Autentifikation uden kodeord

- for mennesker til en webtjeneste

Mere information

- https://authenticatecon.com/agenda/
- https://www.youtube.com/c/TheFIDOAlliance/videos
- https://fidoalliance.org

Hvem er vi?

- Mads Freek, systemudvikler WAYF
- Kasper Sort, systemudvikler DeiC
- Sammen arbejder vi på sikker login
  - 2-faktor
  - Uden kodeord

Hovedbudskab

- Det er ikke svært - for brugerene
- Det er sikkert nok - på en anden måde

Program

- Kort indledning
- Kort demo
- Lidt længere indledning
- Hvad er autentifikation?
- Hvad er faktorerne?
- Demo FIDO2
- Demo TIQR
- Q + evt. A

DEMO

https://webauthn.dgw.deic.dk

Hvad er autentifikation?

- Autentifikation er en del af autorisationen når man skal bruge et system, blandt andre informationer
  - Hvem eller måske rettere hvad er du ..
  - tid på dagen
  - størrelse af beløb
  - …
- Autentifikation er genkendelse af en digital identitet

Digital Identitet (NIST Special Publication 800-63-3)

- Identitets verifikation (IAL 1 - 3)
- Autentifikations verifikation (AAL 1 - 3)
- Føderation (FAL 1- 3)

https://pages.nist.gov/800-63-FAQ/

Autentifikation - faktorerne

- noget man ved - kodeord / pinkode
- noget man har - en dims / en telefon / en pc
- noget man er - et fingeraftryk / ansigts / iris - biometri

Autentifikations midler

- Memorized Secret (Section 5.1.1)
- Look-Up Secret (Section 5.1.2)
- Out-of-Band Devices (Section 5.1.3)
- Single-Factor One-Time Password (OTP) Device (Section 5.1.4)
- Multi-Factor OTP Device (Section 5.1.5)
- Single-Factor Cryptographic Software (Section 5.1.6)
- Single-Factor Cryptographic Device (Section 5.1.7)
- Multi-Factor Cryptographic Software (Section 5.1.8)
- Multi-Factor Cryptographic Device (Section 5.1.9)

	PW	FIDO
Glemt PW	–	√
Genbrug	–	√
Nyt PW	–	√
Phishing	–	√
PW DB kompromittering	–	√
keyloggers/sniffers	–	√
Social engineering	–	–

DeiC's Last Resort Identity Provider (IdP)

- DeiCs Last Resort IdP, gæste IdP
  - Ingen vil tage det samlede ansvar for gæstebrugere
- IdP til brugere uden IdP
- Sikkert login (AAL 2,3 ie. betydelig eller høj, multifaktor)
- Ingen identitets informationer på brugeren, kun credentials på brugeren
- LRIdP'en er kun til autentifikation, al identitets verifikation er overladt til tjenesterne
- Brugeren identificeres ud fra et brugernavn genereret af LRIdP
  - Ikke muligt at bruge e-mail som brugernavn :-(

To metoder

- Webauthn / FIDO2

- tiqr

FIDO2/Webauthn (W3C)

- FIDO1 + pinkode eller biometri
- Sikkerhed i besiddelse + memorized secret / biometri
- offentlige nøgler (public keys) i databasen
- (vi har genereret brugernavnet)
- W3C og de store browsere standard (næsten)
- https://wayfsp.wayf.dk

https://webauthn.io/

tiqr

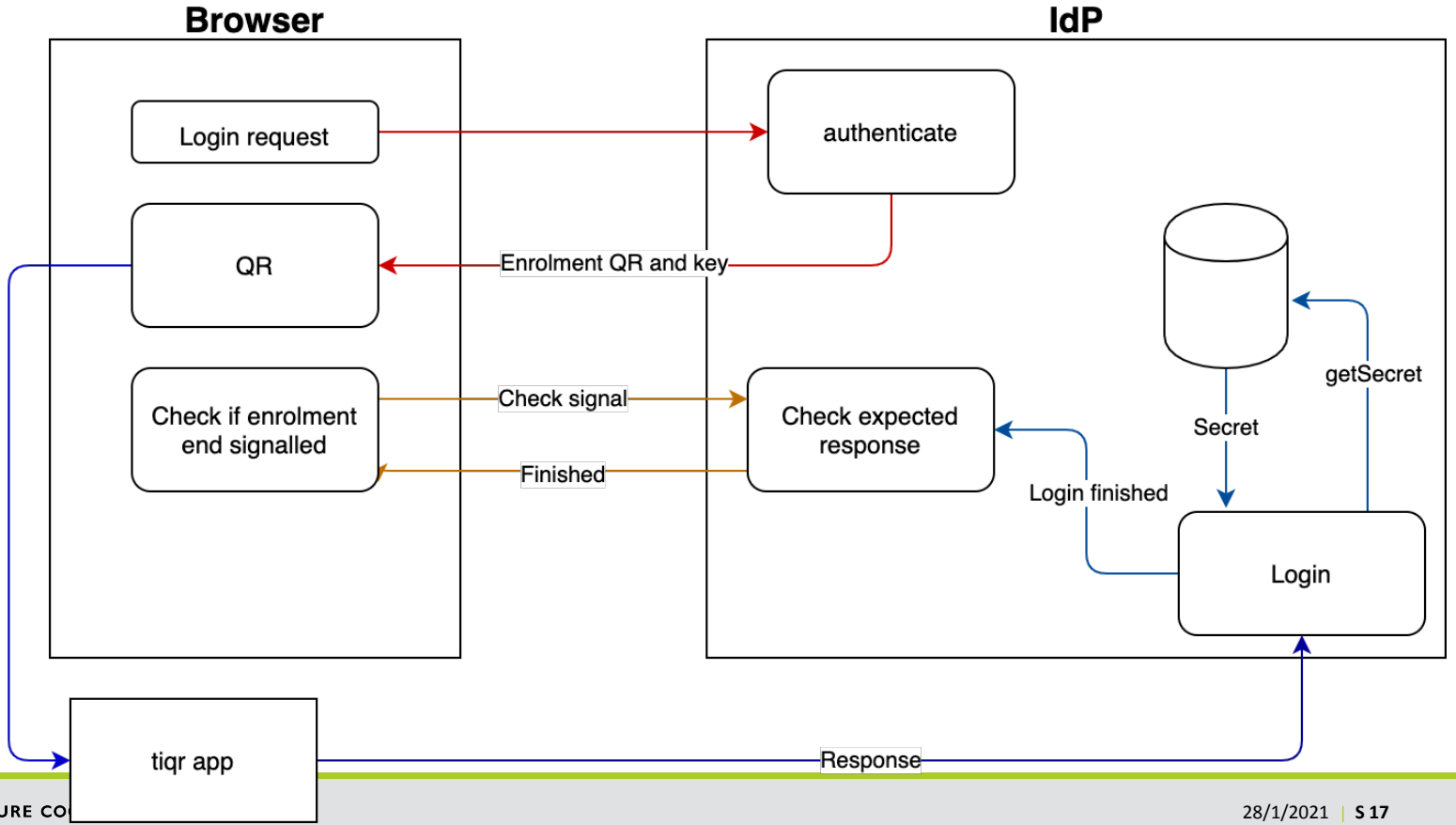
- Fra den hollandske DeiC ækvivalent surf.nl
- Bygger på:
  - OATH Open Authentication Initiative
  - OCRA protocol (OATH Challenge-Response Algorithm)
- QR kode i stedet for en kode brugeren selv skal indtaste
- challenge/response authentication
- https://wayfsp.wayf.dk

https://tiqr.org/

Til sidst

- Vi har ingen registrering med, men vi kan vise det til sidst
- Man kan registrere flere nøgler og både tiqr og FIDO2 nøgle
- Account linking med brugernavn

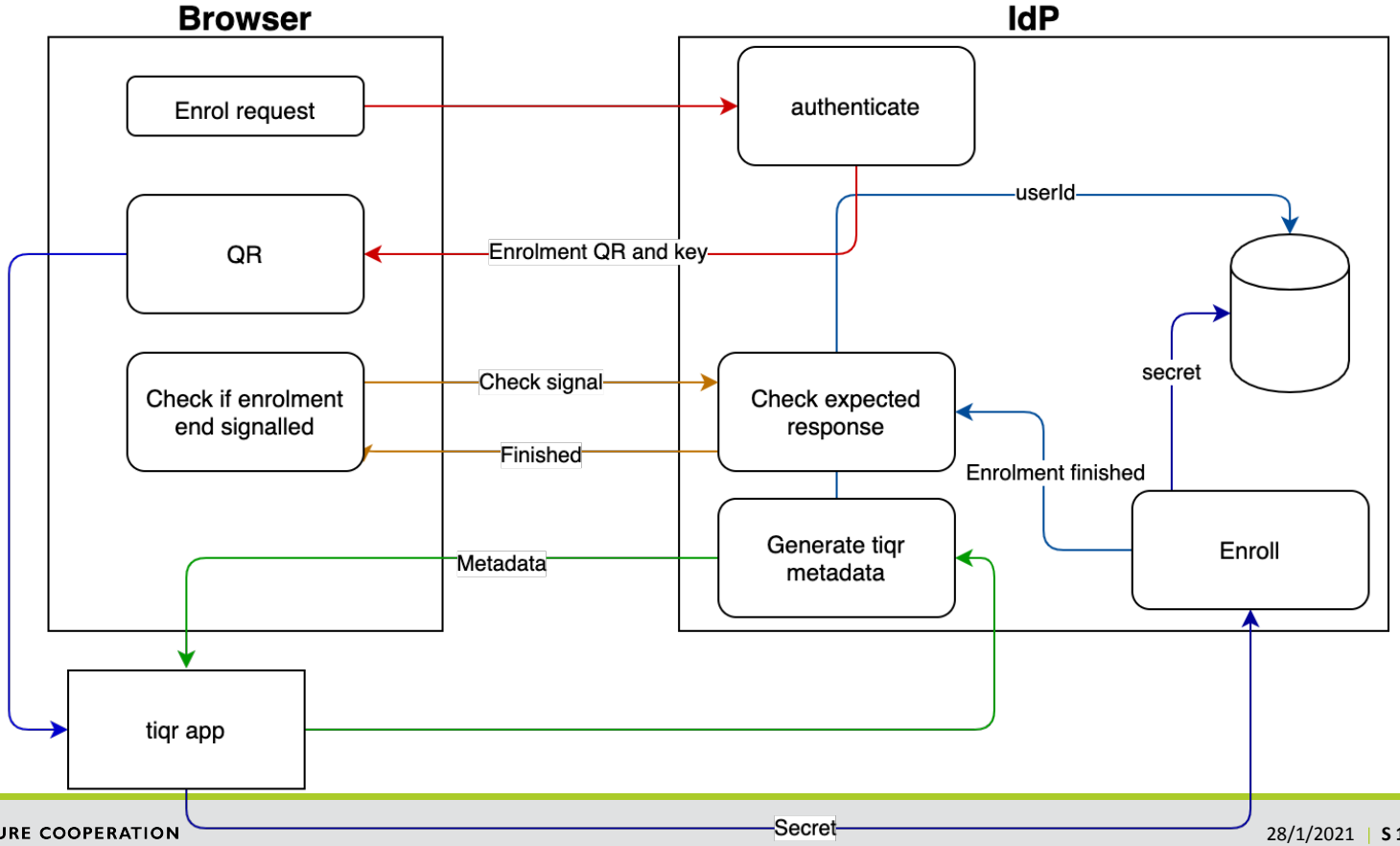
tiqr login


Browser
IdP
Login request
authenticate
QR
Enrolment QR and key
Check if enrolment end signalled
Check signal
Finished
Check expected response
getSecret
Secret
Login finished
Login
tiqr app
Response

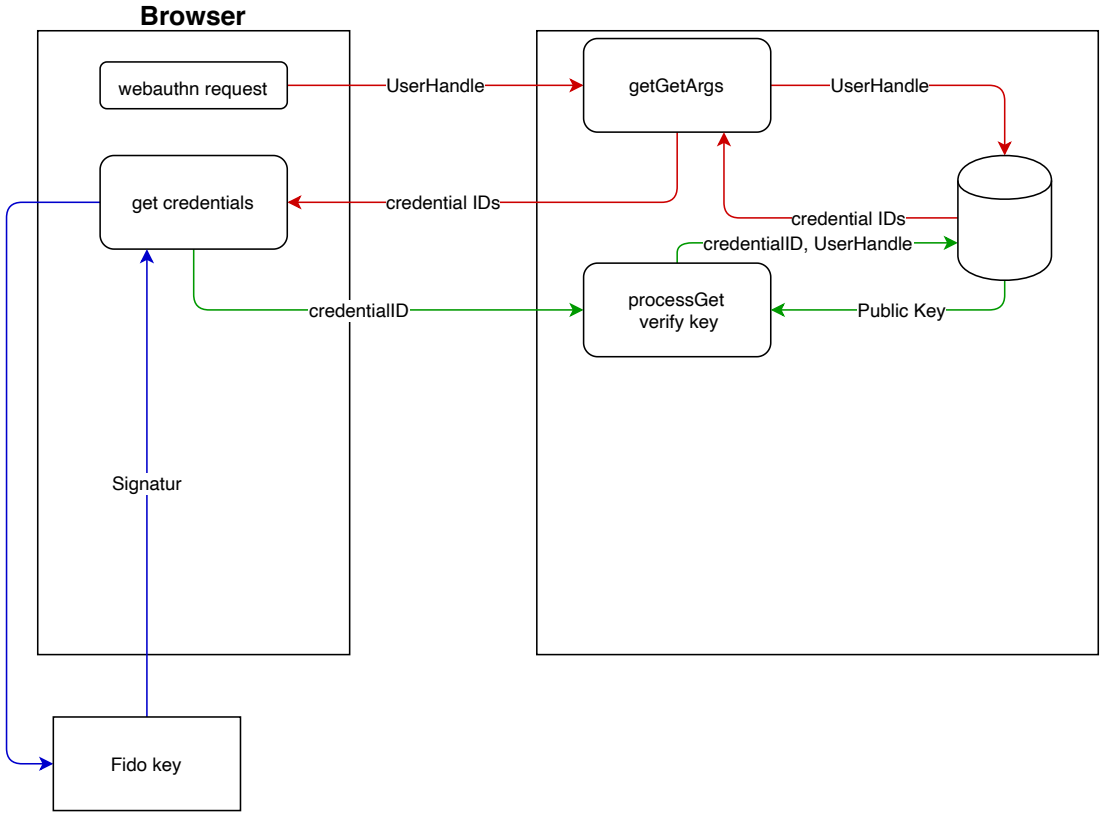
User

Server

tiqr enrol



Teknisk del


Browser
webauthn request
UserHandle
getGetArgs
UserHandle
get credentials
credential IDs
credential IDs
credentialID, UserHandle
credentialID
processGet
verify key
Public Key
Signatur
Fido key