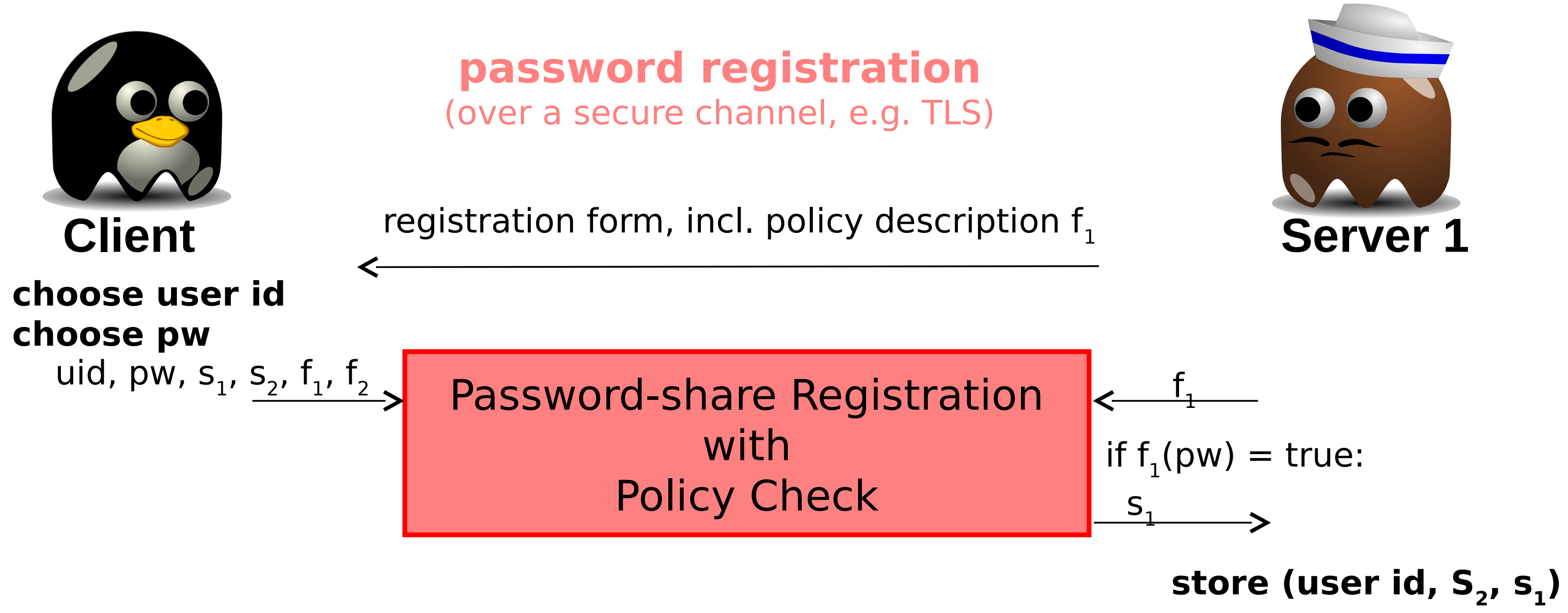
password registration

(over a secure channel, e.g. TLS)



Client

Server 1

registration form, incl. policy description f_1

choose user id
choose pw

uid, pw, s_1, s_2, f_1, f_2

Password-share Registration
with
Policy Check

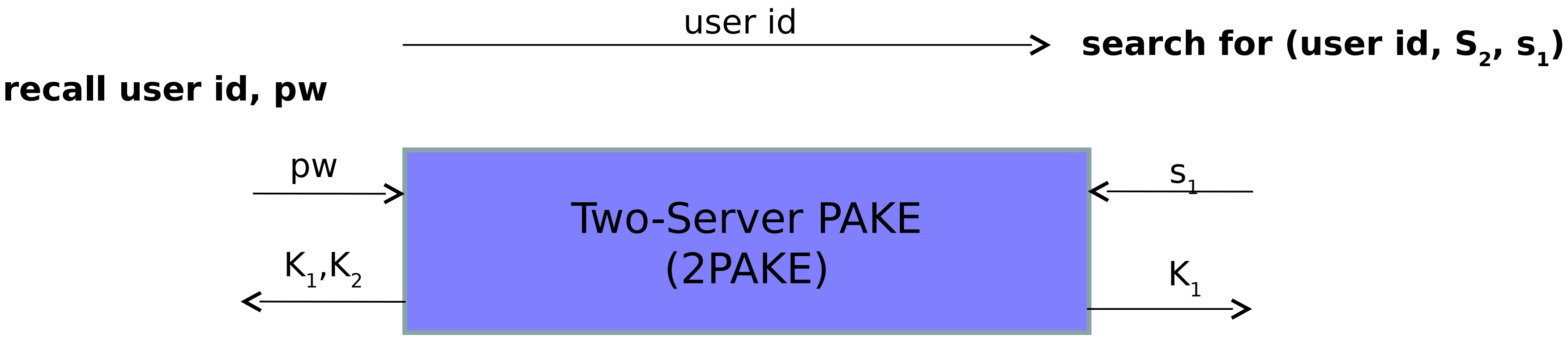
f_1

if f_1(pw) = true:

s_1

store (user id, S_2, s_1)

password authentication



user id

search for (user id, S_2, s_1)

recall user id, pw

pw

s_1

Two-Server PAKE
(2PAKE)

K_1,K_2

K_1