

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 (w_0 , w_1)

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 key pair (w_0 , w_1)

psa_key_derivation_output_key(SPAKE2P_KEY_PAIR)

[Connected registration]

Compute L and output $w_0 \parallel L$

psa_export_public_key()

Registration record ($w_0 \parallel L$)

Import public key (w_0 , L)

psa_import_key(SPAKE2P_PUBLIC_KEY) from $w_0 \parallel L$

Use key pair for authentication flow

Use key for authentication flow