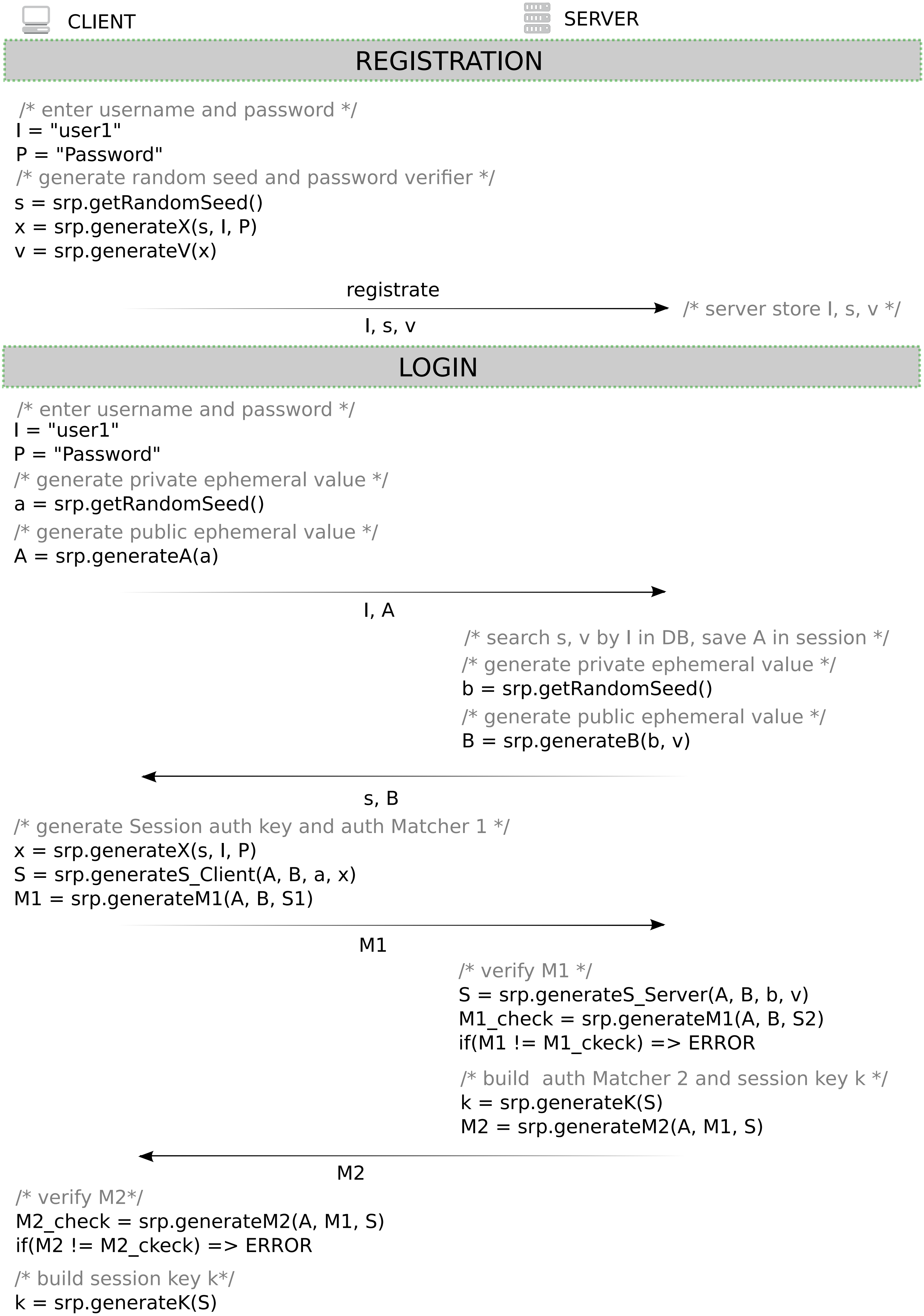

CLIENT

SERVER

REGISTRATION

/* enter username and password */
I = "user1"
P = "Password"
/* generate random seed and password verifier */
s = srp.getRandomSeed()
x = srp.generateX(s, I, P)
v = srp.generateV(x)

registrate → I, s, v

/* server store I, s, v */

LOGIN

/* enter username and password */
I = "user1"
P = "Password"
/* generate private ephemeral value */
a = srp.getRandomSeed()
/* generate public ephemeral value */
A = srp.generateA(a)

→ I, A

/* search s, v by I in DB, save A in session */
/* generate private ephemeral value */
b = srp.getRandomSeed()
/* generate public ephemeral value */
B = srp.generateB(b, v)

← s, B

/* generate Session auth key and auth Matcher 1 */
x = srp.generateX(s, I, P)
S = srp.generateS_Client(A, B, a, x)
M1 = srp.generateM1(A, B, S1)

→ M1

/* verify M1 */
S = srp.generateS_Server(A, B, b, v)
M1_check = srp.generateM1(A, B, S2)
if(M1 != M1_ckeck) => ERROR

/* build auth Matcher 2 and session key k */
k = srp.generateK(S)
M2 = srp.generateM2(A, M1, S)

← M2

/* verify M2*/
M2_check = srp.generateM2(A, M1, S)
if(M2 != M2_ckeck) => ERROR

/* build session key k*/
k = srp.generateK(S)