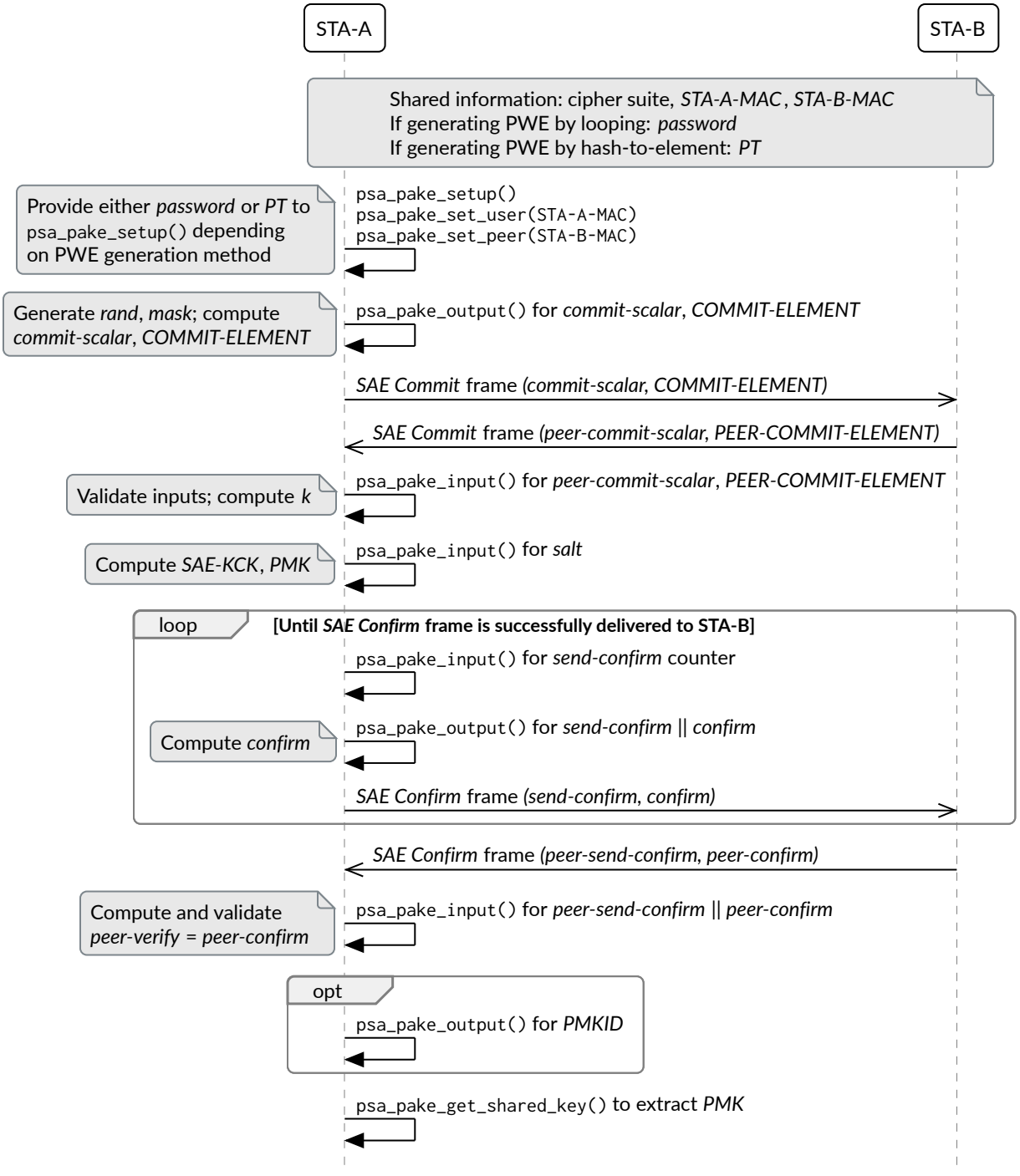
STA-A
STA-B
Shared information: cipher suite, STA-A-MAC, STA-B-MAC
If generating PWE by looping: password
If generating PWE by hash-to-element: PT
Provide either password or PT to psa_pake_setup() depending on PWE generation method
psa_pake_setup()
psa_pake_set_user(STA-A-MAC)
psa_pake_set_peer(STA-B-MAC)
Generate rand, mask; compute commit-scalar, COMMIT-ELEMENT
psa_pake_output() for commit-scalar, COMMIT-ELEMENT
SAE Commit frame (commit-scalar, COMMIT-ELEMENT)
SAE Commit frame (peer-commit-scalar, PEER-COMMIT-ELEMENT)
Validate inputs; compute k
psa_pake_input() for peer-commit-scalar, PEER-COMMIT-ELEMENT
Compute SAE-KCK, PMK
psa_pake_input() for salt
loop
[Until SAE Confirm frame is successfully delivered to STA-B]
psa_pake_input() for send-confirm counter
Compute confirm
psa_pake_output() for send-confirm || confirm
SAE Confirm frame (send-confirm, confirm)
SAE Confirm frame (peer-send-confirm, peer-confirm)
Compute and validate peer-verify = peer-confirm
psa_pake_input() for peer-send-confirm || peer-confirm
opt
psa_pake_output() for PMKID
psa_pake_get_shared_key() to extract PMK