

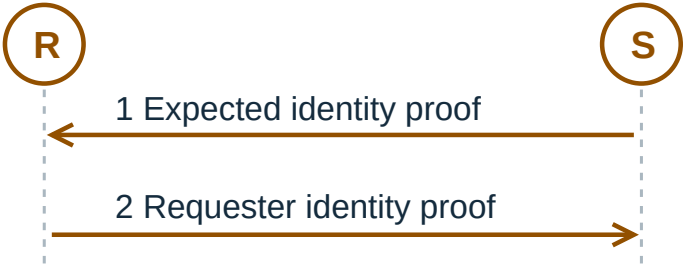
Connection

Select a service mode. Establish the channel. Exchange protected operations.

01 HS2 — choose the identification model

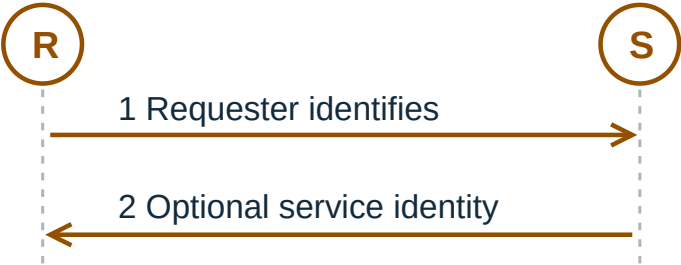
R = requester · S = service

A / KNOWN DESTINATION



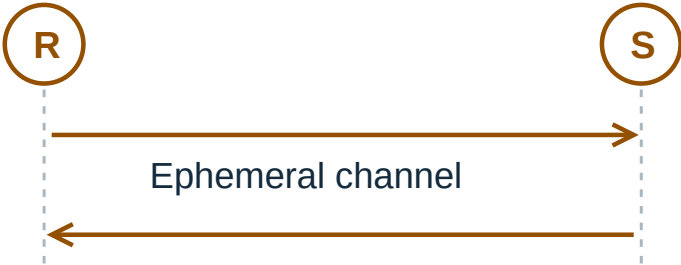
R knows the exact service SCIR.

B / ALIAS SERVICE



Identity disclosure inside the channel.

C / UNIDENTIFIED

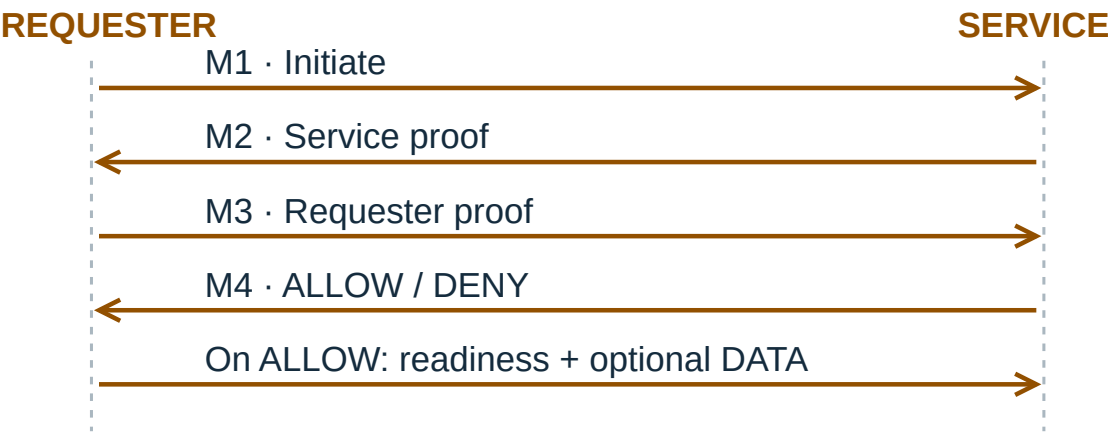


No PRP identity proof on either side.

Identity proof and permission are separate: service policy decides which operations are allowed.
B/C initial key substitution remains a risk; later identity disclosure cannot undo earlier exposure.

02 Initial laboratory profiles / A1 · B1 · C1

A1



B1 / C1

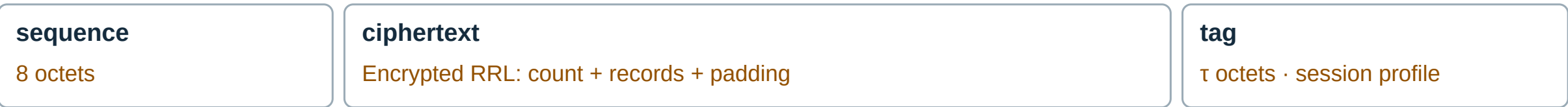


Five-frame establishment.
Explicit profile selection.
A1/B1: Ed25519ctx identities.
C1: no identity proof.

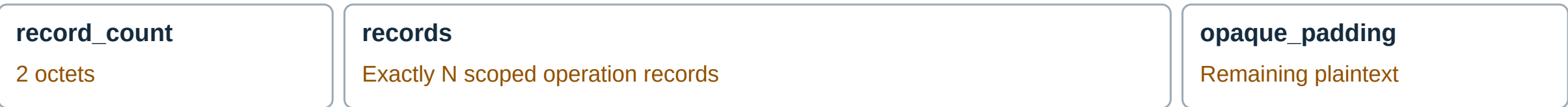
A1 readiness may carry the first DATA, or be internal control. These are laboratory contracts.

03 AOP contains the Route-Record List

AOP / COMPLETE SESSION-PROTECTED PACKET



RRL / DECRYPTED OPERATION CONTAINER



Each record: route_alias[2] | kind[1] | flags[1] | body_length[2] | body[variable].
Authenticate the complete AOP before dispatch. Record kinds are selected by the service.

04 Exchange data; maintain rules with RCP



RCP governs authenticated relationship rules. Relationships, keys and paths have distinct lifetimes.
B1/C1 have separate record framing. A1 selects a restricted RRL service without padding.

CONTINUE / RELATION CONTROL ATLAS

HS2 establishes the channel; RCP declares, proposes and conditions the rules of the relationship.