Tresorit password authentication

Notation

- *u – user's unique identifier (e.g. e-mail address)*
- *p* – user password
- *x* – secret derived from user password
- *s* – salt of a message, uniformly randomly generated by the client
- *n* – a freshly generated, uniformly random number (nonce)
- *H(p,s,i)* – a password derivation function, where *p* password, *s* salt, *i* is the number of iterations. Current function is PBKDFv2_HMAC_SHA1

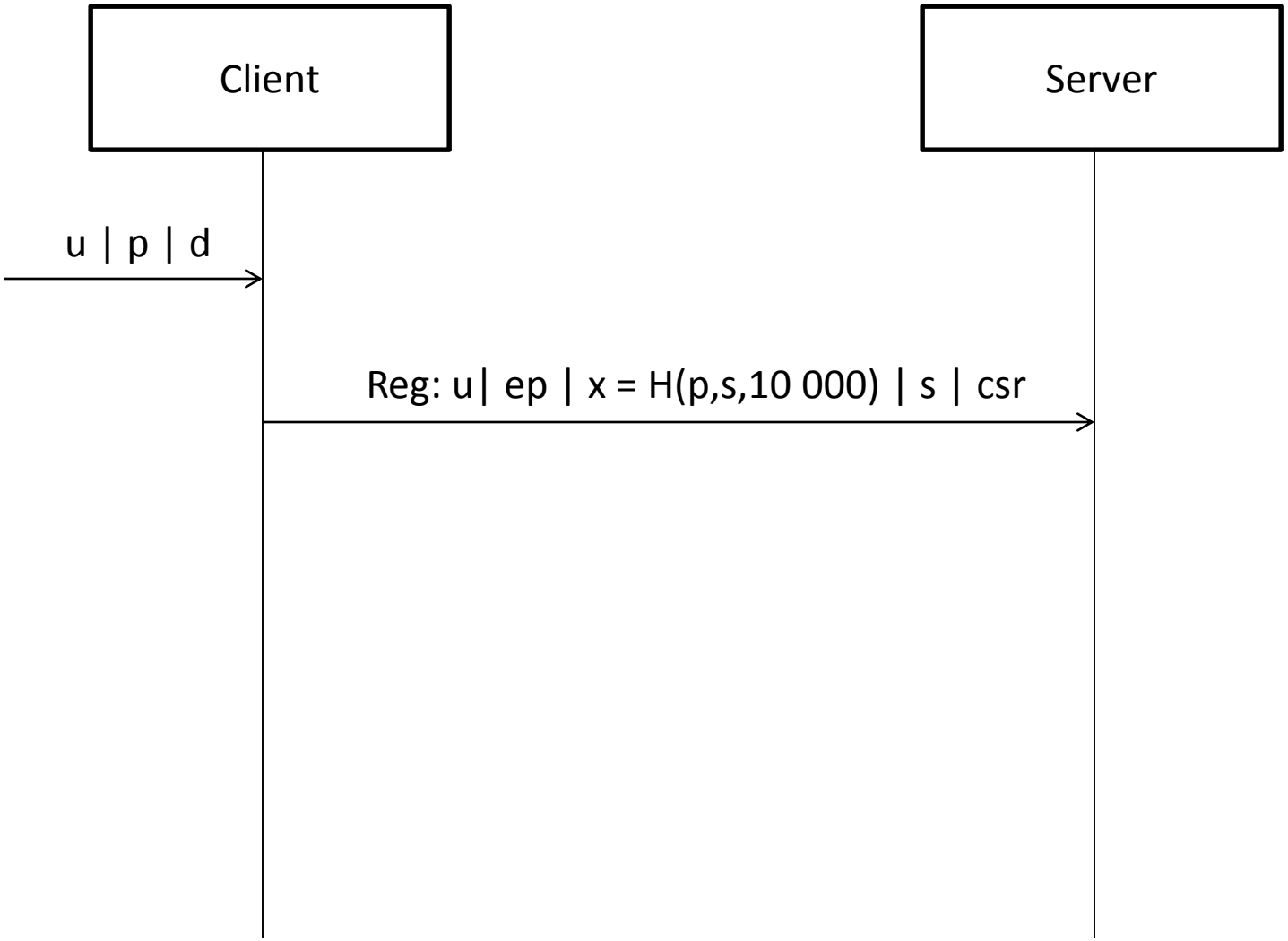
Minimal assumption

- All communication is over TLS (!!)
  - Server MUST be authenticated
  - User is not authenticated
  - Encryption is not required
  - Integrity protection is required
  - All steps should be proceeded in one session

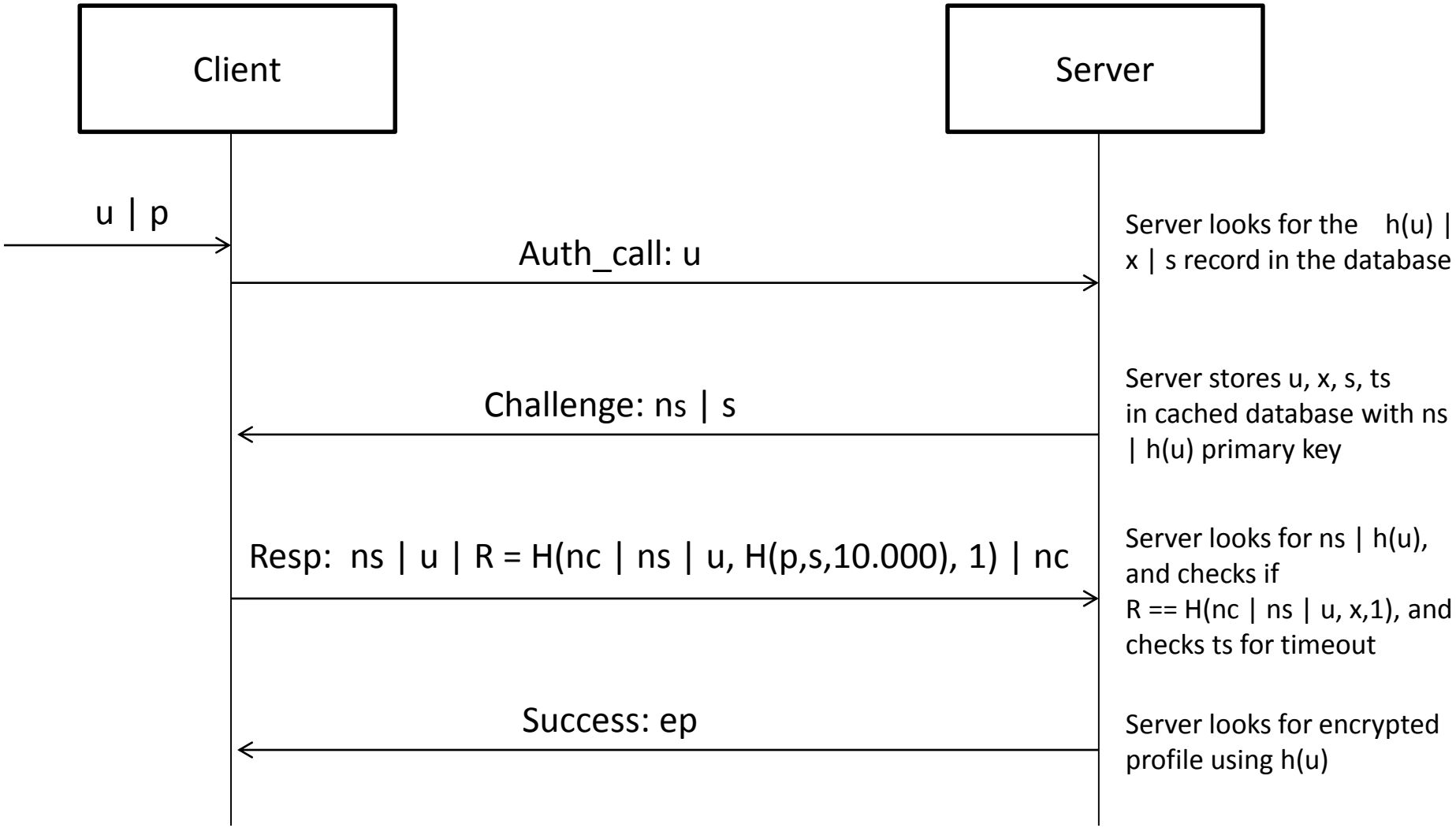
Actual setup

- All communication is over TLS
  - Server MUST be authenticated with valid certificate
  - User is not authenticated with certificate
  - Encryption is set up with AES-128
  - Integrity protection is set up
  - All steps are proceeded in one session

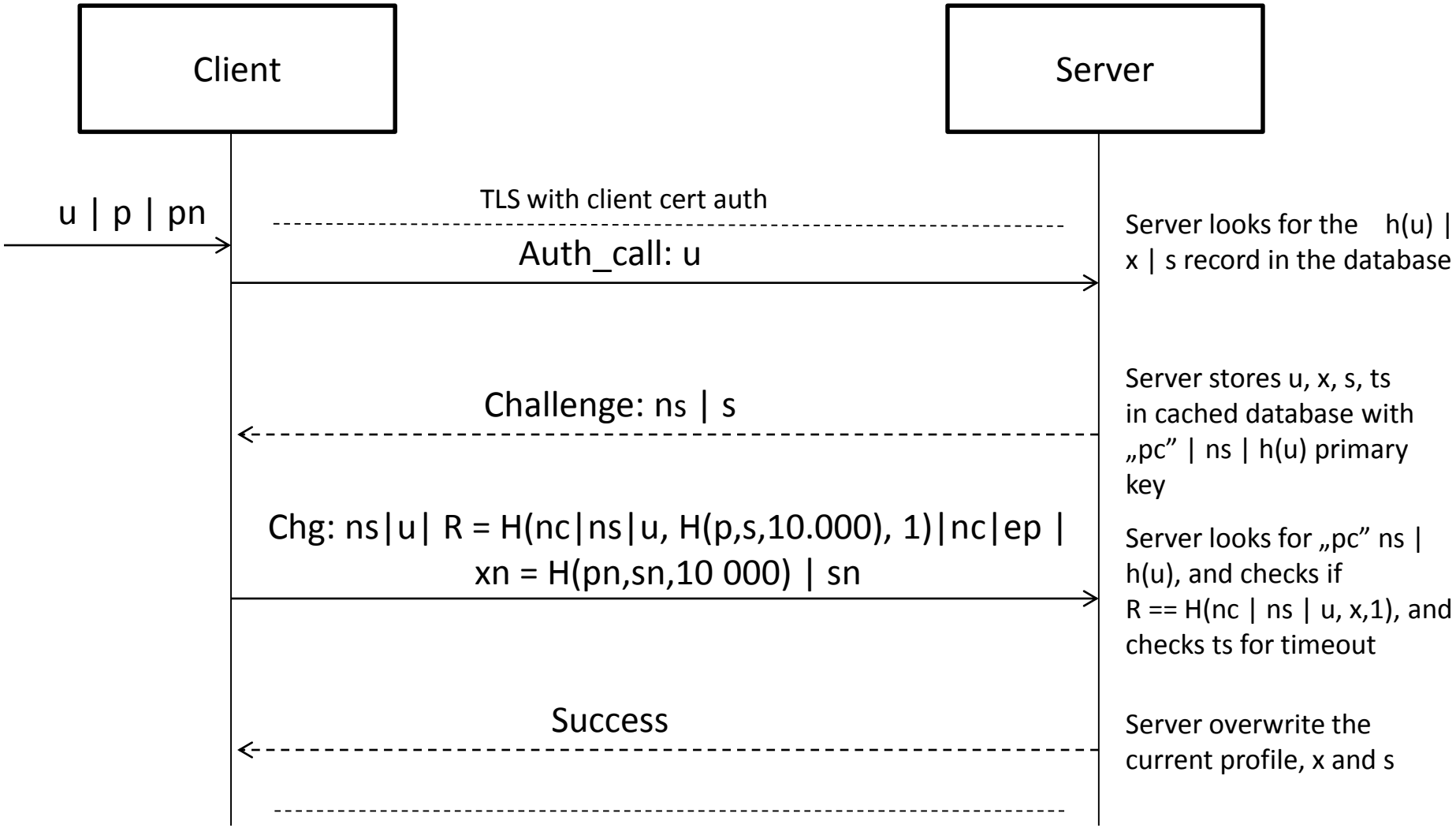
Registration



Authentication



Password change with Device Cert



Password change with User Cert