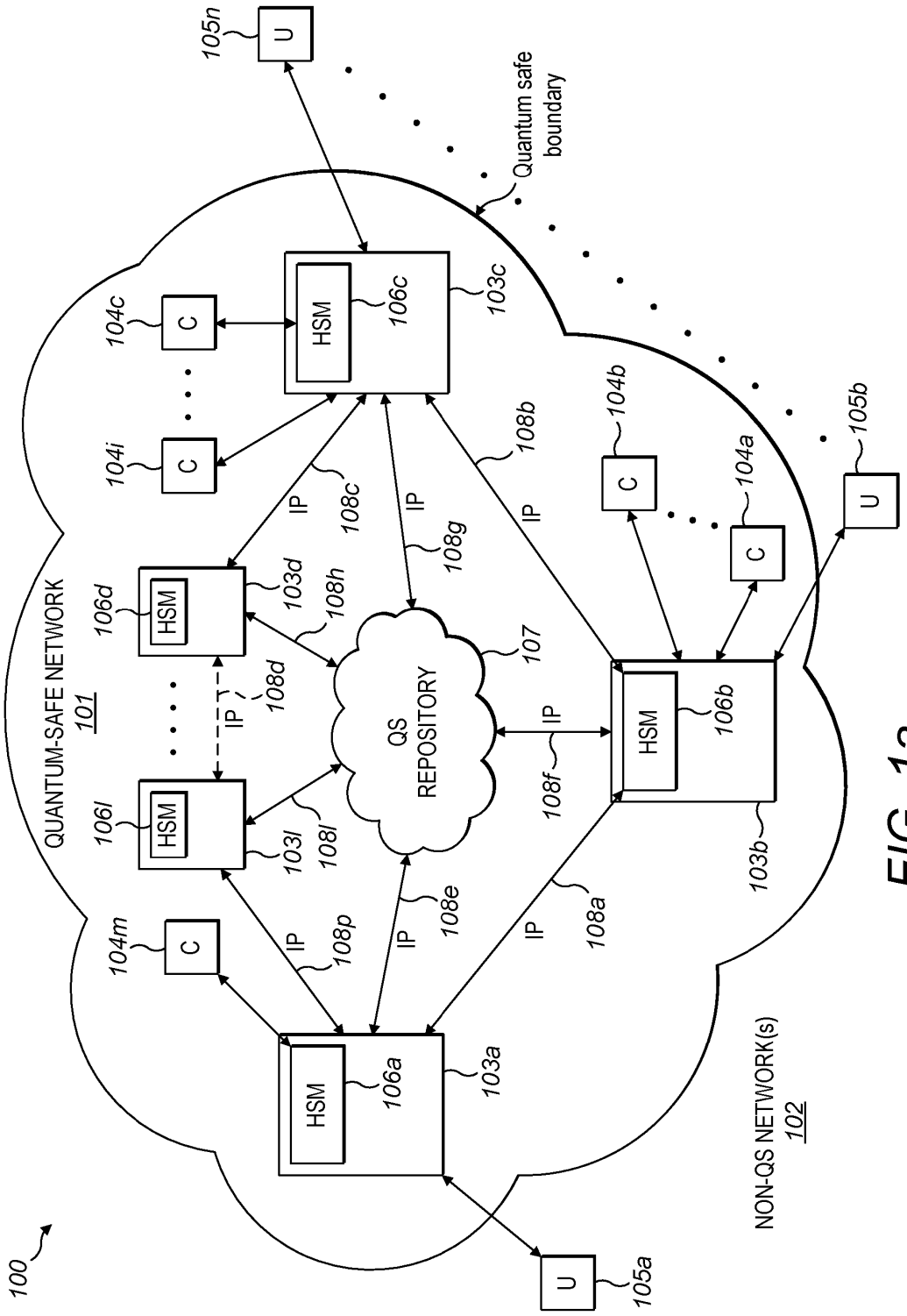

100
QUANTUM-SAFE NETWORK
101
NON-QS NETWORK(s)
102
Quantum safe boundary
QS REPOSITORY
107
HSM
106a
106b
106c
106d
106l
C
104a
104b
104c
104i
104m
U
105a
105b
105n
IP
103a
103b
103c
103d
103l
108a
108b
108c
108d
108e
108f
108g
108h
108l
108p

FIG. 1a

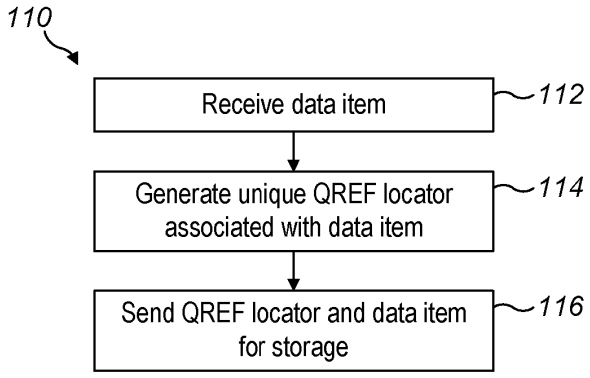

110
Receive data item
112
Generate unique QREF locator associated with data item
114
Send QREF locator and data item for storage
116

FIG. 1b

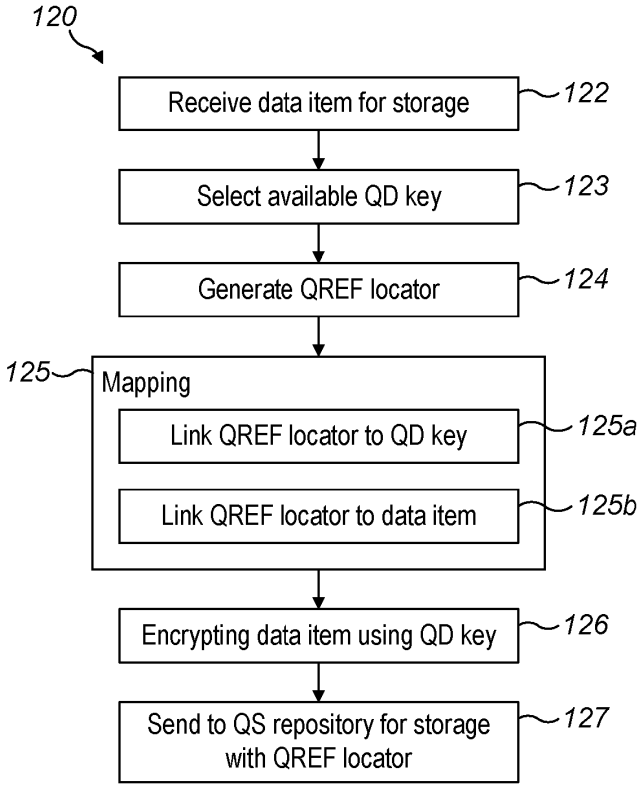

120
Receive data item for storage
122
Select available QD key
123
Generate QREF locator
124
125
Mapping
Link QREF locator to QD key
125a
Link QREF locator to data item
125b
Encrypting data item using QD key
126
Send to QS repository for storage with QREF locator
127

FIG. 1c

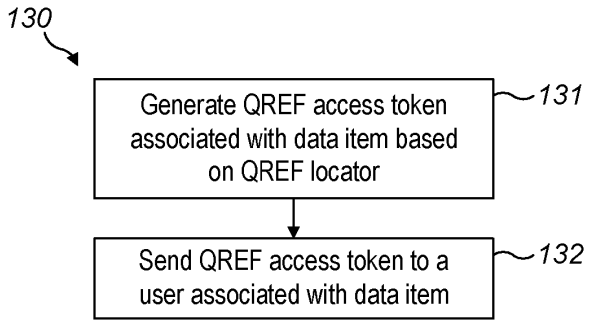

130
Generate QREF access token associated with data item based on QREF locator
131
Send QREF access token to a user associated with data item
132

FIG. 1d

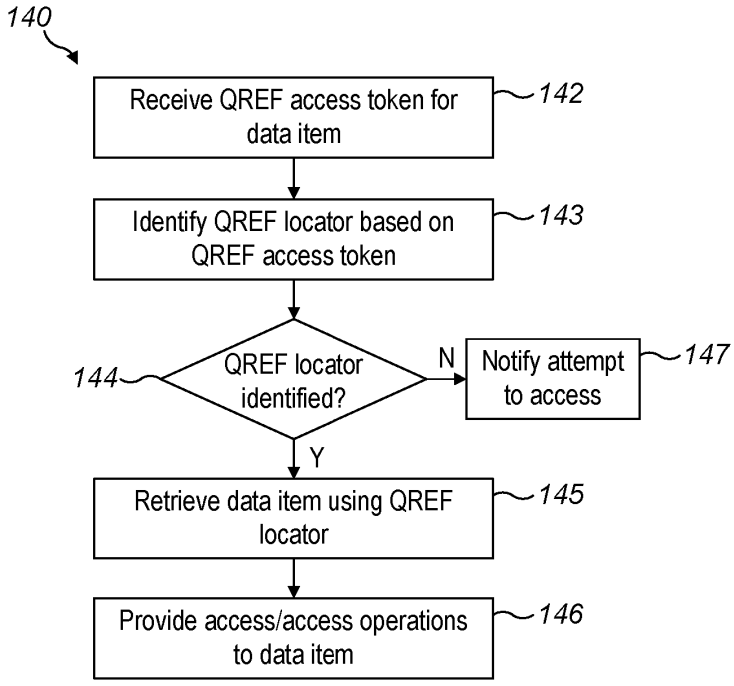

140
Receive QREF access token for data item
142
Identify QREF locator based on QREF access token
143
144
QREF locator identified?
N
Notify attempt to access
147
Y
Retrieve data item using QREF locator
145
Provide access/access operations to data item
146

FIG. 1e

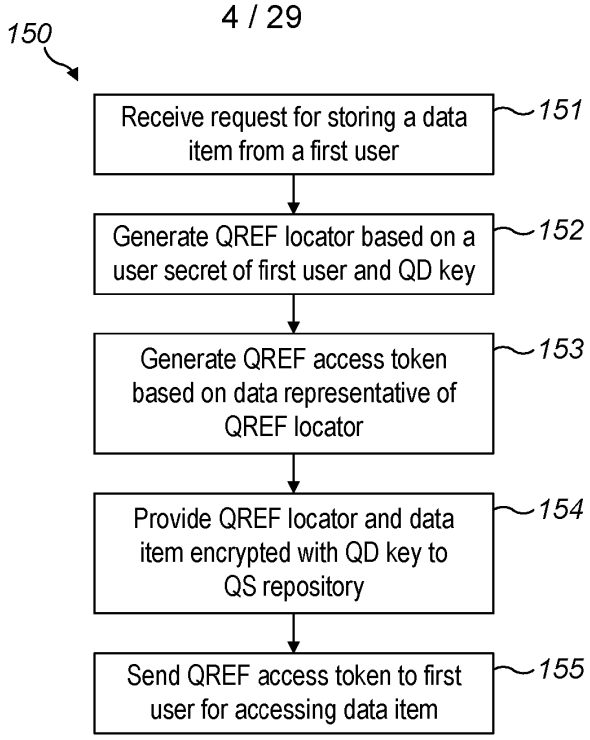

150
Receive request for storing a data item from a first user
151
Generate QREF locator based on a user secret of first user and QD key
152
Generate QREF access token based on data representative of QREF locator
153
Provide QREF locator and data item encrypted with QD key to QS repository
154
Send QREF access token to first user for accessing data item
155

FIG. 1f

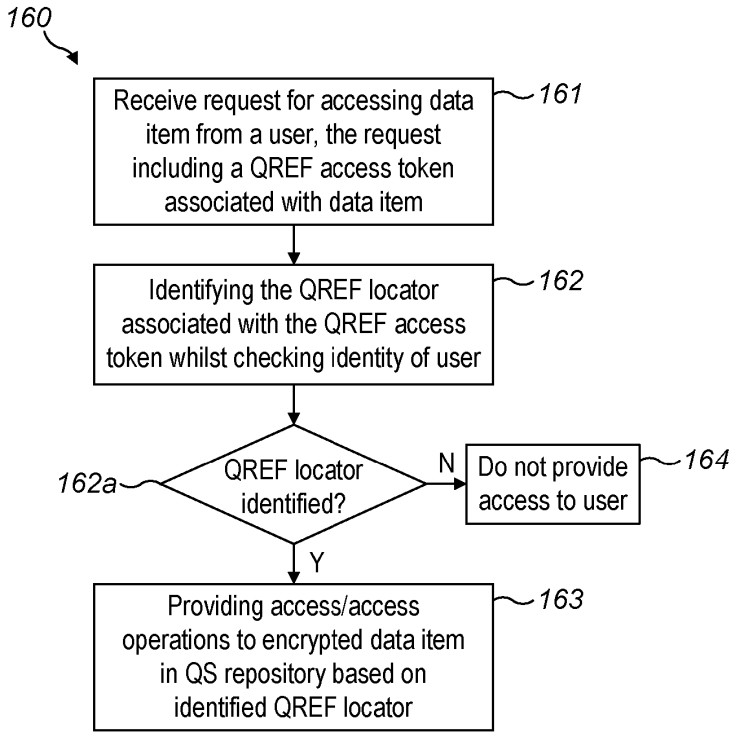

160
Receive request for accessing data item from a user, the request including a QREF access token associated with data item
161
Identifying the QREF locator associated with the QREF access token whilst checking identity of user
162
162a
QREF locator identified?
N
Do not provide access to user
164
Y
Providing access/access operations to encrypted data item in QS repository based on identified QREF locator
163

FIG. 1g

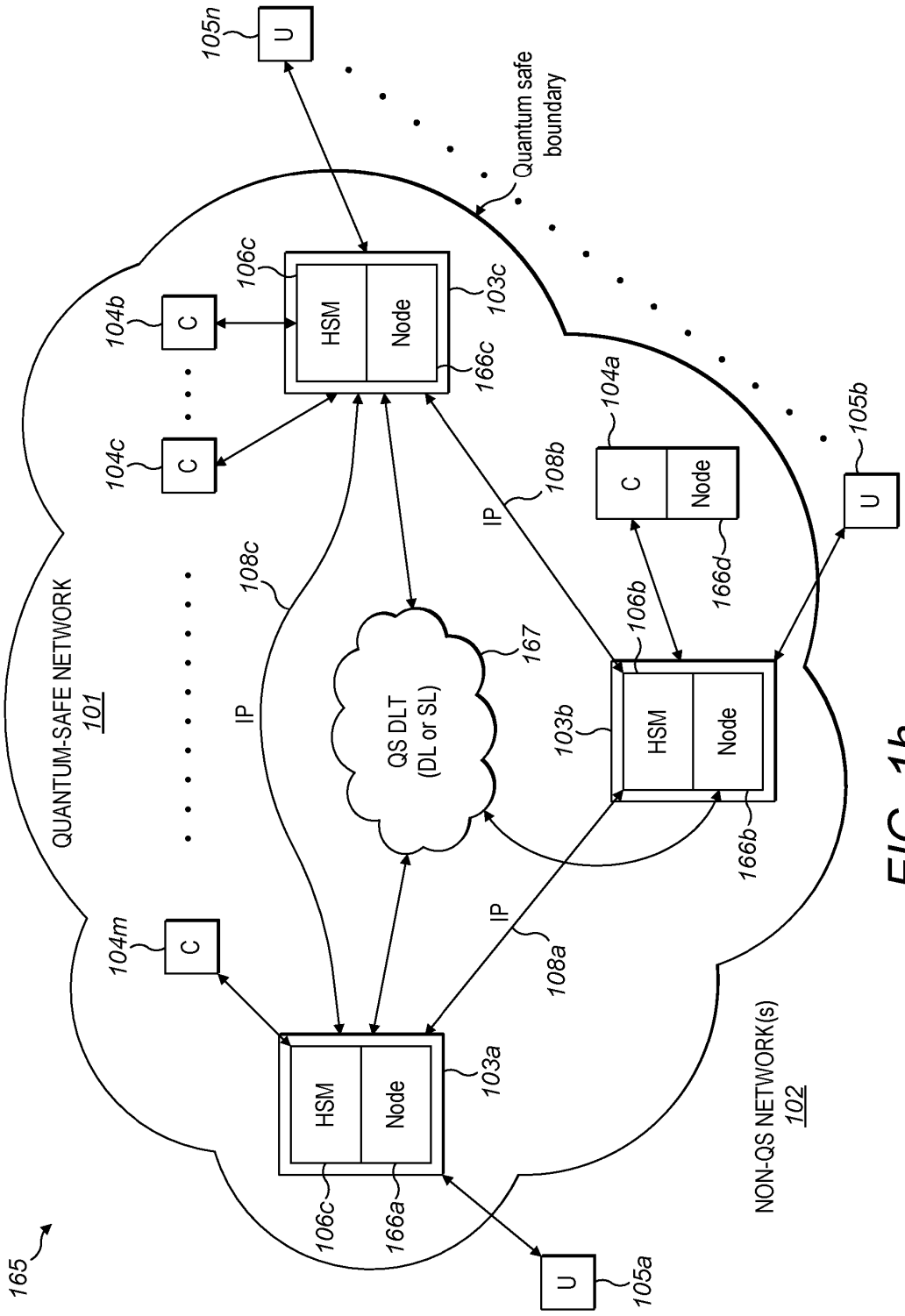

165
QUANTUM-SAFE NETWORK
101
NON-QS NETWORK(s)
102
Quantum safe boundary
QS DLT (DL or SL)
167
HSM
Node
C
U
IP
105n
105b
105a
104a
104b
104c
104m
106c
106b
103c
103b
103a
166c
166d
166b
166a
108c
108b
108a

FIG. 1h

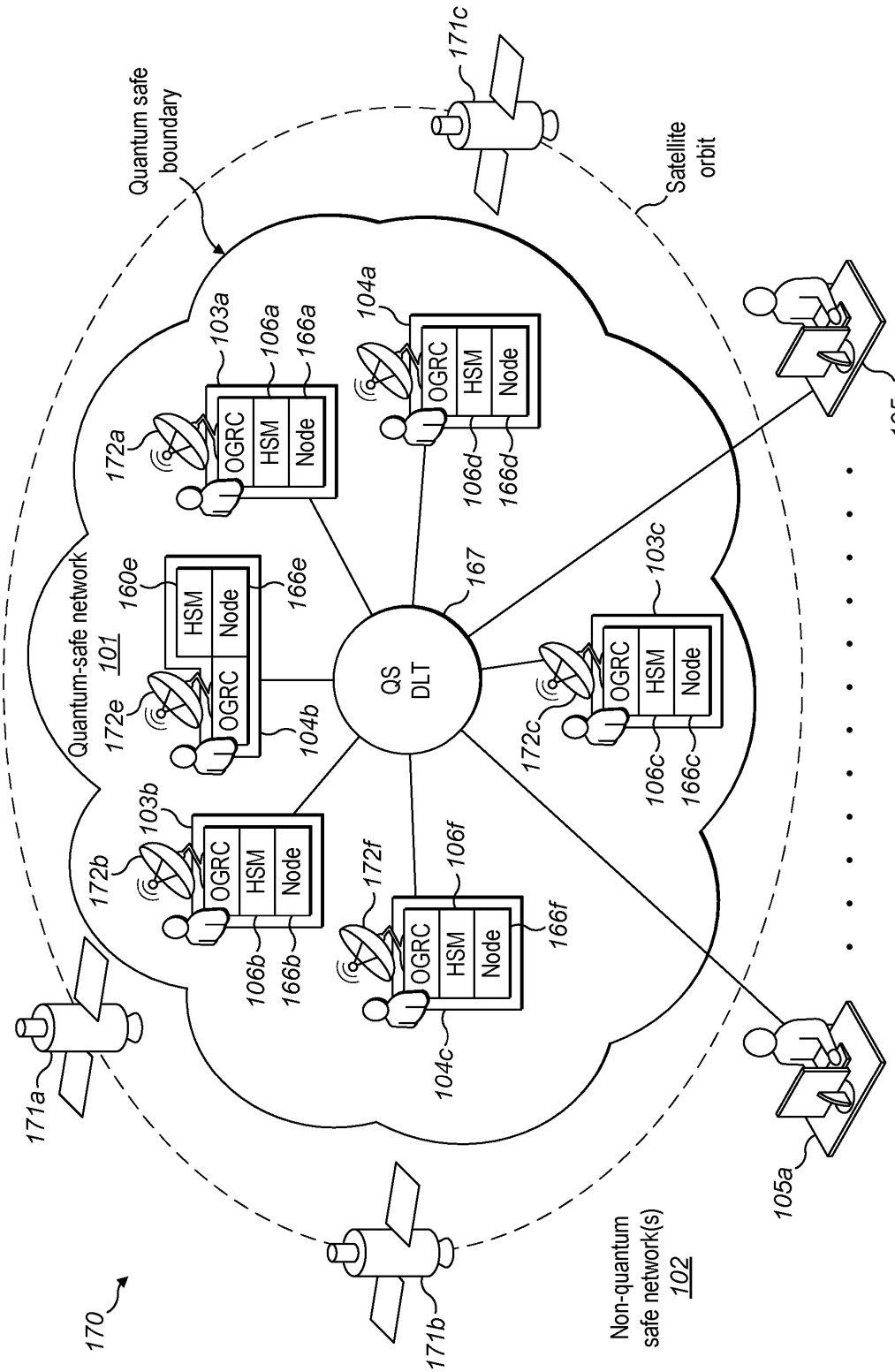

Quantum safe boundary
Satellite orbit
Quantum-safe network 101
Non-quantum safe network(s) 102
QS DLT
167
OGRC
HSM
Node
103a
106a
166a
104a
106d
166d
172a
160e
166e
172e
104b
103c
172c
106c
166c
103b
172b
106b
166b
172f
106f
166f
104c
171a
171b
171c
105a
105n
170

FIG. 1i

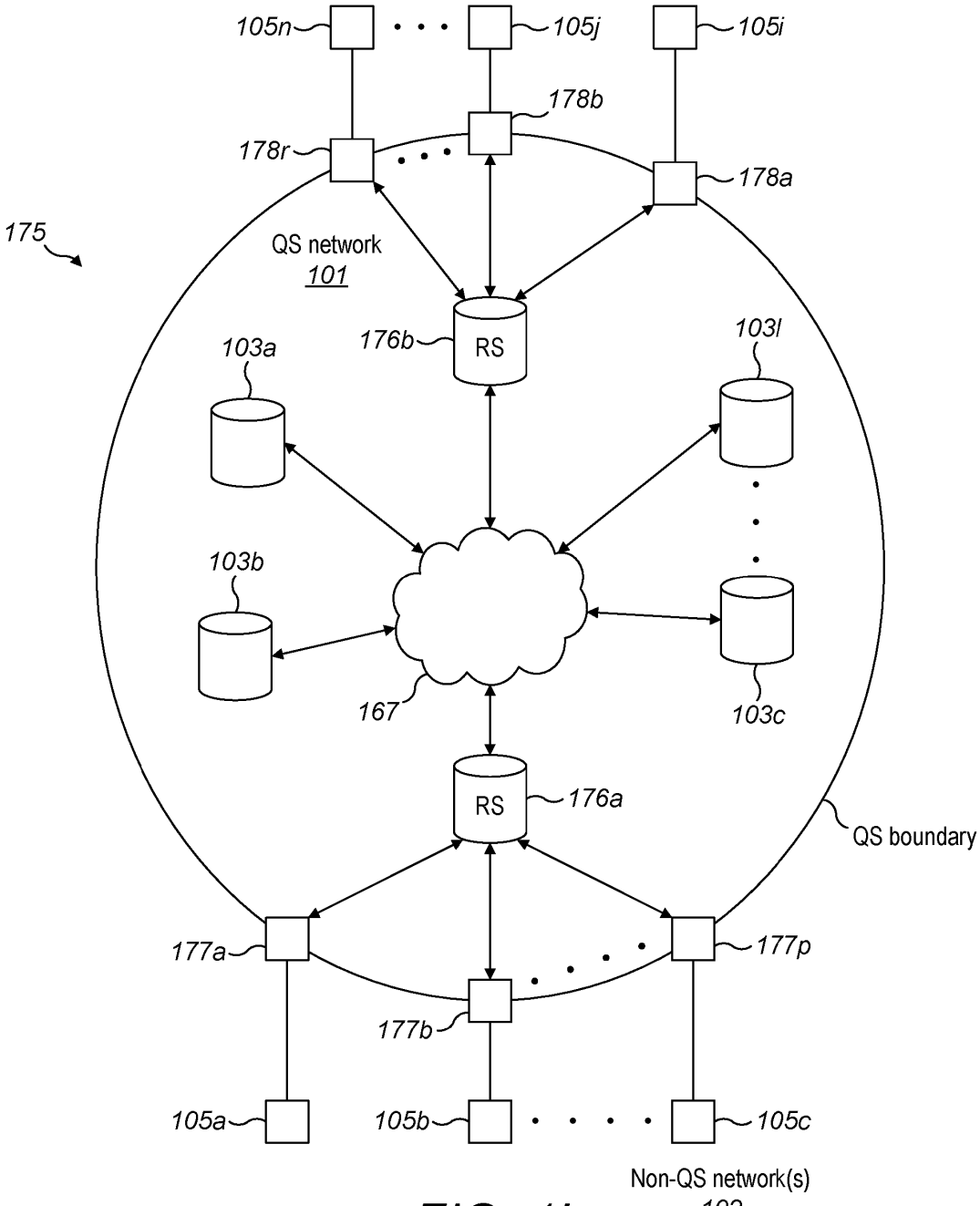

105n
105j
105i
178b
178r
178a
175
QS network
101
176b
RS
103a
103l
103b
167
103c
RS
176a
QS boundary
177a
177p
177b
105a
105b
105c
Non-QS network(s)
102

FIG. 1j

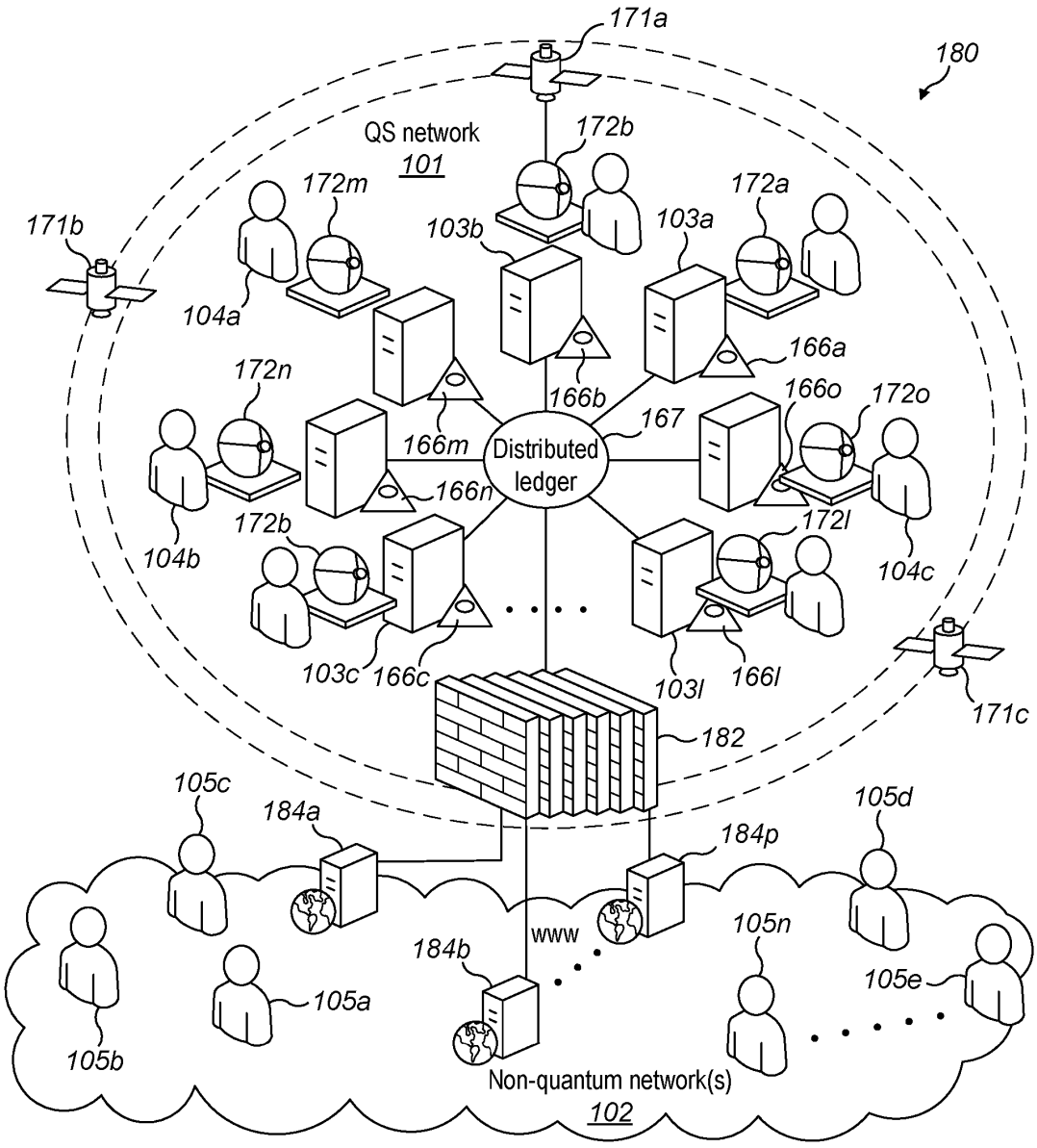

171a
180
QS network
101
172b
172m
172a
171b
103b
103a
104a
166a
172n
166b
166o
172o
167
166m
Distributed
ledger
166n
172b
172l
104b
104c
103c
166c
103l
166l
171c
182
105c
184a
105d
184p
www
105n
184b
105a
105e
105b
Non-quantum network(s)
102

FIG. 1k

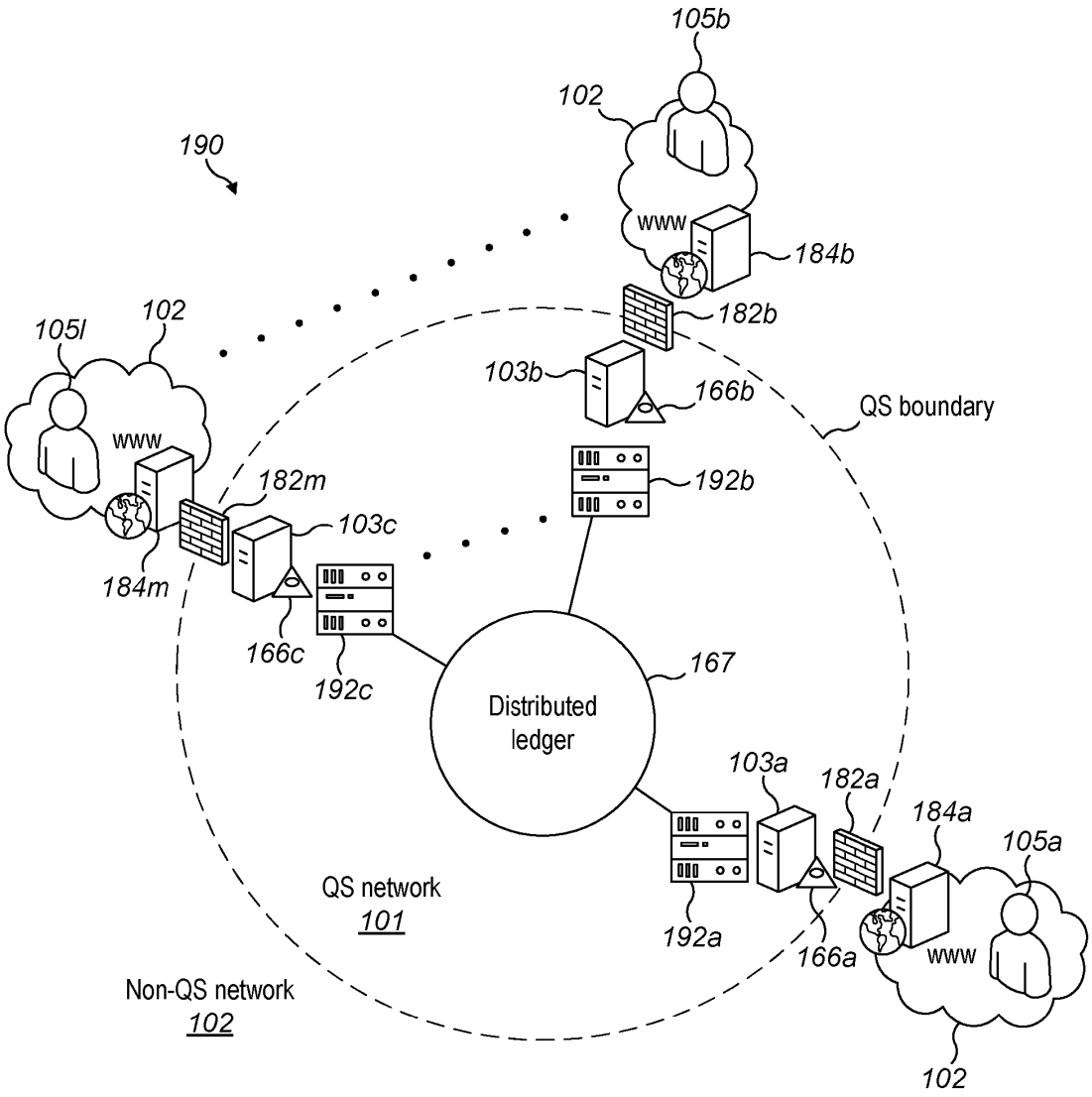

105b
102
190
www
184b
182b
105l
102
103b
166b
QS boundary
www
182m
192b
103c
184m
166c
192c
167
Distributed ledger
103a
182a
184a
105a
QS network
101
192a
166a
www
Non-QS network
102
102

FIG. 1I

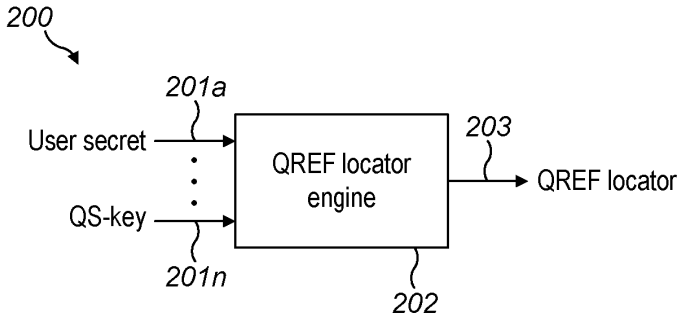

200
201a
User secret
QS-key
201n
QREF locator engine
203
QREF locator
202

FIG. 2a

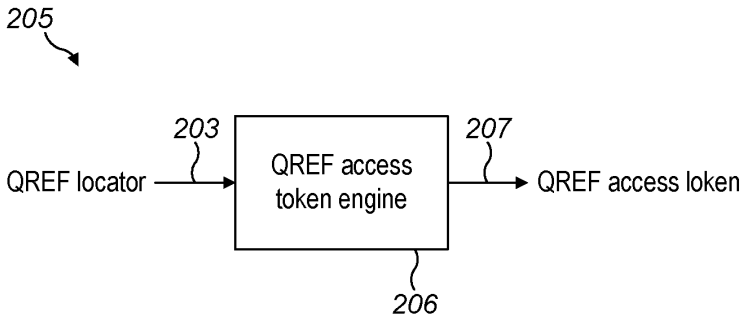

205
203
QREF locator
QREF access token engine
207
QREF access loken
206

FIG. 2b

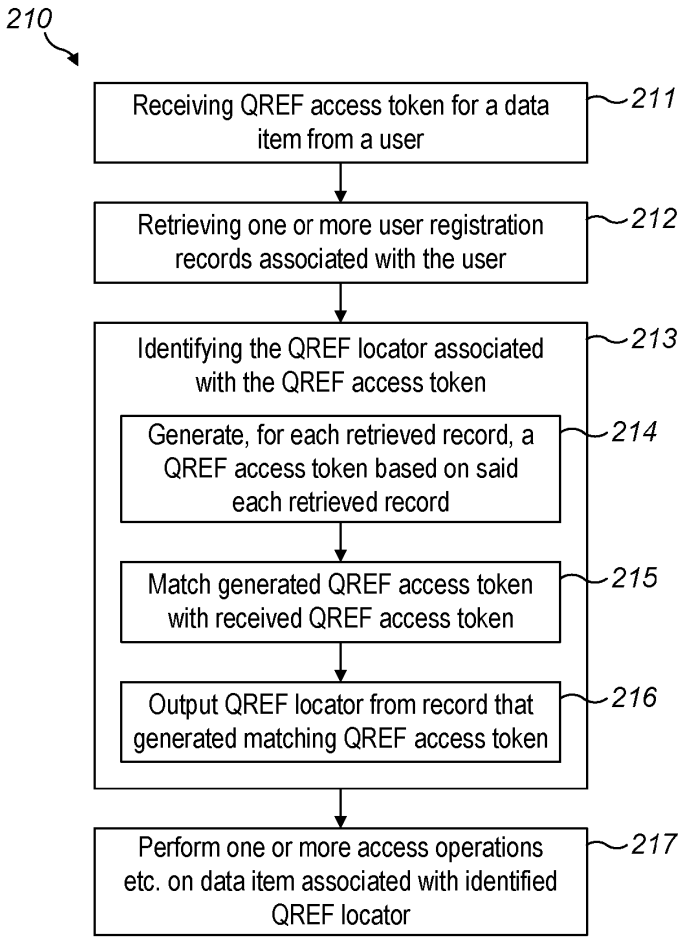

210
Receiving QREF access token for a data item from a user
211
Retrieving one or more user registration records associated with the user
212
Identifying the QREF locator associated with the QREF access token
213
Generate, for each retrieved record, a QREF access token based on said each retrieved record
214
Match generated QREF access token with received QREF access token
215
Output QREF locator from record that generated matching QREF access token
216
Perform one or more access operations etc. on data item associated with identified QREF locator
217

FIG. 2c

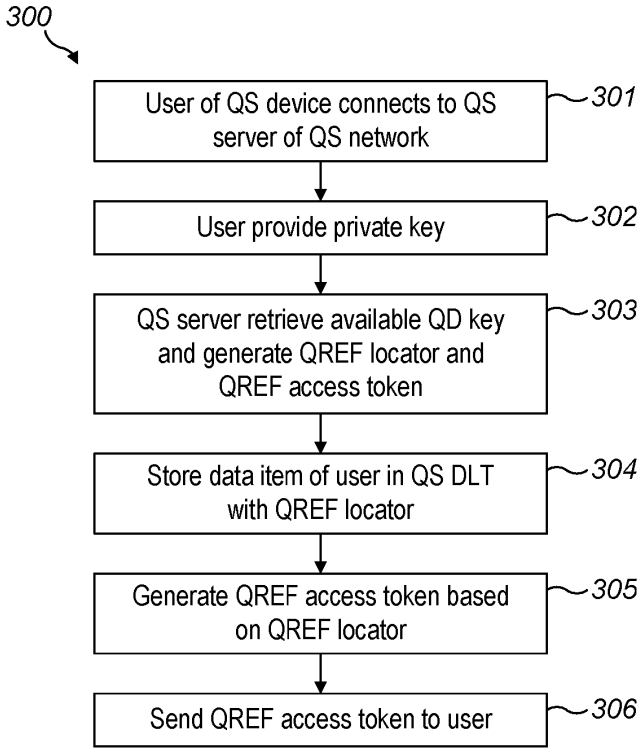

300
User of QS device connects to QS server of QS network
301
User provide private key
302
QS server retrieve available QD key and generate QREF locator and QREF access token
303
Store data item of user in QS DLT with QREF locator
304
Generate QREF access token based on QREF locator
305
Send QREF access token to user
306

FIG. 3a

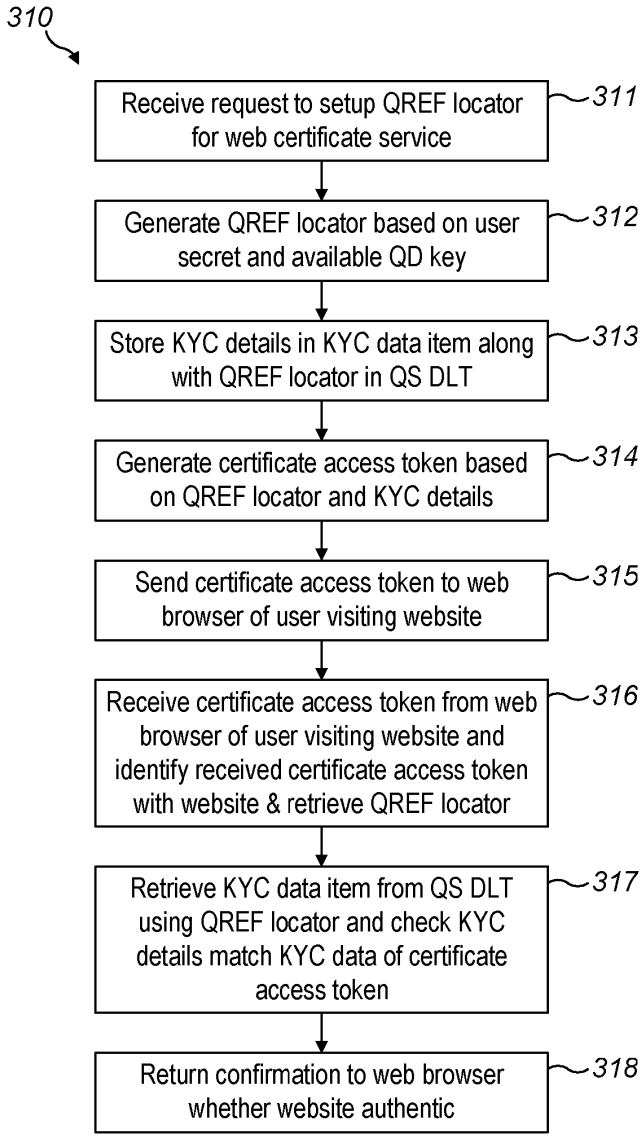

310
Receive request to setup QREF locator for web certificate service
311
Generate QREF locator based on user secret and available QD key
312
Store KYC details in KYC data item along with QREF locator in QS DLT
313
Generate certificate access token based on QREF locator and KYC details
314
Send certificate access token to web browser of user visiting website
315
Receive certificate access token from web browser of user visiting website and identify received certificate access token with website & retrieve QREF locator
316
Retrieve KYC data item from QS DLT using QREF locator and check KYC details match KYC data of certificate access token
317
Return confirmation to web browser whether website authentic
318

FIG. 3b

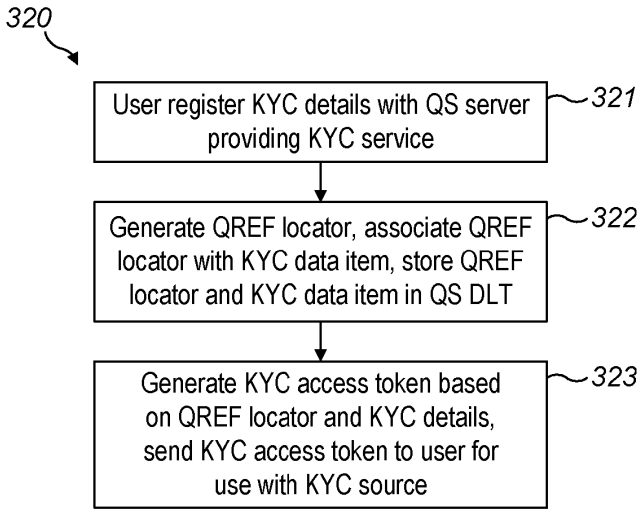

320
User register KYC details with QS server providing KYC service
321
Generate QREF locator, associate QREF locator with KYC data item, store QREF locator and KYC data item in QS DLT
322
Generate KYC access token based on QREF locator and KYC details, send KYC access token to user for use with KYC source
323

FIG. 3c

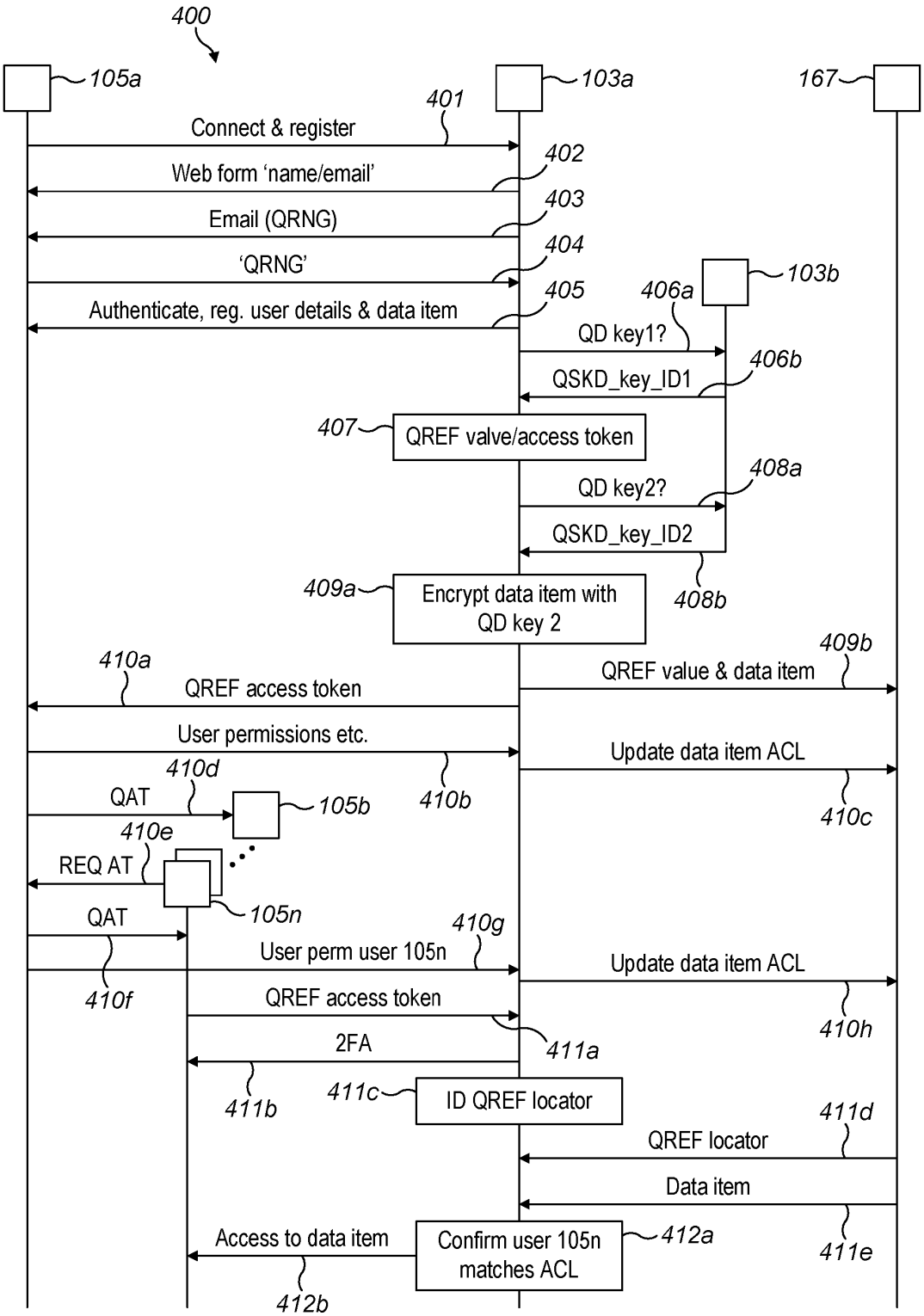

400
105a
103a
167
401
Connect & register
402
Web form 'name/email'
403
Email (QRNG)
404
'QRNG'
405
Authenticate, reg. user details & data item
103b
406a
QD key1?
406b
QSKD_key_ID1
407
QREF valve/access token
408a
QD key2?
QSKD_key_ID2
408b
409a
Encrypt data item with QD key 2
409b
QREF value & data item
410a
QREF access token
User permissions etc.
410b
Update data item ACL
410c
410d
QAT
105b
410e
REQ AT
105n
QAT
410f
410g
User perm user 105n
Update data item ACL
410h
QREF access token
411a
2FA
411b
411c
ID QREF locator
411d
QREF locator
Data item
411e
Access to data item
412b
Confirm user 105n matches ACL
412a

FIG. 4a

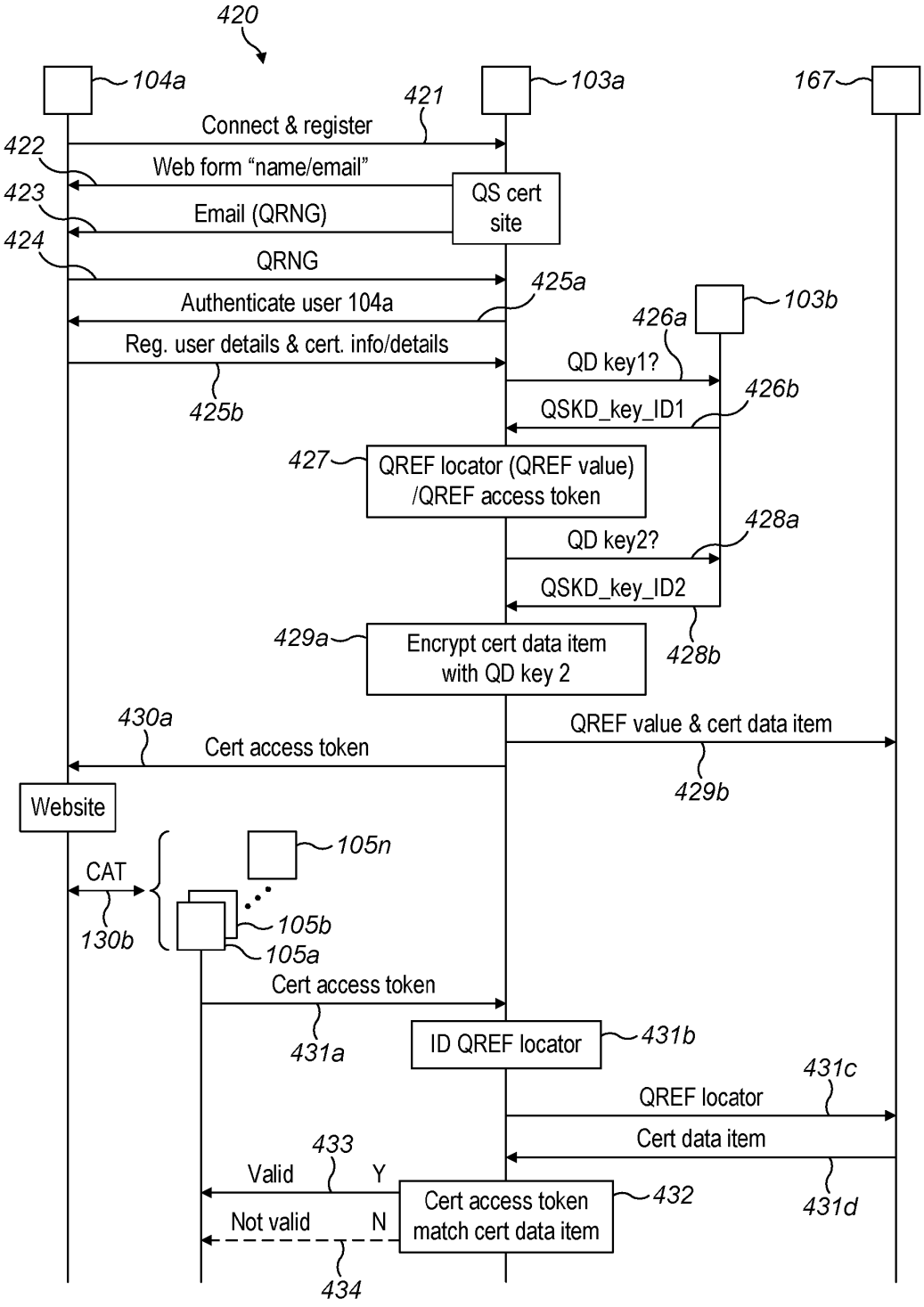

420
104a
103a
167
421
Connect & register
422
Web form "name/email"
423
Email (QRNG)
QS cert site
424
QRNG
425a
Authenticate user 104a
103b
426a
Reg. user details & cert. info/details
QD key1?
426b
QSKD_key_ID1
425b
427
QREF locator (QREF value) /QREF access token
428a
QD key2?
QSKD_key_ID2
429a
Encrypt cert data item with QD key 2
428b
430a
Cert access token
QREF value & cert data item
429b
Website
105n
CAT
105b
130b
105a
Cert access token
431a
ID QREF locator
431b
431c
QREF locator
Cert data item
433
Valid
Y
Cert access token match cert data item
432
Not valid
N
431d
434

FIG. 4b

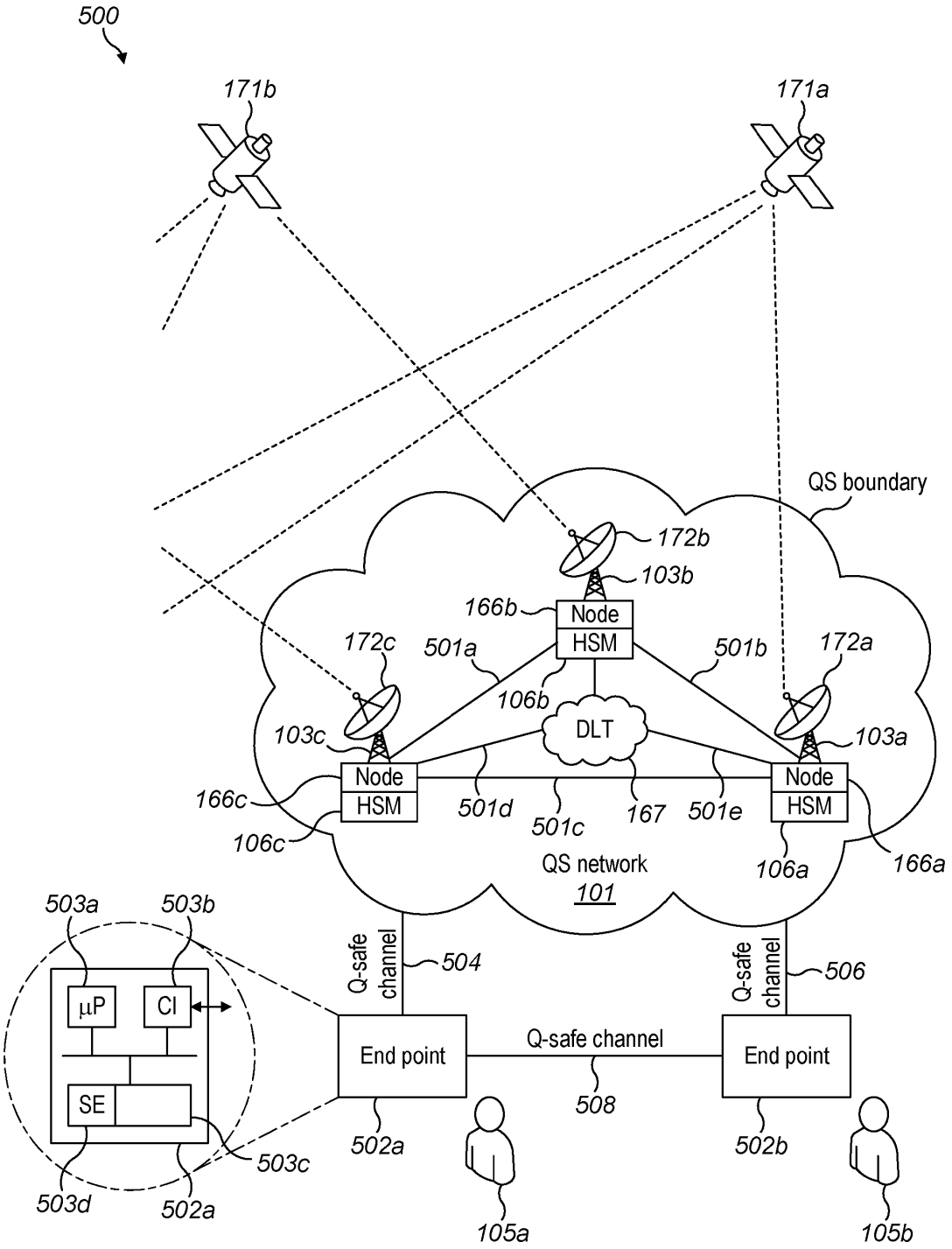

500
171b
171a
QS boundary
172b
103b
166b
Node
HSM
172c
501a
501b
172a
106b
DLT
103c
103a
Node
HSM
Node
HSM
166c
501d
501c
167
501e
106c
106a
166a
QS network
101
503a
503b
Q-safe channel
504
Q-safe channel
506
µP
CI
End point
Q-safe channel
End point
508
SE
503c
502a
502b
503d
502a
105a
105b

FIG. 5a

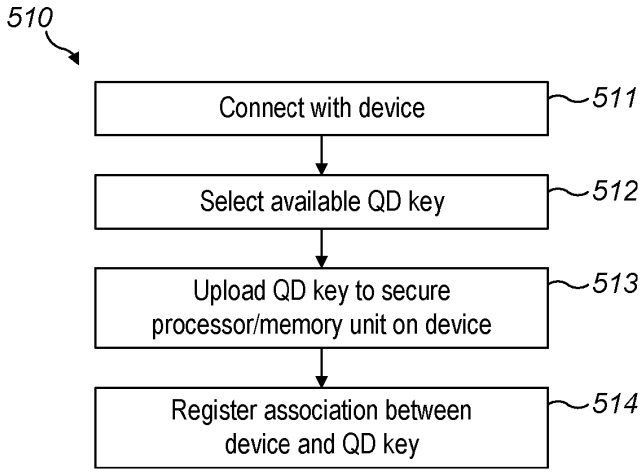

510
Connect with device
511
Select available QD key
512
Upload QD key to secure processor/memory unit on device
513
Register association between device and QD key
514

FIG. 5b

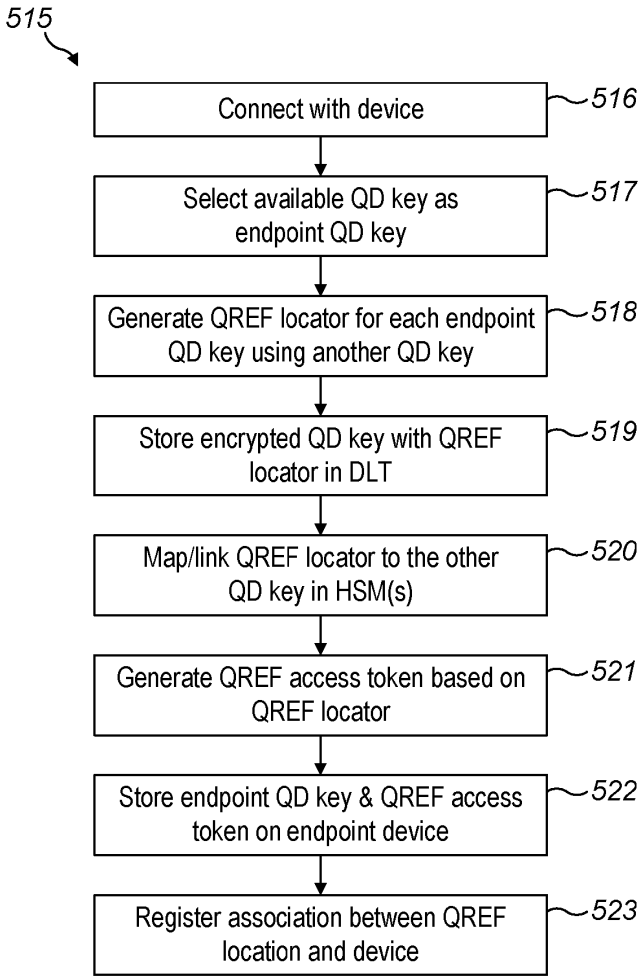

515
Connect with device
516
Select available QD key as endpoint QD key
517
Generate QREF locator for each endpoint QD key using another QD key
518
Store encrypted QD key with QREF locator in DLT
519
Map/link QREF locator to the other QD key in HSM(s)
520
Generate QREF access token based on QREF locator
521
Store endpoint QD key & QREF access token on endpoint device
522
Register association between QREF location and device
523

FIG. 5c

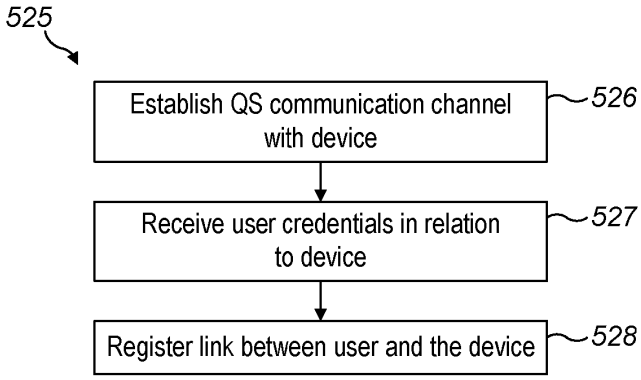

525
Establish QS communication channel with device
526
Receive user credentials in relation to device
527
Register link between user and the device
528

FIG. 5d

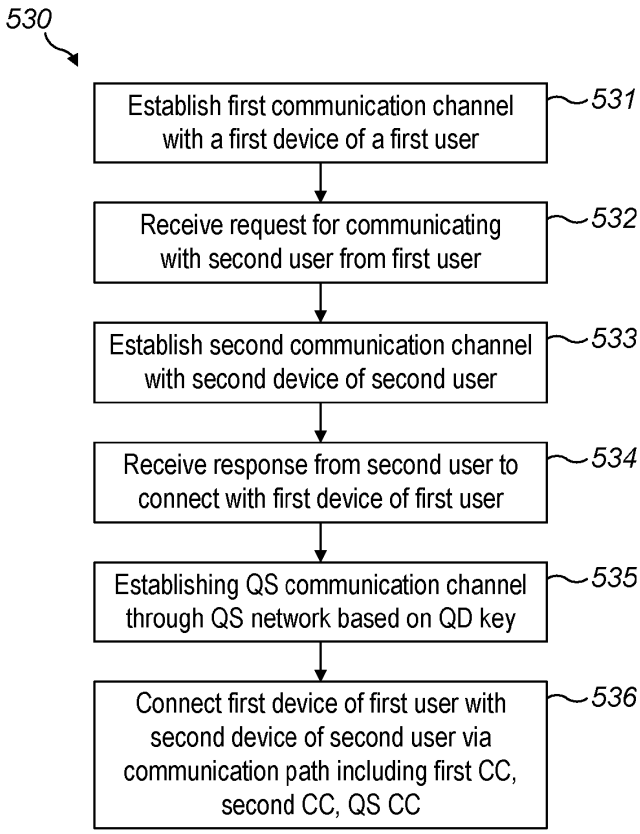

530
Establish first communication channel with a first device of a first user
531
Receive request for communicating with second user from first user
532
Establish second communication channel with second device of second user
533
Receive response from second user to connect with first device of first user
534
Establishing QS communication channel through QS network based on QD key
535
Connect first device of first user with second device of second user via communication path including first CC, second CC, QS CC
536

FIG. 5e

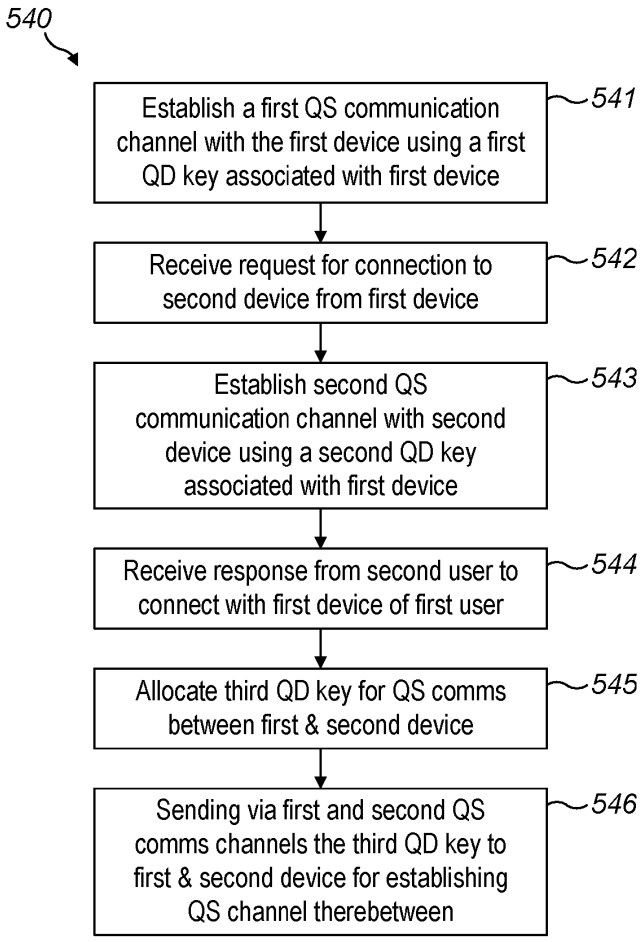

540
Establish a first QS communication channel with the first device using a first QD key associated with first device
541
Receive request for connection to second device from first device
542
Establish second QS communication channel with second device using a second QD key associated with first device
543
Receive response from second user to connect with first device of first user
544
Allocate third QD key for QS comms between first & second device
545
Sending via first and second QS comms channels the third QD key to first & second device for establishing QS channel therebetween
546

FIG. 5f

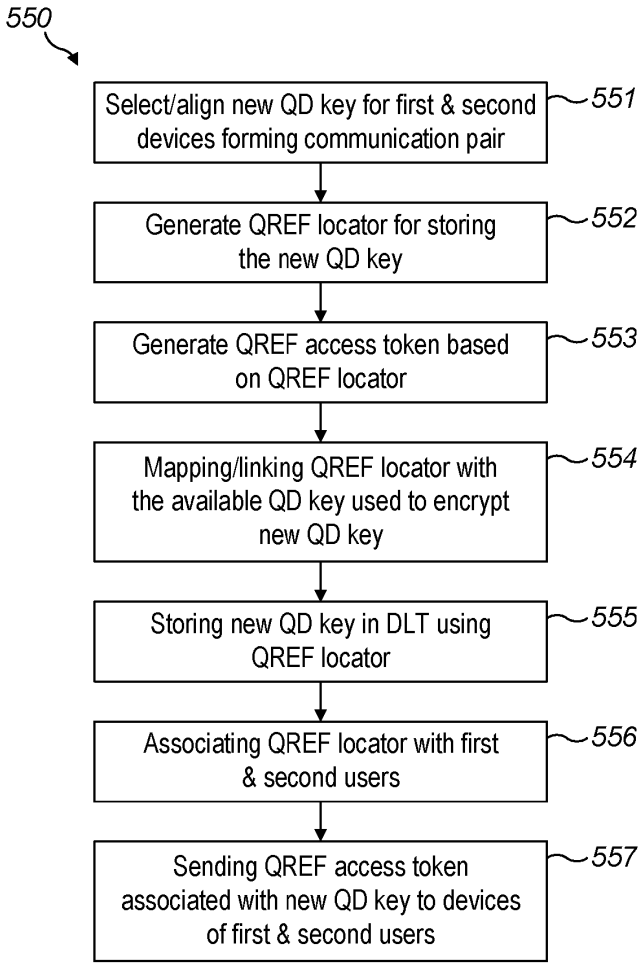

550
Select/align new QD key for first & second devices forming communication pair
551
Generate QREF locator for storing the new QD key
552
Generate QREF access token based on QREF locator
553
Mapping/linking QREF locator with the available QD key used to encrypt new QD key
554
Storing new QD key in DLT using QREF locator
555
Associating QREF locator with first & second users
556
Sending QREF access token associated with new QD key to devices of first & second users
557

FIG. 5g

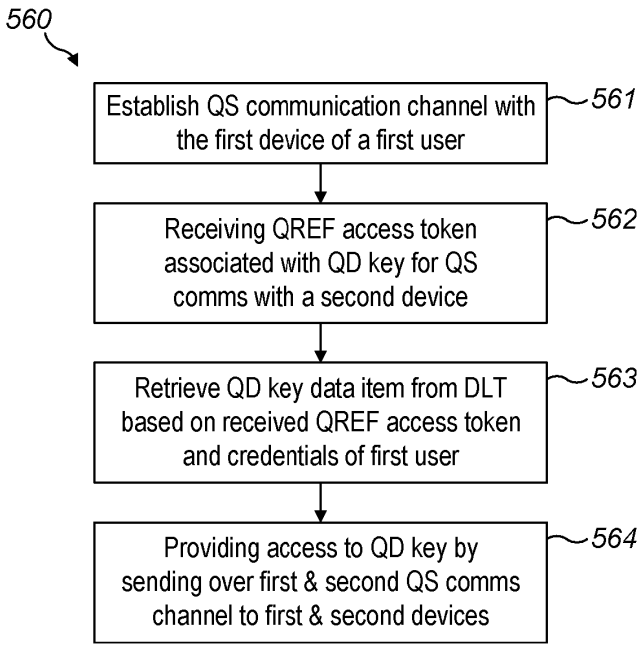

560
Establish QS communication channel with the first device of a first user
561
Receiving QREF access token associated with QD key for QS comms with a second device
562
Retrieve QD key data item from DLT based on received QREF access token and credentials of first user
563
Providing access to QD key by sending over first & second QS comms channel to first & second devices
564

FIG. 5h

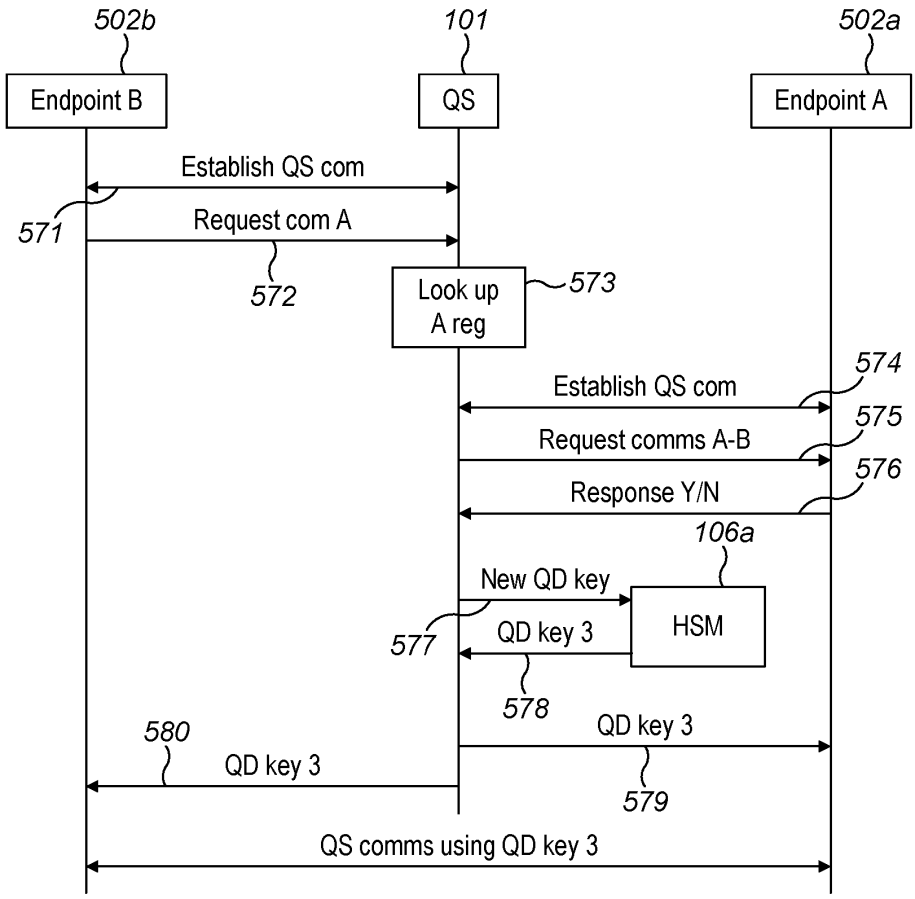

502b
101
502a
Endpoint B
QS
Endpoint A
Establish QS com
571
Request com A
572
Look up
A reg
573
574
Establish QS com
575
Request comms A-B
576
Response Y/N
106a
New QD key
HSM
577
QD key 3
578
580
QD key 3
QD key 3
579
QS comms using QD key 3

FIG. 5i

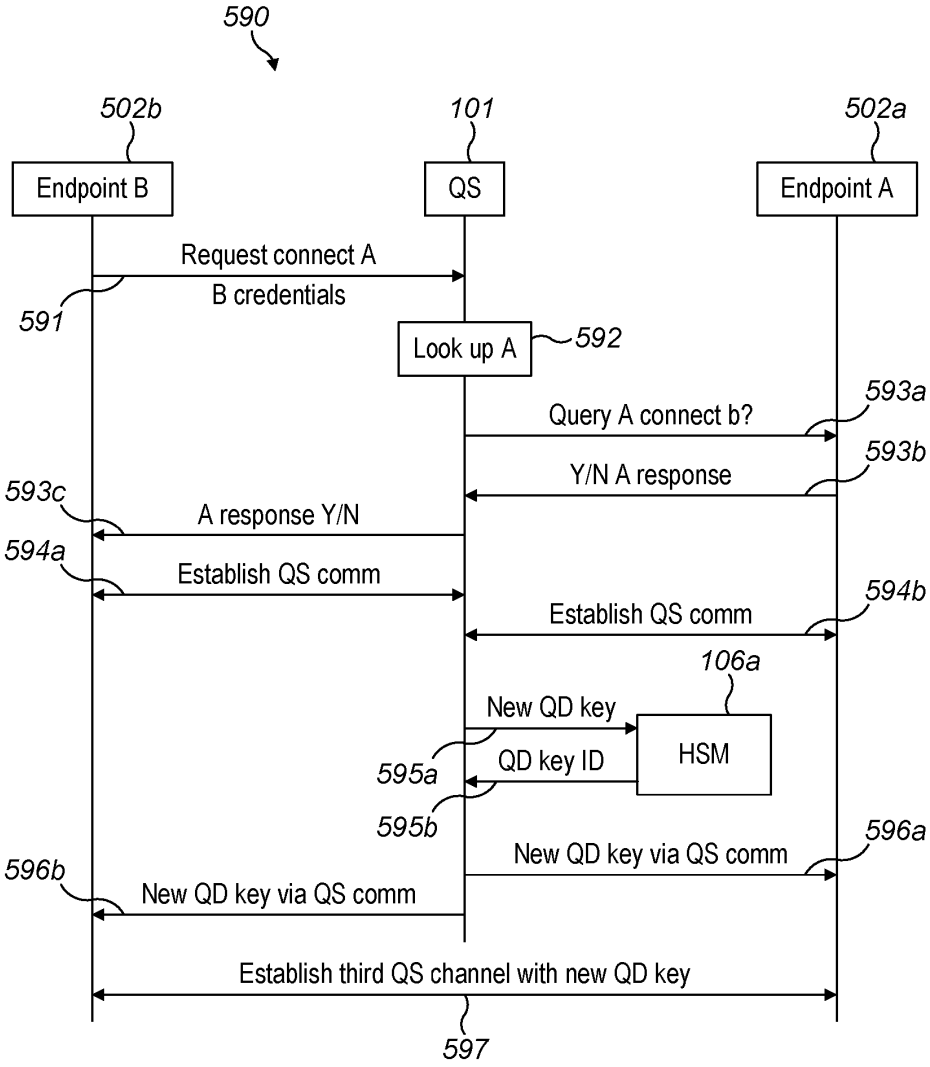

590
502b
101
502a
Endpoint B
QS
Endpoint A
Request connect A
B credentials
591
Look up A
592
593a
Query A connect b?
593b
Y/N A response
593c
A response Y/N
594a
Establish QS comm
Establish QS comm
594b
106a
New QD key
HSM
595a
QD key ID
595b
596a
New QD key via QS comm
596b
New QD key via QS comm
Establish third QS channel with new QD key
597

FIG. 5j

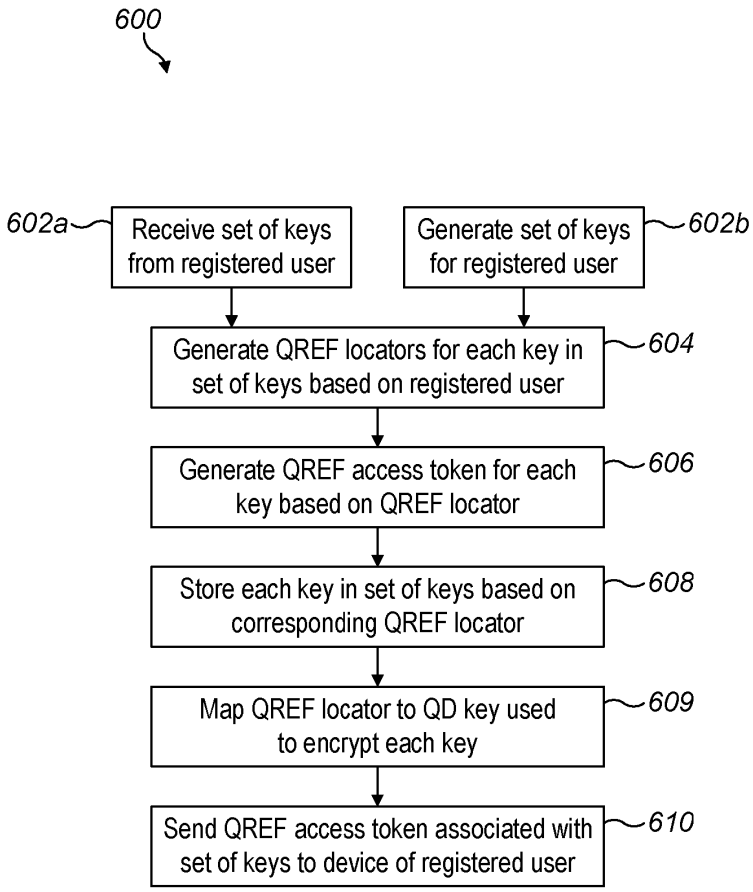

600
602a
Receive set of keys from registered user
Generate set of keys for registered user
602b
Generate QREF locators for each key in set of keys based on registered user
604
Generate QREF access token for each key based on QREF locator
606
Store each key in set of keys based on corresponding QREF locator
608
Map QREF locator to QD key used to encrypt each key
609
Send QREF access token associated with set of keys to device of registered user
610

FIG. 6a

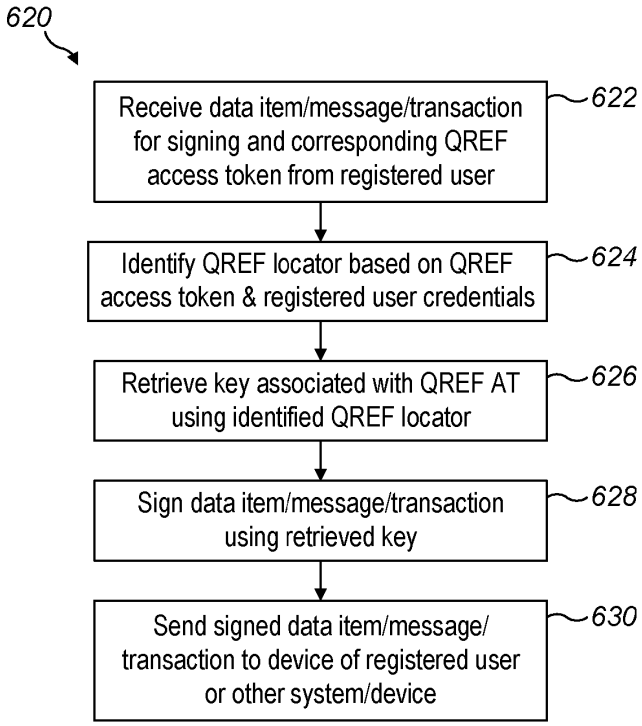

620
Receive data item/message/transaction for signing and corresponding QREF access token from registered user
622
Identify QREF locator based on QREF access token & registered user credentials
624
Retrieve key associated with QREF AT using identified QREF locator
626
Sign data item/message/transaction using retrieved key
628
Send signed data item/message/ transaction to device of registered user or other system/device
630

FIG. 6b

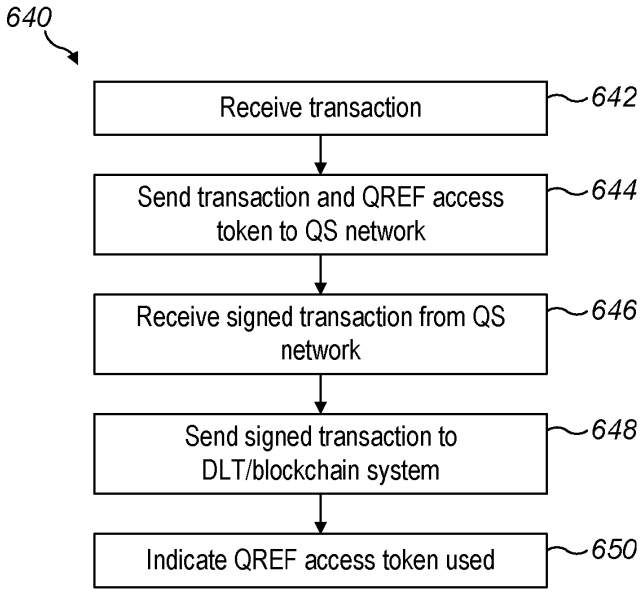

640
Receive transaction
642
Send transaction and QREF access token to QS network
644
Receive signed transaction from QS network
646
Send signed transaction to DLT/blockchain system
648
Indicate QREF access token used
650

FIG. 6c

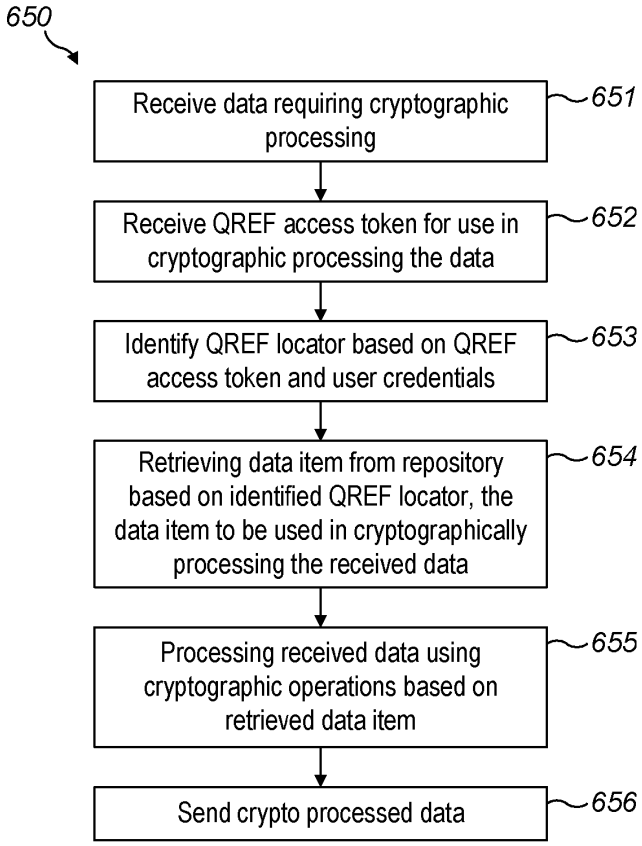

650
Receive data requiring cryptographic processing
651
Receive QREF access token for use in cryptographic processing the data
652
Identify QREF locator based on QREF access token and user credentials
653
Retrieving data item from repository based on identified QREF locator, the data item to be used in cryptographically processing the received data
654
Processing received data using cryptographic operations based on retrieved data item
655
Send crypto processed data
656

FIG. 6d

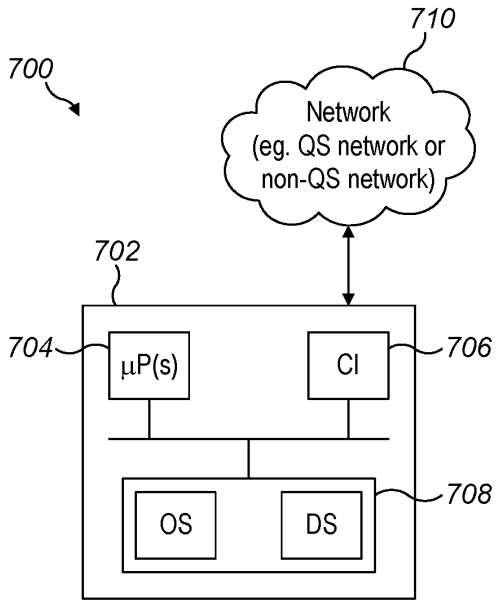

710
700
Network
(eg. QS network or
non-QS network)
702
704
µP(s)
CI
706
OS
DS
708

FIG. 7a

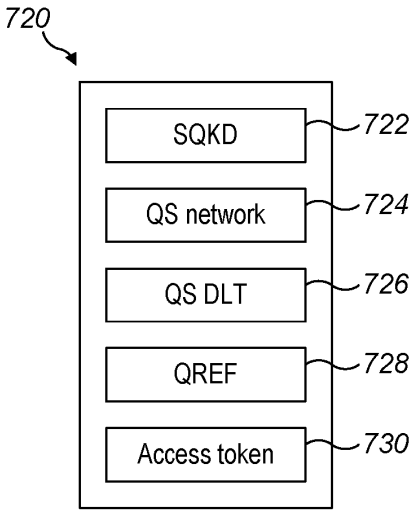

720
SQKD
722
QS network
724
QS DLT
726
QREF
728
Access token
730

FIG. 7b