Practical case

Context:

A company is developing a new authentication protocol. The company cryptographers have been investigating alternatives to password hashing and have found that Zero-Knowledge Proof (ZKP) is a viable alternative to hashing in an authentication schema. Moreover, the cryptographers have found a ZKP protocol suitable for this purpose. As part of an agile team, you have accepted the challenge of implementing the ZKP Protocol and a Proof-of-Concept application that utilizes the protocol to register and authenticate users.

The ZKP Protocol

The ZKP protocol is described in the book "Cryptography: An Introduction (3rd Edition) Nigel Smart" page 377 section "3. Sigma Protocols" subsection "3.2. Chaum–Pedersen Protocol." We want to adapt this protocol to support 1-factor authentication, that is, the exact matching of a number (registration password) stored during registration and another number (login password) generated during the login process. We now describe the registration and the login processes.

Registration Process

The prover (client) has a secret password *x* (i.e. it is a number) and wishes to register it with the verifier (server). To do that, they calculate y1 and y2 using public g and h and the secret x and sends to the verifier y1, y2.

Login Process

The login process is done following the ZKP Protocol shown in the diagram. Been the Prover the authenticating party and the Verifier the server running the authentication check: