Protecting medical data

with passwordless authentication

Carl Svensson, KRY/LIVI @ PasswordsCon 2018

Biography

- MSc in Computer Science, KTH
- Head of Security, KRY/LIVI
- CTF: HackingForSoju
- E-mail (private): calle.svensson@zeta-two.com
- E-mail (work): carl@kry.se
- Twitter: @zetatwo

Agenda

1. KRY/LIVI, Background
2. Authentication so far
3. Expanding to other countries
4. Design process
5. Our solution
6. Results: 6 months in

Disclaimers, this talk:

- About constraints
- About business
- About process
- Not about technology

KRY/LIVI, Healthcare online

- Online healthcare provider
- Healthcare data
- Possibly the most sensitive

- "Patient first", UX/UI important

- 500 000+ users
- 3% of primary care in Sweden

Authentication in Sweden

- BankID, digital identity
- Issued and validated by banks
- Private but used in public
- Well-established

Authentication in Norway

- Pretty much the same as Sweden

Expanding to Europe

- In UK, no personal ID number
- In France, typically no ID at doctor

- "Passwords suck" - Our CEO
- "We are launching in 3 months" - Also our CEO

Problem statement

- Challenges
  - Authenticate without passwords
  - No digital ID available
  - User friendly
  - User friendly
  - User friendly
  - Secure
- Consolation
  - Users are valuable

Understand the data model

- A person is not a phone
- People have kids
- Device (1-*) User (*-*) Patient

Understanding the scenarios

- New device
  - Access to old
  - No access to old
- Old device
  - Reinstall
- Strong authentication
  - Onfido
- Empty account?
  - Allow weak authentciation
- Revokation?

Public key challenge-reponse with tiered identity

- Registration
  - Create a device
  - If no user, create
  - If user is patient: Onfido
- First medical interaction
  - Create patient
  - Link user to patient
- On create patient
  - Onfido verification
- Multiple devices per patient
  - Register new user
  - Link users

Results: Pros

- No password!
- (mostly) Seamless
- (pretty) User friendly
- (fairly) Secure

Results: Cons

- Breaks conventional mental model
- Overloads words
- Revokation not fast enough

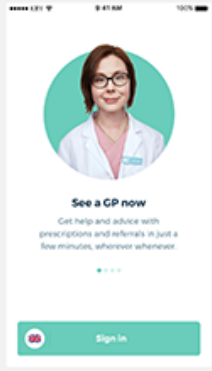
Evaluation: How did it go?

- Users are registering
- Users are staying
- No known incidents
- Iterative process

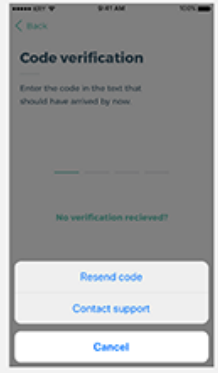
Thank you for listening!

Questions?

User Signup

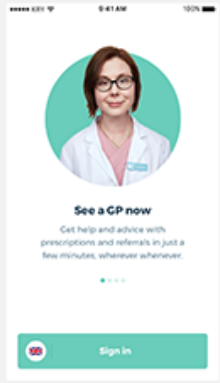


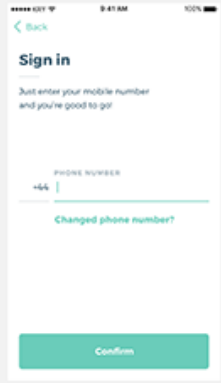
If passcode does not arrive in 1 minute.



User

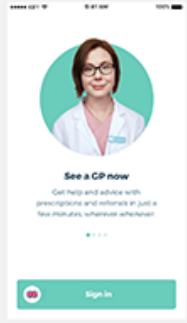
Unlock: New phone/app



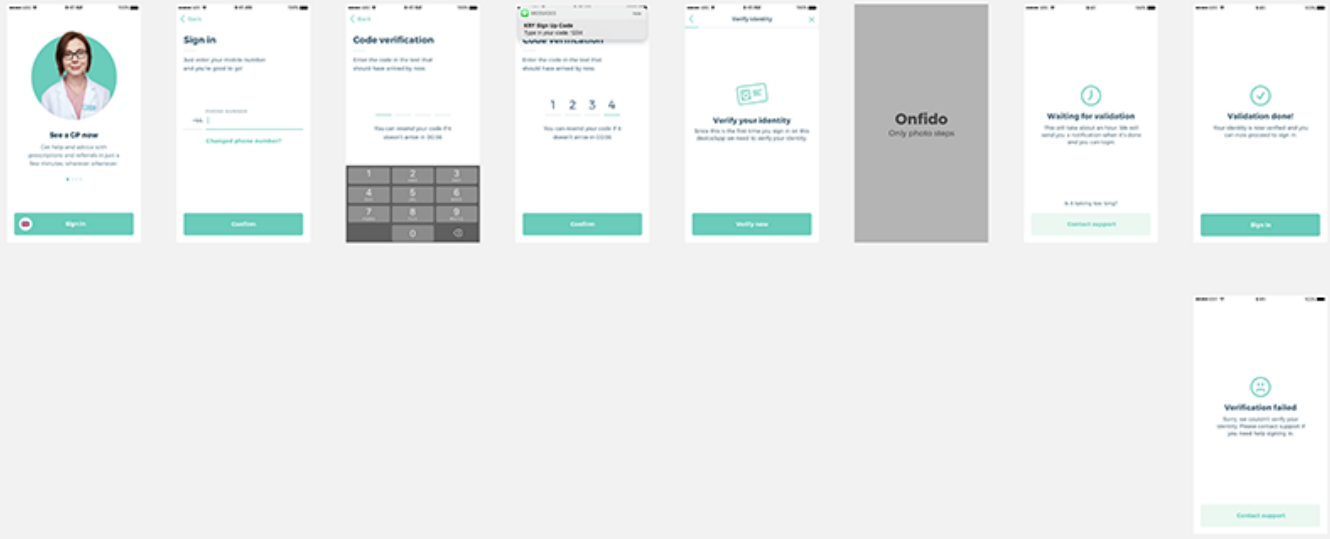


Patient

Login: New phone number, new phone/app



Patient
Login: New phone/app



Patient

Unlock

Passcode/TouchID