
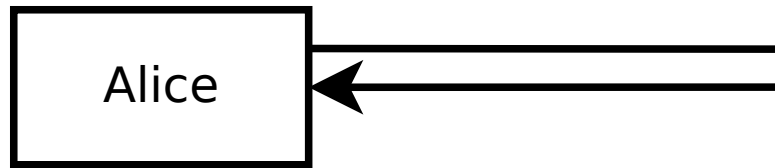


Registeren

PBKDF2(wachtwoord),andere informatie

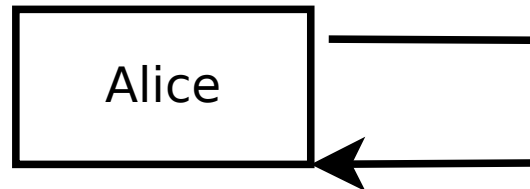
- 
1. Aanmaken shared secret.
 2. Aanmaken ID.

1
2



Inloggen

1. Ingeven van ID en wachtwoord
2. $\text{PBKDF2}(\text{wachtwoord})$.



3. Foto maken van QR-code
4. $\text{response} = \text{TOTP}(\text{shared secret}, \text{challenge XOR})$

Transactie uitvoeren

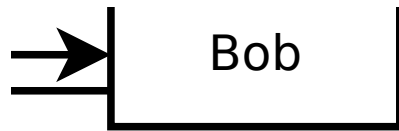
Terug sturen van shared secret en ID.
Shared secret in de vorm van QR-code.
ID in een pdf.

PBKDF(wachtwoord),ID

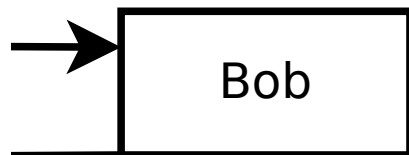
QR-code met 8 random bytes (challenge).

R UT)

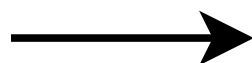
8 digit response



3. $pw = \text{bcrypt}(\text{PBKDF2}(\text{wachtwoord}, \text{salt}))$
4. $Ess = E(\text{PBKDF2}(\text{wachtwoord}, \text{salt}))$
5. Oplaan in databank:
pw, Ess, andere informatie.



1. $b = \text{bcrypt}(\text{PBKDF2}(\text{wachtwoord}, \text{salt}))$
2. $b' = \text{wachtwoord in databank}$
3. controleren of $b=b'$.
4. decrypteren van shared secret
5. 8 random bytes maken en ϵ



1. Bereken T1 en T2
(de unix time).
2. Bereken response R1 en R2
 $R1 = \text{TOTP}(\text{shared secret}, \text{challenge})$
 $R2 = \text{TOTP}(\text{shared secret}, \text{challenge})$
3. Controleren response.