

station (STA)

Initial information : cipher suite, *SSID*, *password* [, *password-identifier*]

alt

[Hash-to-element generation of password element]

```
psa_key_derivation_setup(WPA3_SAE_H2E)
psa_key_derivation_input_bytes(SALT = SSID)
psa_key_derivation_input_key(PASSWORD = password)
```



opt

```
psa_key_derivation_input_bytes(INFO = password-identifier)
```



Compute password token *PT*

```
psa_key_derivation_output_key(WPA3_SAE_XX)
```



Use *PT* for authentication flow

[Generation of the password element by looping]

Use *password* for authentication flow