

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

psa\_key\_derivation\_output\_key(SPAKE2P\_KEY\_PAIR)

Compute key pair ( $w_0$ ,  $w_1$ )

alt

[Independent registration]

psa\_key\_derivation\_setup(PBKDF)  
psa\_key\_derivation\_input\_key(password)  
psa\_key\_derivation\_input\_xxx() for PBKDF-params

psa\_key\_derivation\_output\_key(SPAKE2P\_KEY\_PAIR)

Compute key pair ( $w_0$ ,  $w_1$ )

[Connected registration]

Compute  $L$  and output  $w_0 || L$

psa\_export\_public\_key()

Registration record ( $w_0 || L$ )

Import public key ( $w_0$ ,  $L$ )

psa\_import\_key(SPAKE2P\_PUBLIC\_KEY) from  $w_0 || L$

Use key pair for authentication flow

Use key for authentication flow