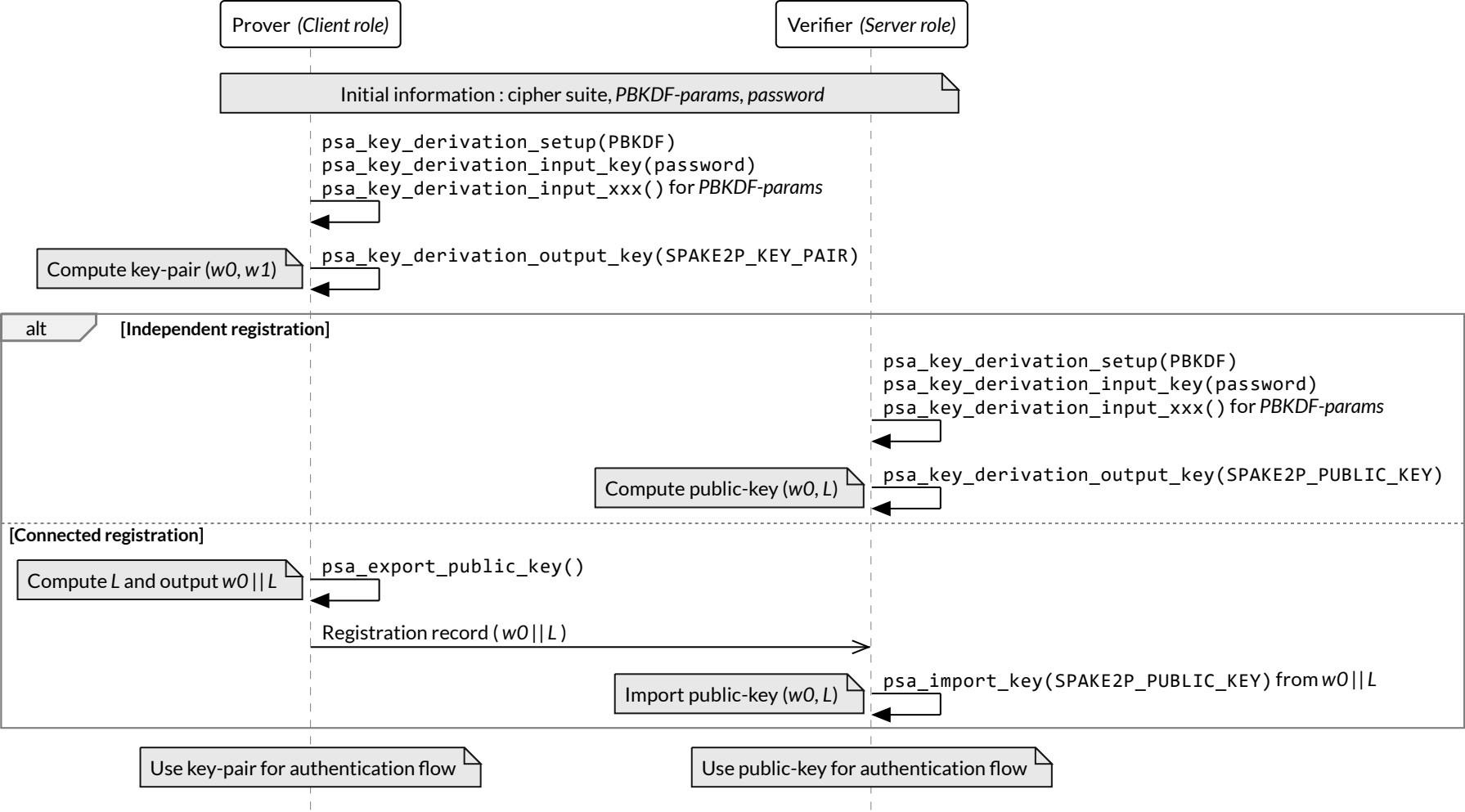
Prover (Client role)
Verifier (Server role)
Initial information : cipher suite, PBKDF-params, password
psa_key_derivation_setup(PBKDF)
psa_key_derivation_input_key(password)
psa_key_derivation_input_xxx() for PBKDF-params
Compute key-pair (w0, w1)
psa_key_derivation_output_key(SPAKE2P_KEY_PAIR)
alt
[Independent registration]
psa_key_derivation_setup(PBKDF)
psa_key_derivation_input_key(password)
psa_key_derivation_input_xxx() for PBKDF-params
Compute public-key (w0, L)
psa_key_derivation_output_key(SPAKE2P_PUBLIC_KEY)
[Connected registration]
Compute L and output w0 || L
psa_export_public_key()
Registration record (w0 || L)
Import public-key (w0, L)
psa_import_key(SPAKE2P_PUBLIC_KEY) from w0 || L
Use key-pair for authentication flow
Use public-key for authentication flow