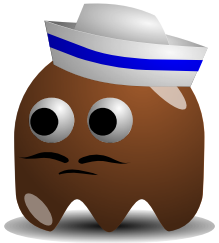
Client



Server 1

Server 2

password registration

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

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_2

f_1

if f(pw) = true:

s_1

s_2

store (user id, S_2, s_1)

password authentication

user id

search for (user id, S_2, s_1)

recall user id, pw

pw

K_1,K_2

Two-Server PAKE (2PAKE)

s_1

s_2

K_1