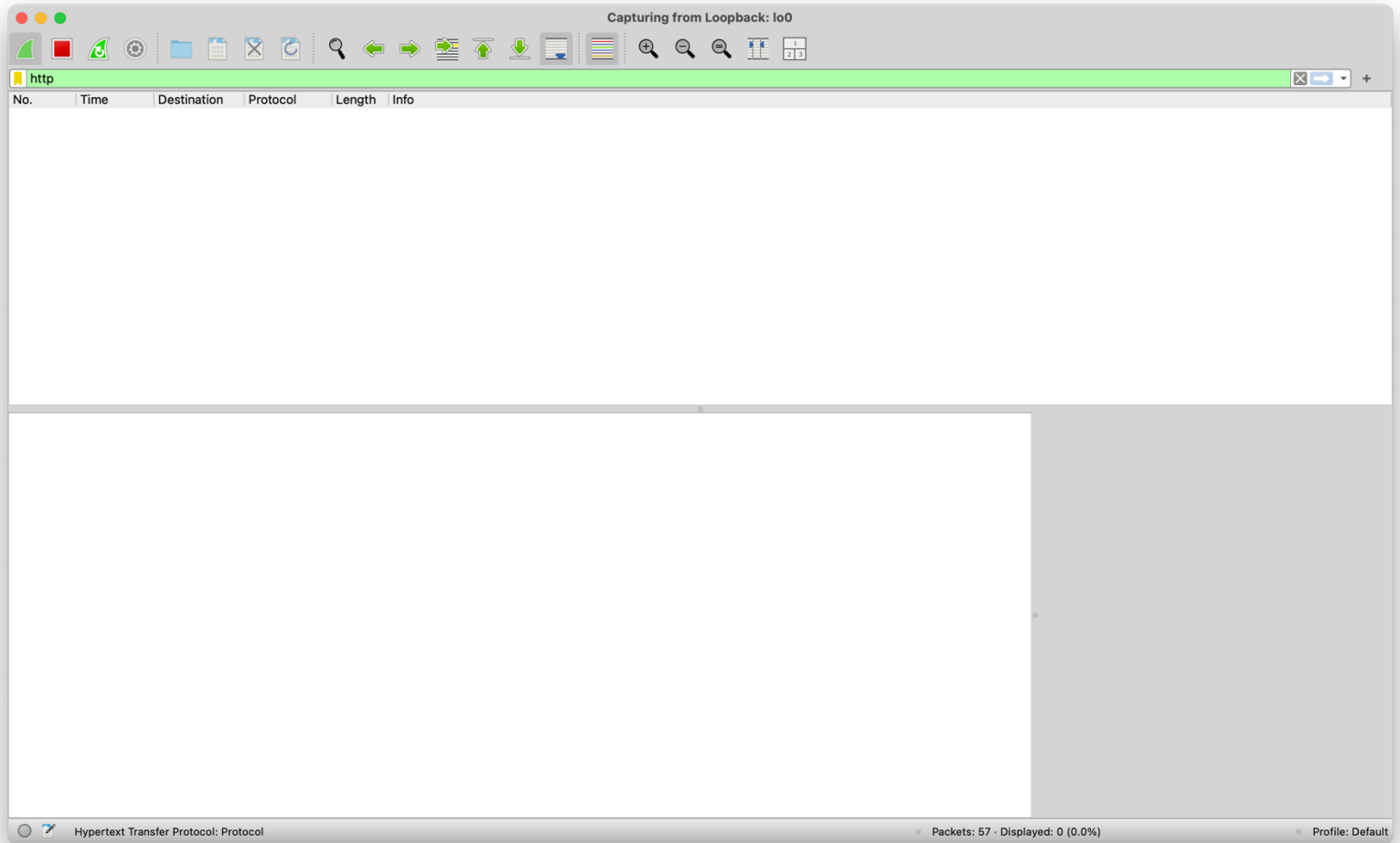
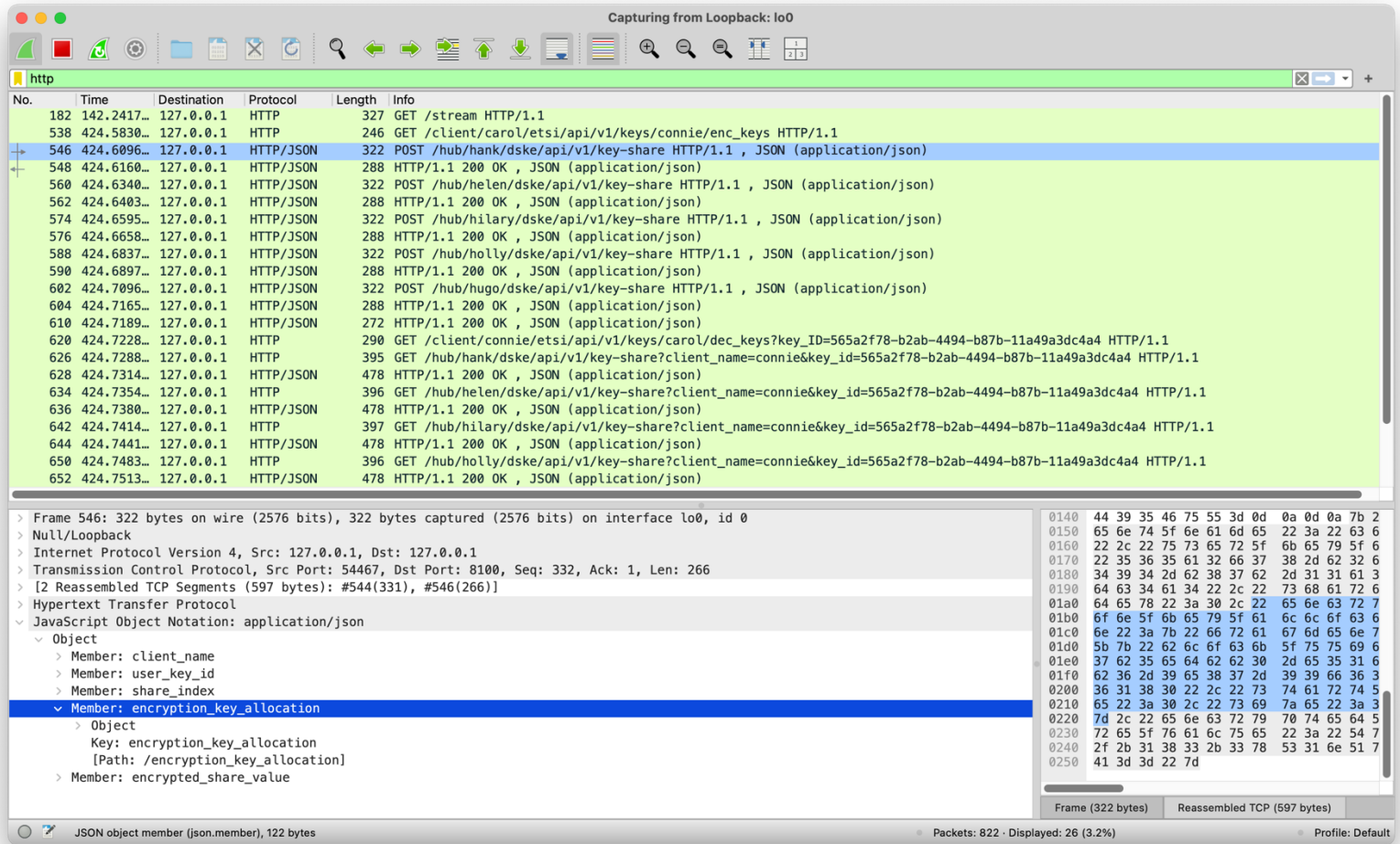
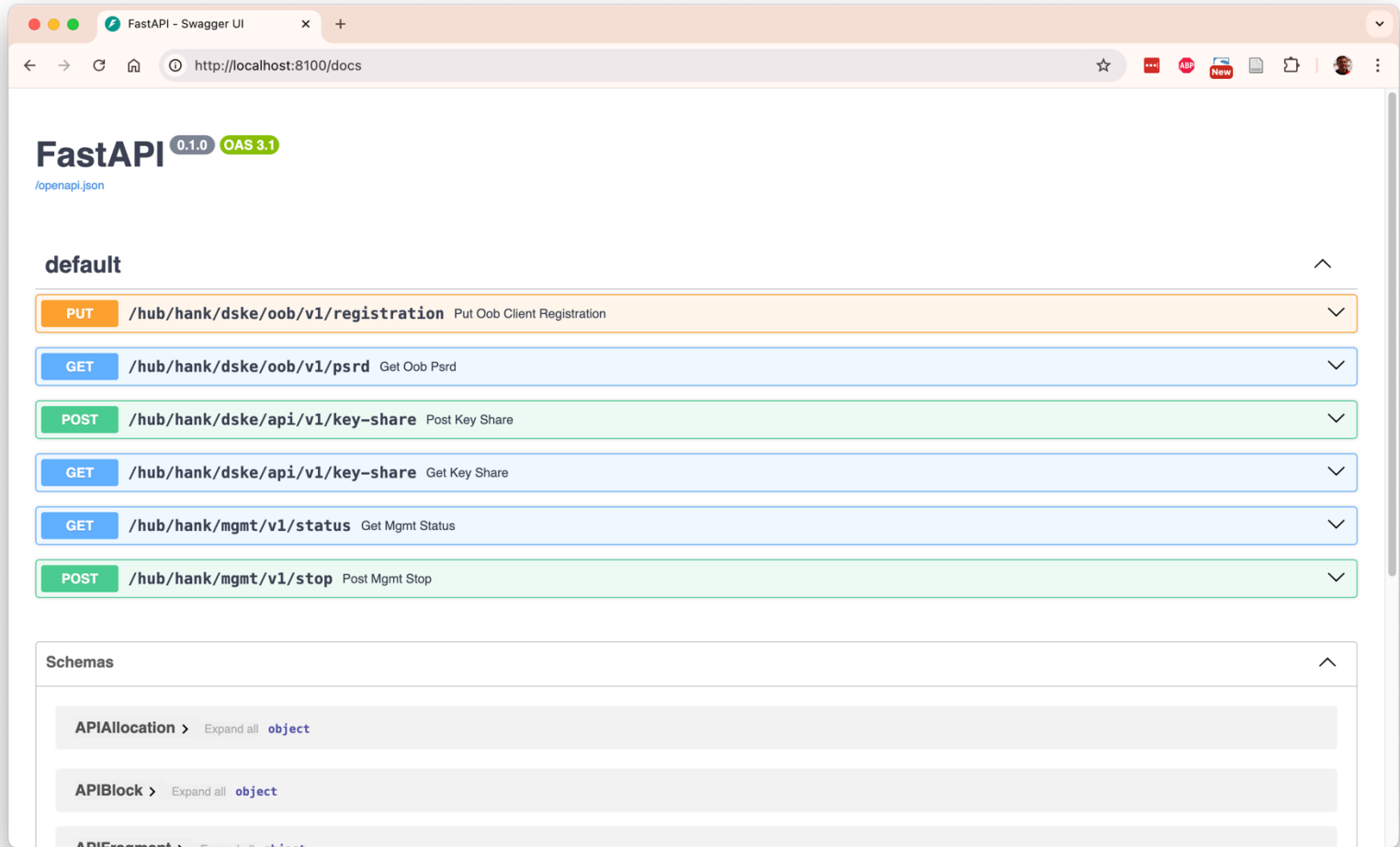
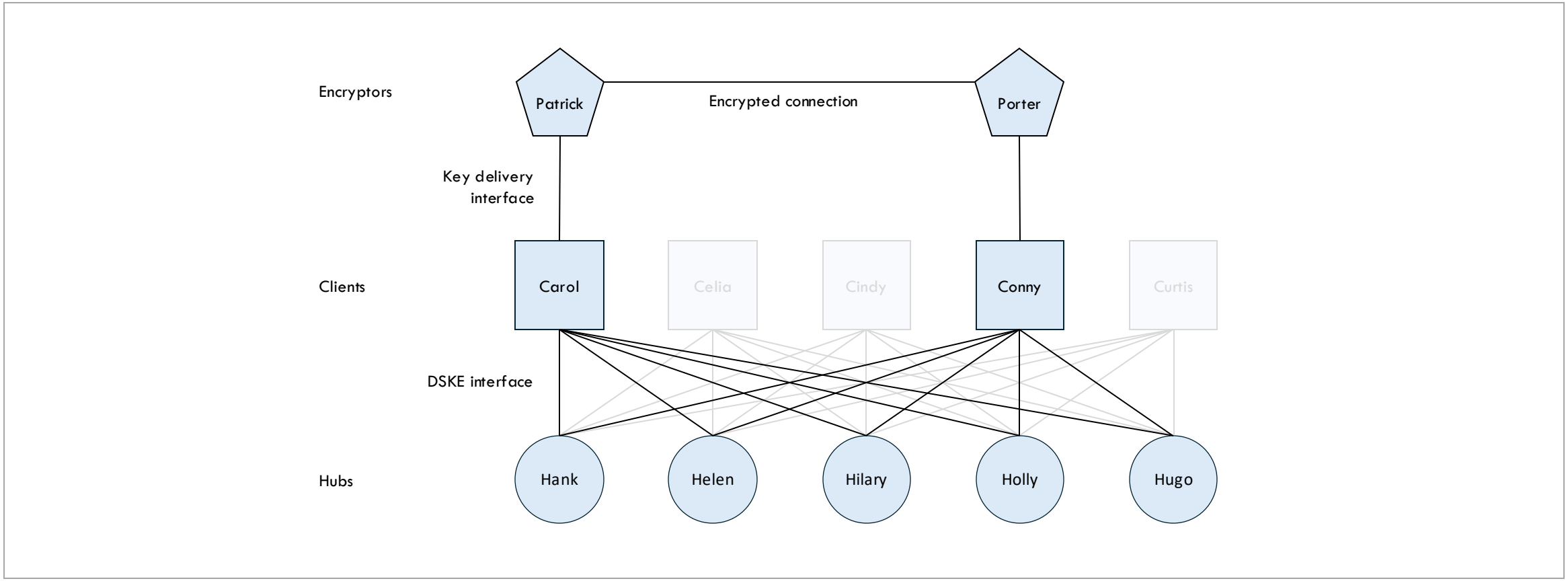
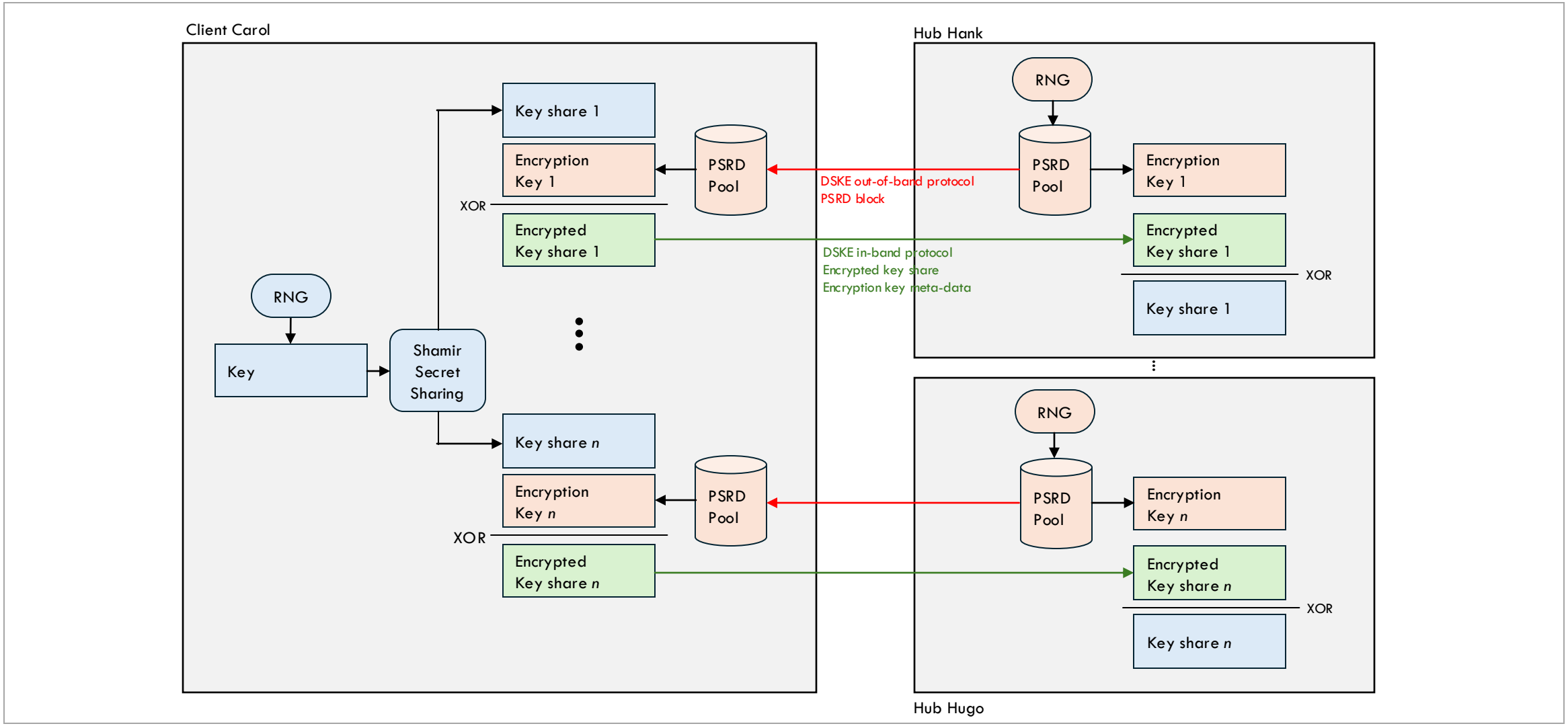
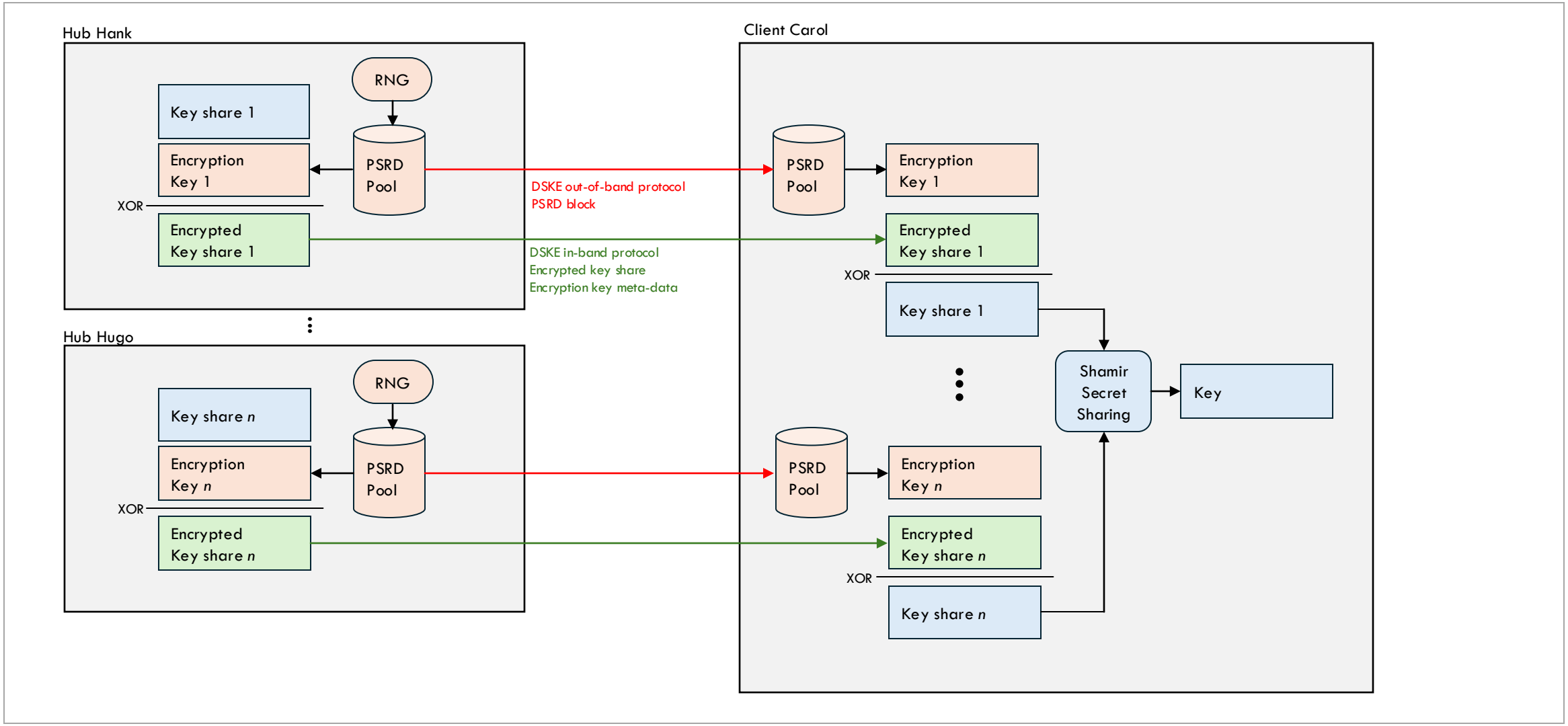

Capturing from Loopback: lo0
http
No.
Time
Destination
Protocol
Length
Info
Hypertext Transfer Protocol: Protocol
Packets: 57 · Displayed: 0 (0.0%)
Profile: Default

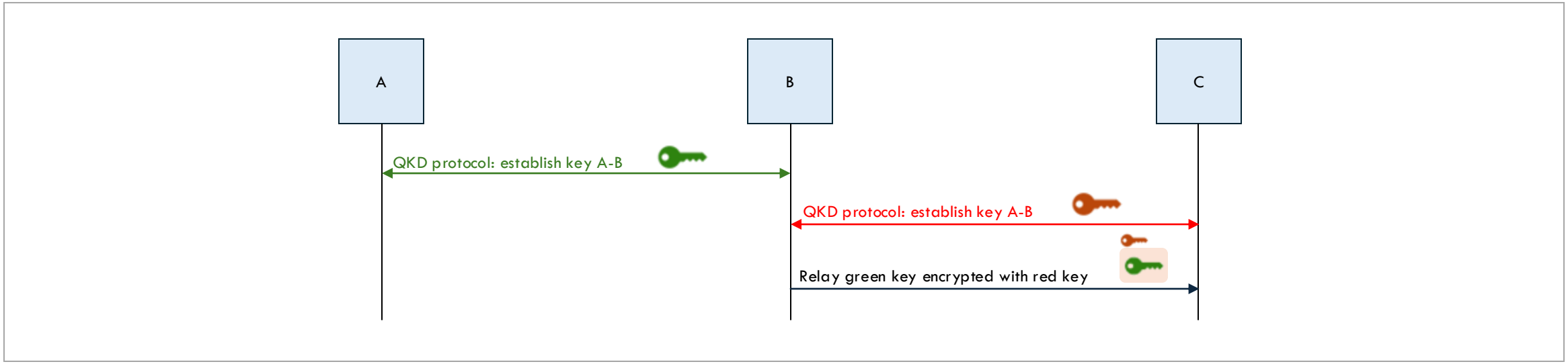

Capturing from Loopback: lo0
http
No. Time Destination Protocol Length Info
182 142.2417… 127.0.0.1 HTTP 327 GET /stream HTTP/1.1
538 424.5830… 127.0.0.1 HTTP 246 GET /client/carol/etsi/api/v1/keys/connie/enc_keys HTTP/1.1
546 424.6096… 127.0.0.1 HTTP/JSON 322 POST /hub/hank/dske/api/v1/key-share HTTP/1.1 , JSON (application/json)
548 424.6160… 127.0.0.1 HTTP/JSON 288 HTTP/1.1 200 OK , JSON (application/json)
560 424.6340… 127.0.0.1 HTTP/JSON 322 POST /hub/helen/dske/api/v1/key-share HTTP/1.1 , JSON (application/json)
562 424.6403… 127.0.0.1 HTTP/JSON 288 HTTP/1.1 200 OK , JSON (application/json)
574 424.6595… 127.0.0.1 HTTP/JSON 322 POST /hub/hilary/dske/api/v1/key-share HTTP/1.1 , JSON (application/json)
576 424.6658… 127.0.0.1 HTTP/JSON 288 HTTP/1.1 200 OK , JSON (application/json)
588 424.6837… 127.0.0.1 HTTP/JSON 322 POST /hub/holly/dske/api/v1/key-share HTTP/1.1 , JSON (application/json)
590 424.6897… 127.0.0.1 HTTP/JSON 288 HTTP/1.1 200 OK , JSON (application/json)
602 424.7096… 127.0.0.1 HTTP/JSON 322 POST /hub/hugo/dske/api/v1/key-share HTTP/1.1 , JSON (application/json)
604 424.7165… 127.0.0.1 HTTP/JSON 288 HTTP/1.1 200 OK , JSON (application/json)
610 424.7189… 127.0.0.1 HTTP/JSON 272 HTTP/1.1 200 OK , JSON (application/json)
620 424.7228… 127.0.0.1 HTTP 290 GET /client/connie/etsi/api/v1/keys/carol/dec_keys?key_ID=565a2f78-b2ab-4494-b87b-11a49a3dc4a4 HTTP/1.1
626 424.7288… 127.0.0.1 HTTP 395 GET /hub/hank/dske/api/v1/key-share?client_name=connie&key_id=565a2f78-b2ab-4494-b87b-11a49a3dc4a4 HTTP/1.1
628 424.7314… 127.0.0.1 HTTP/JSON 478 HTTP/1.1 200 OK , JSON (application/json)
634 424.7354… 127.0.0.1 HTTP 396 GET /hub/helen/dske/api/v1/key-share?client_name=connie&key_id=565a2f78-b2ab-4494-b87b-11a49a3dc4a4 HTTP/1.1
636 424.7380… 127.0.0.1 HTTP/JSON 478 HTTP/1.1 200 OK , JSON (application/json)
642 424.7414… 127.0.0.1 HTTP 397 GET /hub/hilary/dske/api/v1/key-share?client_name=connie&key_id=565a2f78-b2ab-4494-b87b-11a49a3dc4a4 HTTP/1.1
644 424.7441… 127.0.0.1 HTTP/JSON 478 HTTP/1.1 200 OK , JSON (application/json)
650 424.7483… 127.0.0.1 HTTP 396 GET /hub/holly/dske/api/v1/key-share?client_name=connie&key_id=565a2f78-b2ab-4494-b87b-11a49a3dc4a4 HTTP/1.1
652 424.7513… 127.0.0.1 HTTP/JSON 478 HTTP/1.1 200 OK , JSON (application/json)
Frame 546: 322 bytes on wire (2576 bits), 322 bytes captured (2576 bits) on interface lo0, id 0
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 54467, Dst Port: 8100, Seq: 332, Ack: 1, Len: 266
[2 Reassembled TCP Segments (597 bytes): #544(331), #546(266)]
Hypertext Transfer Protocol
JavaScript Object Notation: application/json
Object
Member: client_name
Member: user_key_id
Member: share_index
Member: encryption_key_allocation
Object
Key: encryption_key_allocation
[Path: /encryption_key_allocation]
Member: encrypted_share_value
0140 44 39 35 46 75 55 3d 0d 0a 0d 0a 7b 2
0150 65 6e 74 5f 6e 61 6d 65 22 3a 22 63 6
0160 22 2c 22 75 73 65 72 5f 6b 65 79 5f 6
0170 22 35 36 35 61 32 66 37 38 2d 62 32 6
0180 34 39 34 2d 62 38 37 62 2d 31 31 61 3
0190 64 63 34 61 34 22 2c 22 73 68 61 72 6
01a0 64 65 78 22 3a 30 2c 22 65 6e 63 72 7
01b0 6f 6e 5f 6b 65 79 5f 61 6c 6c 6f 63 6
01c0 6e 22 3a 7b 22 66 72 61 67 6d 65 6e 7
01d0 5b 7b 22 62 6c 6f 63 6b 5f 75 75 69 6
01e0 37 62 35 65 64 62 62 30 2d 65 35 31 6
01f0 62 36 2d 39 65 38 37 2d 39 39 66 36 3
0200 36 31 38 30 22 2c 22 73 74 61 72 74 5
0210 65 22 3a 30 2c 22 73 69 7a 65 22 3a 3
0220 7d 2c 22 65 6e 63 72 79 70 74 65 64 5
0230 72 65 5f 76 61 6c 75 65 22 3a 22 54 7
0240 2f 2b 31 38 33 2b 33 78 53 31 6e 51 7
0250 41 3d 3d 22 7d
Frame (322 bytes)
Reassembled TCP (597 bytes)
JSON object member (json.member), 122 bytes
Packets: 822 · Displayed: 26 (3.2%)
Profile: Default

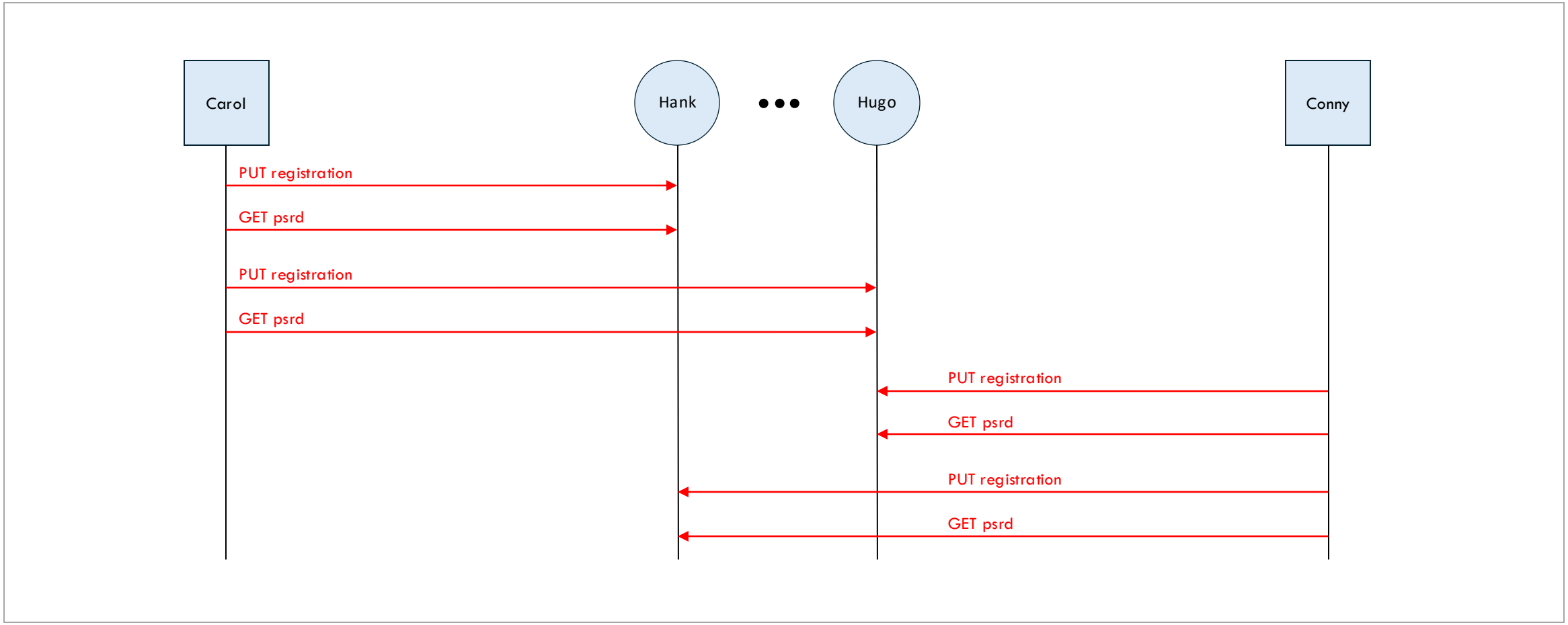

FastAPI - Swagger UI
http://localhost:8100/docs
FastAPI
0.1.0
OAS 3.1
/openapi.json
default
PUT /hub/hank/dske/oob/v1/registration Put Oob Client Registration
GET /hub/hank/dske/oob/v1/psrd Get Oob Psrd
POST /hub/hank/dske/api/v1/key-share Post Key Share
GET /hub/hank/dske/api/v1/key-share Get Key Share
GET /hub/hank/mgmt/v1/status Get Mgmt Status
POST /hub/hank/mgmt/v1/stop Post Mgmt Stop
Schemas
APIAllocation Expand all object
APIBlock Expand all object

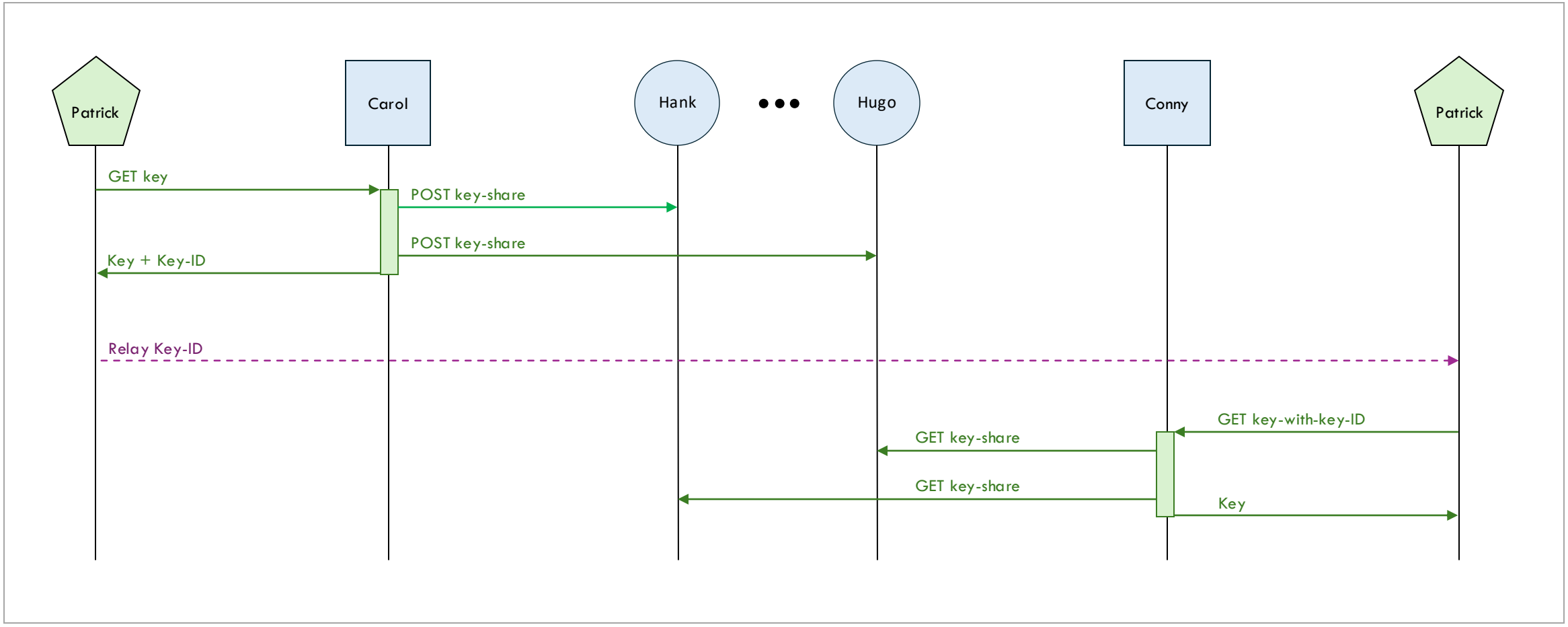

Encryptors
Patrick
Encrypted connection
Porter
Key delivery interface
Clients
Carol
Celia
Cindy
Conny
Curtis
DSKE interface
Hubs
Hank
Helen
Hilary
Holly
Hugo

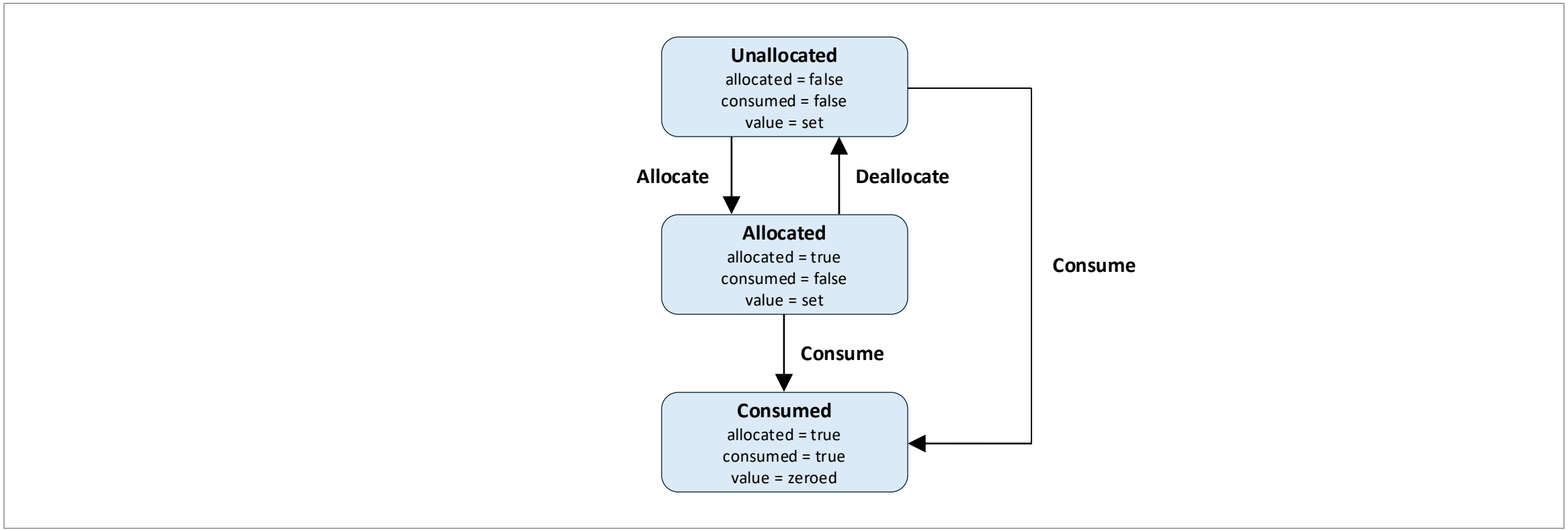

Client Carol
Hub Hank
Hub Hugo
RNG
Key
Shamir Secret Sharing
Key share 1
Encryption Key 1
XOR
Encrypted Key share 1
PSRD Pool
Key share n
Encryption Key n
Encrypted Key share n
DSKE out-of-band protocol
PSRD block
DSKE in-band protocol
Encrypted key share
Encryption key meta-data
RNG
PSRD Pool
Encryption Key 1
Encrypted Key share 1
XOR
Key share 1
RNG
PSRD Pool
Encryption Key n
Encrypted Key share n
XOR
Key share n

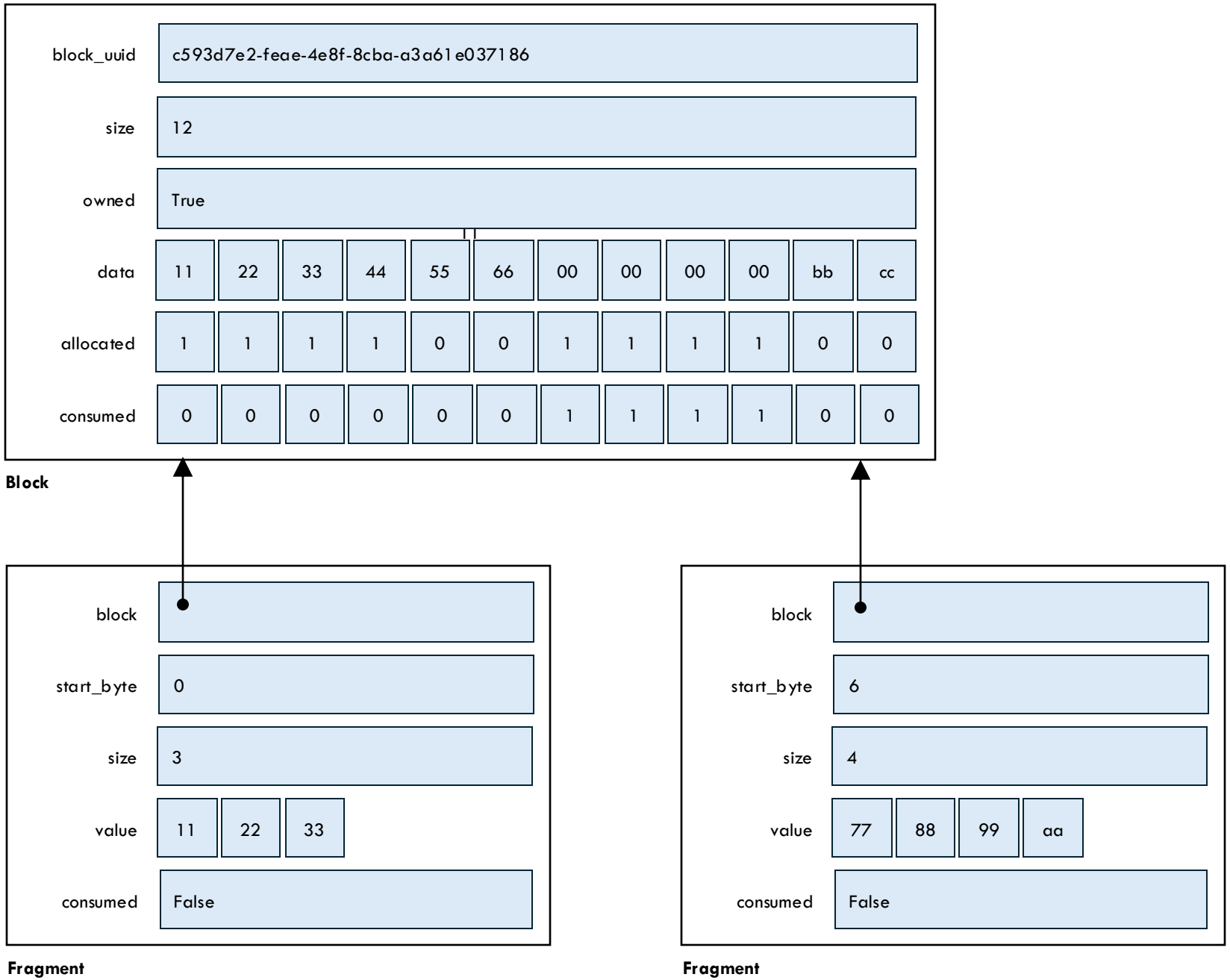

Hub Hank
RNG
Key share 1
Encryption Key 1
PSRD Pool
XOR
Encrypted Key share 1
DSKE out-of-band protocol
PSRD block
DSKE in-band protocol
Encrypted key share
Encryption key meta-data
Client Carol
PSRD Pool
Encryption Key 1
Encrypted Key share 1
XOR
Key share 1
Shamir Secret Sharing
Key
Hub Hugo
RNG
Key share n
Encryption Key n
PSRD Pool
XOR
Encrypted Key share n
PSRD Pool
Encryption Key n
Encrypted Key share n
XOR
Key share n


A
B
C
QKD protocol: establish key A-B
QKD protocol: establish key A-B
Relay green key encrypted with red key


Carol
Hank
Hugo
Conny
PUT registration
GET psrd
PUT registration
GET psrd
PUT registration
GET psrd
PUT registration
GET psrd


Patrick
Carol
Hank
Hugo
Conny
Patrick
GET key
POST key-share
POST key-share
Key + Key-ID
Relay Key-ID
GET key-with-key-ID
GET key-share
GET key-share
Key


Unallocated
allocated = false
consumed = false
value = set
Allocate
Deallocate
Allocated
allocated = true
consumed = false
value = set
Consume
Consume
Consumed
allocated = true
consumed = true
value = zeroed


block_uuid
c593d7e2-feae-4e8f-8cba-a3a61e037186
size
12
owned
True
data
11 22 33 44 55 66 00 00 00 00 bb cc
allocated
1 1 1 1 0 0 1 1 1 1 0 0
consumed
0 0 0 0 0 0 1 1 1 1 0 0
Block
block
start_byte
0
size
3
value
11 22 33
consumed
False
Fragment
block
start_byte
6
size
4
value
77 88 99 aa
consumed
False
Fragment