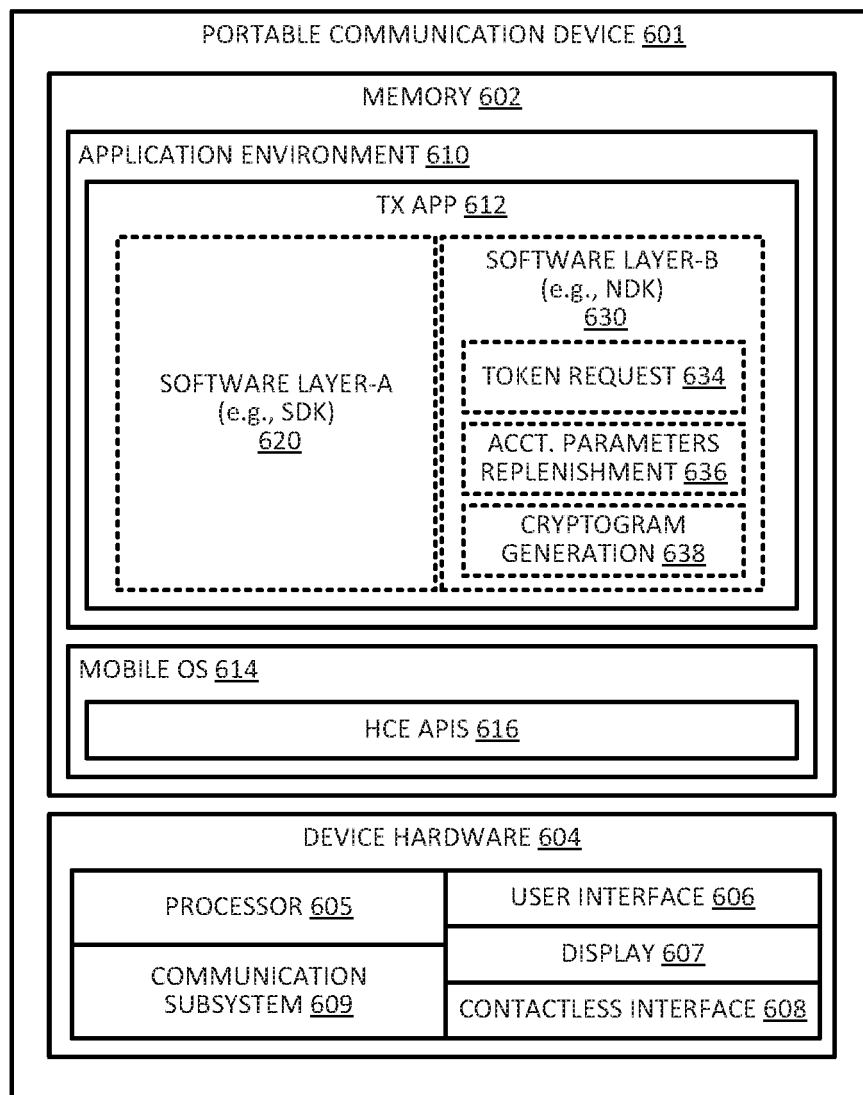


FIG. 6

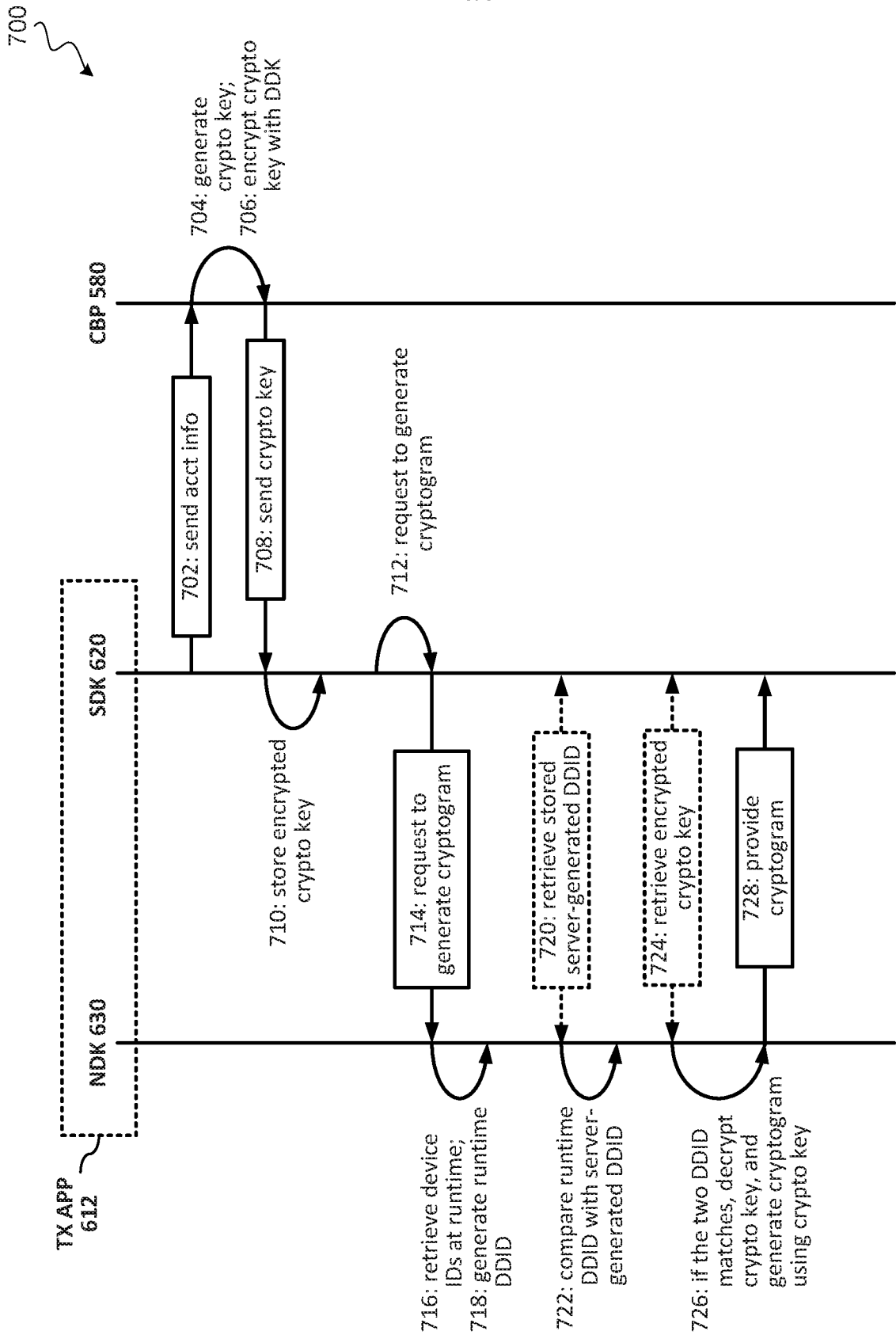


FIG. 7

7/8

800

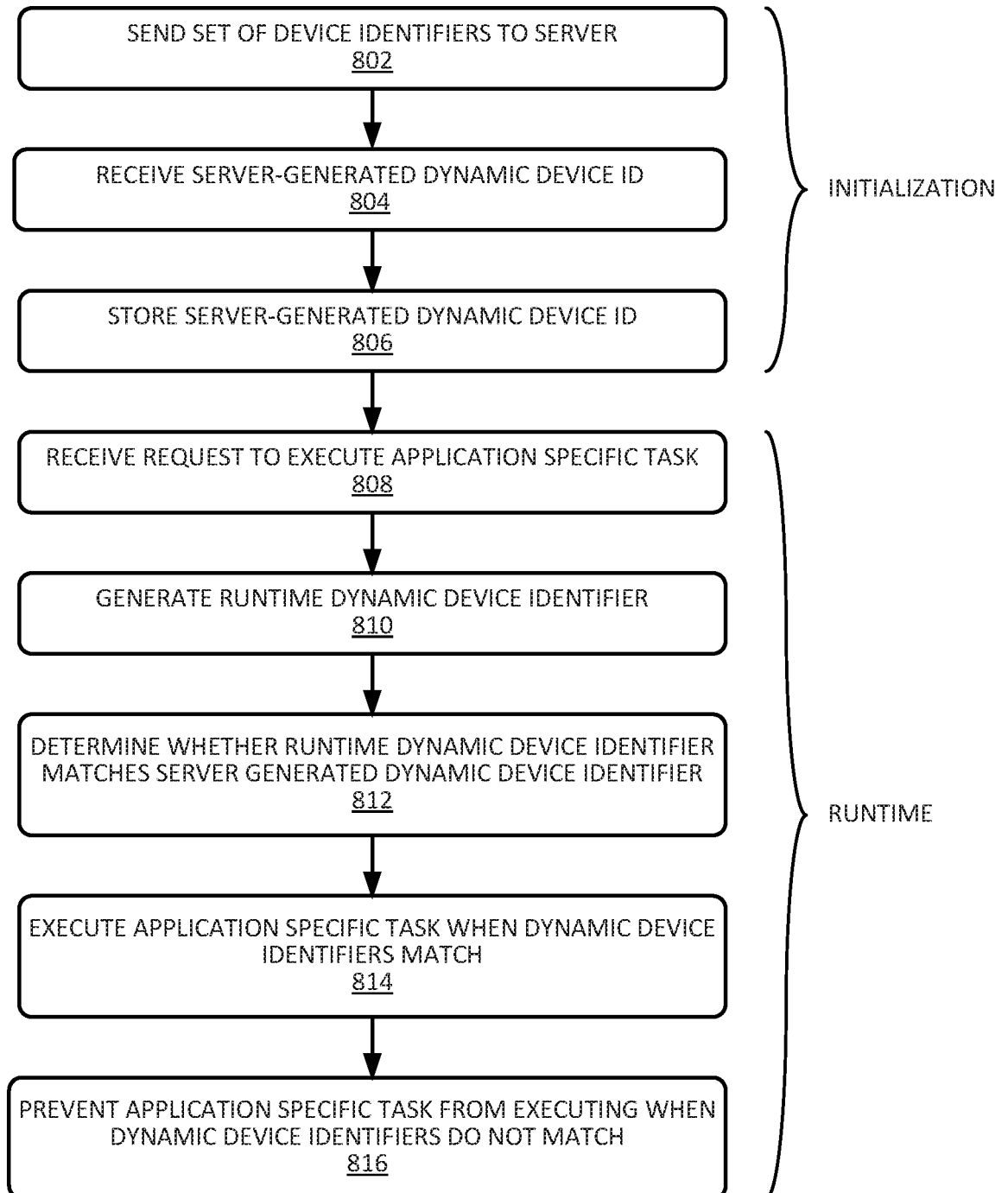


FIG. 8

<u>KEY</u>	<u>SOURCE</u>	<u>USAGE</u>
SERVER PUBLIC KEY 902	EMBEDDED IN NDK	ENCRYPT INFORMATION SENT TO SERVER
DEVICE PRIVATE KEY 904 (e.g., RSA)	GENERATED BY NDK AT INITIALIZATION TIME	DIGITAL SIGNING OF INFORMATION SENT TO SERVER; DECRYPT INFORMATION RECEIVED FROM SERVER ENCRYPTED WITH DEVICE PUBLIC KEY
DEVICE DERIVATION KEY 906	GENERATED BY NDK FROM NONCE PROVIDED BY SERVER	DECRYPT INFORMATION RECEIVED FROM SERVER ENCRYPTED WITH THE SERVER'S DEVIC DERIVATION KEY
CRYPTOGRAM KEY 908 (e.g., LUK)	PROVISIONED BY SERVER	CRYPTOGRAM GENERATION DURING RUNTIME

FIG. 9