0.0.1 Client-side

Om onze wachtwoorden veilig op te slaan maken we gebruik van het volgende algoritme.

0.0.2 Client-side

Langs de client-side hebben we de username U en het wachtwoord P. We concateneren dit tot $S = U||P$, dit is de client-side salt. Het wachtwoord gaat samen met de salt S en scrypt iteratief beveiligen. Scrypt is het equiv van bcrypt maar is een memory hard algoritme. De output daarvan noemen we Sc word samen met de username doorgestuurd naar de server.

0.0.3 Server-side

De server ontvangt het paar (Sc, U). De server maakt een random salt aan die, samen met Sc wordt gebruikt om een encryptie key te maken voor de user zijn sequence key en zijn persoonlijke informatie op te slaan. We noemen deze salt $Salt_1$. $DK = PBKDF2(PRF, Sc, Salt_1, c, 256)$. Nu maken we een random sequence key aan te zal worden gebruikt om onze OTP mee aan te sturen, we noemen dit de OTP-sessie key. We slaan Sc, OTP-sessie key en een couter op in de databank geencrypteerd met het AES-cijfer met als input key DK.