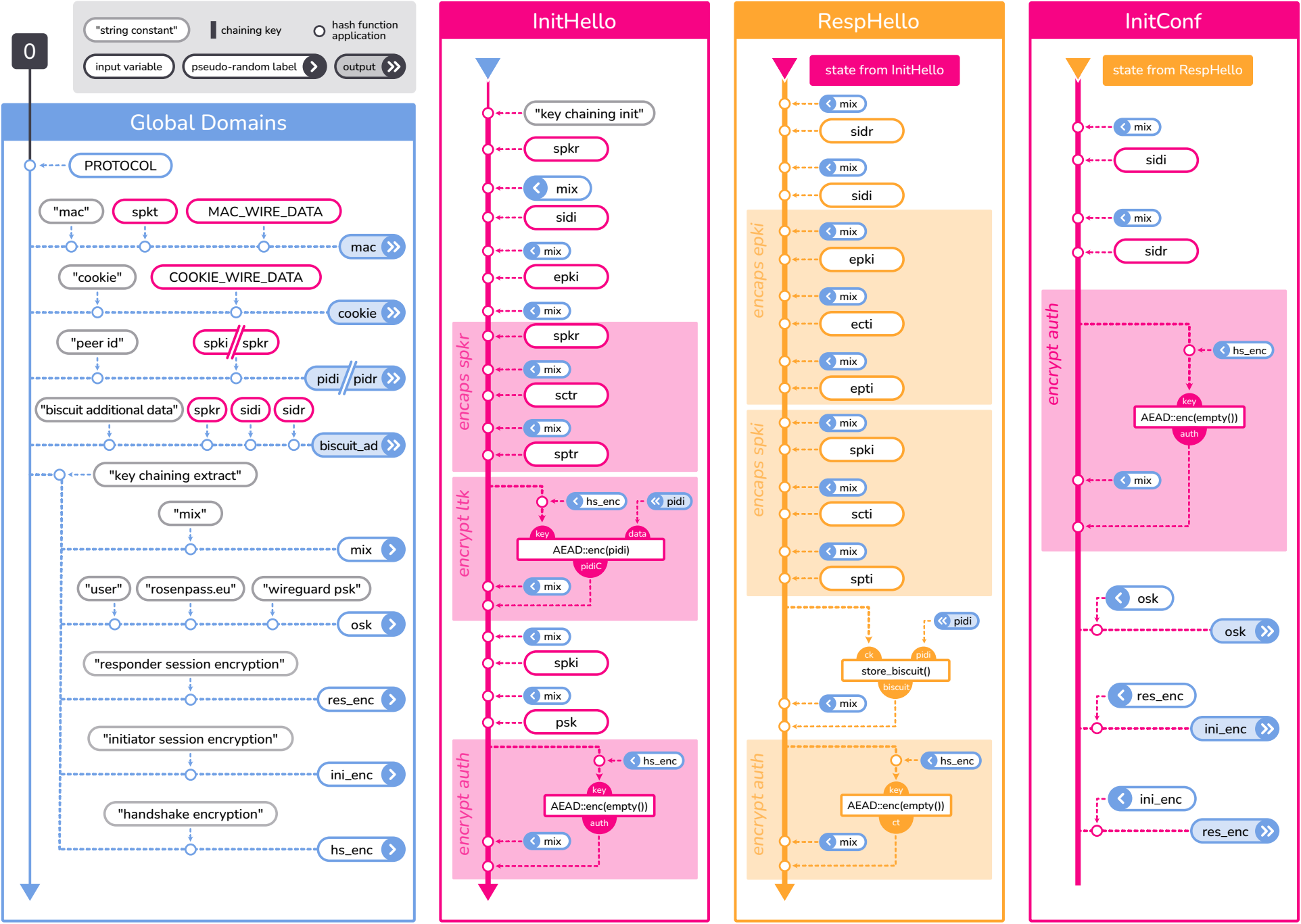
"string constant"
chaining key
hash function application
input variable
pseudo-random label
output
0
Global Domains
PROTOCOL
"mac"
spkt
MAC_WIRE_DATA
mac
"cookie"
COOKIE_WIRE_DATA
cookie
"peer id"
spki
spkr
pidi
pidr
"biscuit additional data"
spkr
sidi
sidr
biscuit_ad
"key chaining extract"
"mix"
mix
"user"
"rosenpass.eu"
"wireguard psk"
osk
"responder session encryption"
res_enc
"initiator session encryption"
ini_enc
"handshake encryption"
hs_enc
InitHello
"key chaining init"
spkr
mix
sidi
mix
epki
mix
encaps spkr
spkr
mix
sctr
mix
sptr
encrypt ltk
hs_enc
pidi
key
data
AEAD::enc(pidi)
pidiC
mix
mix
spki
mix
psk
encrypt auth
hs_enc
key
AEAD::enc(empty())
auth
mix
RespHello
state from InitHello
mix
sidr
mix
sidi
encaps epki
mix
epki
mix
ecti
mix
epti
encaps spki
mix
spki
mix
scti
mix
spti
pidi
ck
pidi
store_biscuit()
biscuit
mix
encrypt auth
hs_enc
key
AEAD::enc(empty())
ct
mix
InitConf
state from RespHello
mix
sidi
mix
sidr
encrypt auth
hs_enc
key
AEAD::enc(empty())
auth
mix
osk
osk
res_enc
ini_enc
ini_enc
res_enc