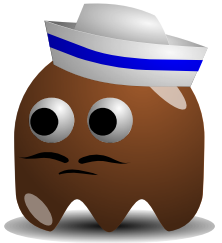
Client

password registration

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



Server

registration form, incl. policy description f

choose user id
choose pw

pw, f

f

Password Registration
with
Policy Check

r

if f(pw) = true:
H(pw, r)

user id, r

store (user id, H(pw, r), r)

password authentication

user id

search for (user id, H(pw, r), r)

recall user id, pw

pw

H(pw, r), r

Verifier-based PAKE
(VPAKE)

K

K