



# “State of the IRMA”

Nieuwe en komende IRMA ontwikkelingen

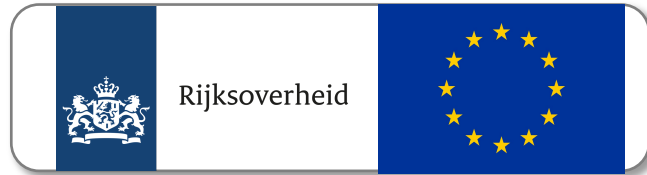
5 november 2021

Martijn Sanders, Product Owner IRMA

Sietse Ringers, Architect IRMA



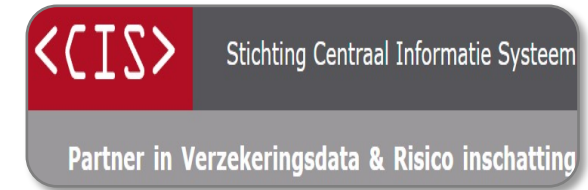
# Wat is er bereikt



Lobby gedachtengoed



Parkeerbewijzen met IRMA



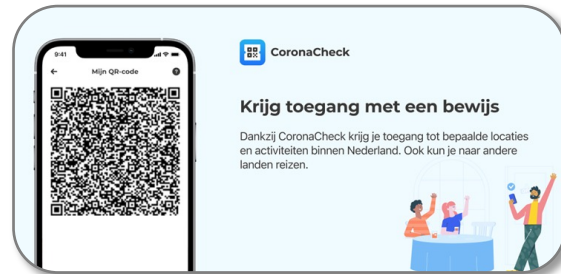
Openheid data CIS



Schaalbare infrastructuur



Lancering IRMAconnect



IRMA crypto core in CoronaCheck app



Data & Algoritme marktplaats



# Focus 2021-2022

- ISO 27001
- eIDAS & WDO
- Rol en toepassing IRMA
- Gebruikerservaring
- Verbeteren infrastructuur
- Marketing & communicatie



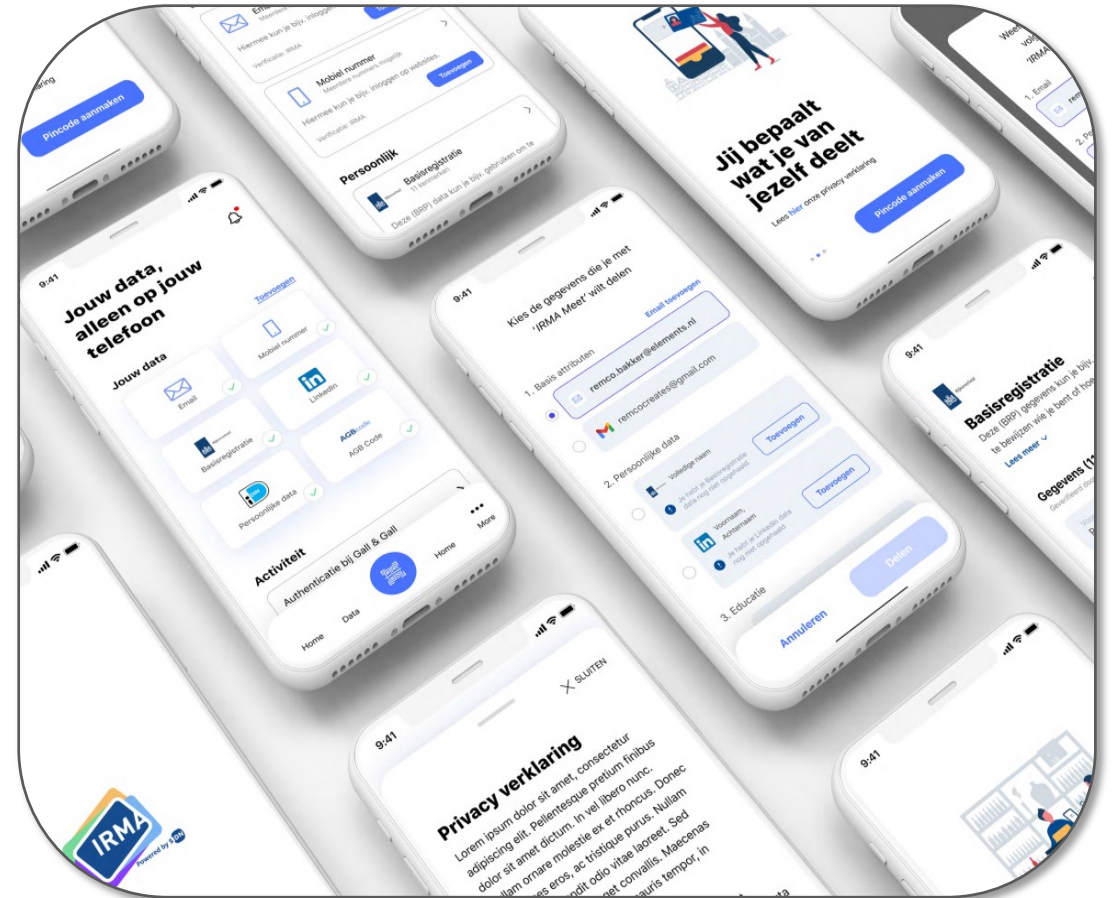
Binnen SIDN 15 mensen direct betrokken bij IRMA



# IRMA mobile UX 2.0

- Verbeteren klantervaring
- Nieuwe look & feel
- Kaartjes vs. attribute based
- Toegankelijkheidseisen (WDO)
- Nieuwe features
  - Secure PIN
  - Landscape mode

Target 01-07-2022, verdere communicatie volgt



# eIDAS

- Voorloper WDO
- Trustlevel Substantieel & Hoog
- Innovalor traject
- Voorwaarden
  - TPM (Trusted Platform Module)
  - Aanpassingen IRMA app
  - Issuance processen



# KVK issuer

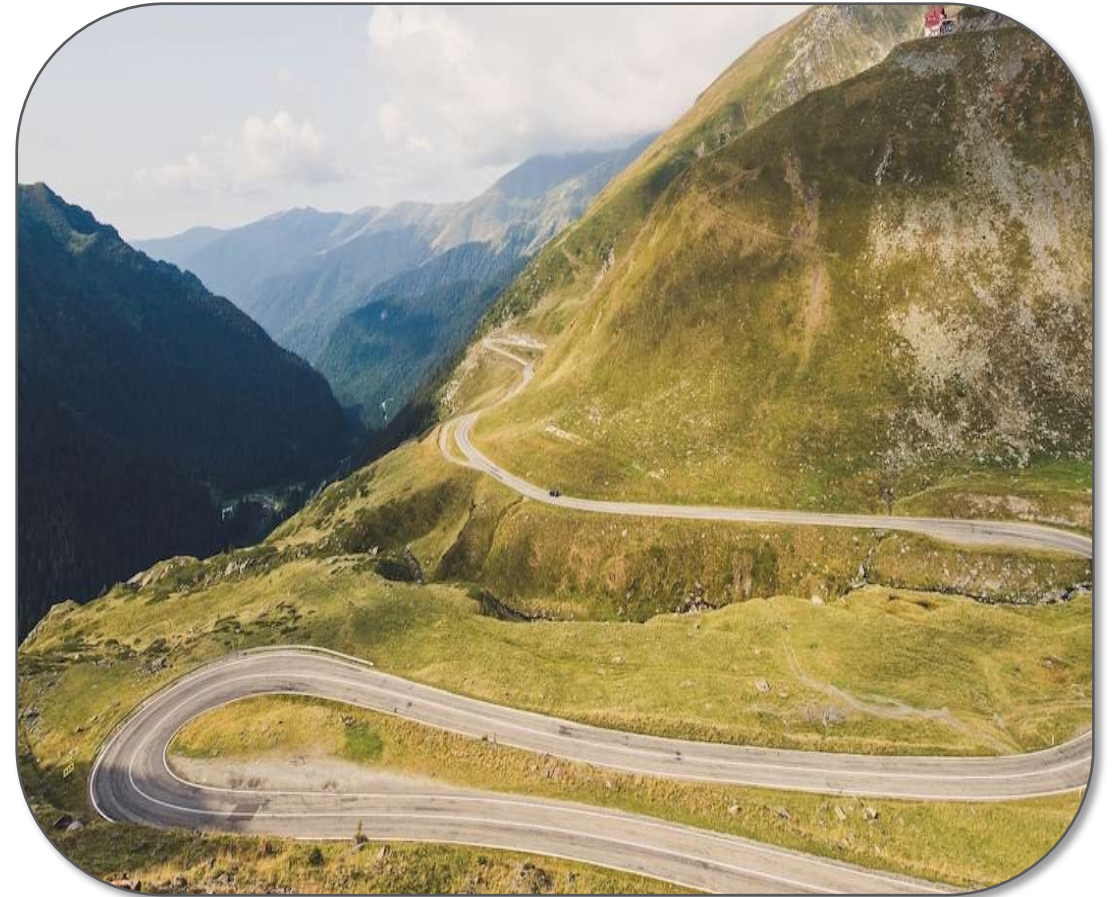
- Samenwerking met KVK
- KVK credential in app
- Inzet in OpenPlanet project
- IRMA ingang in bedrijfsleven



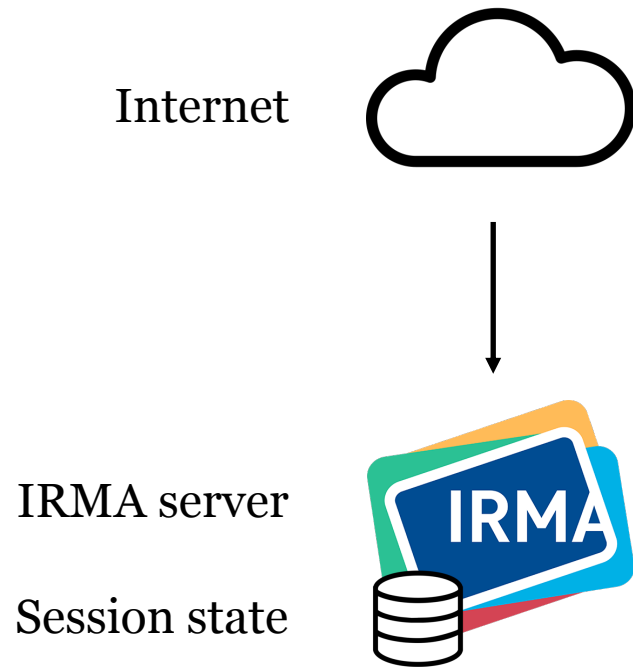
# Toekomst

Mogelijke roadmap items:

- Online backup
- Range proofs
- Cascading revocation
- Universal QR support



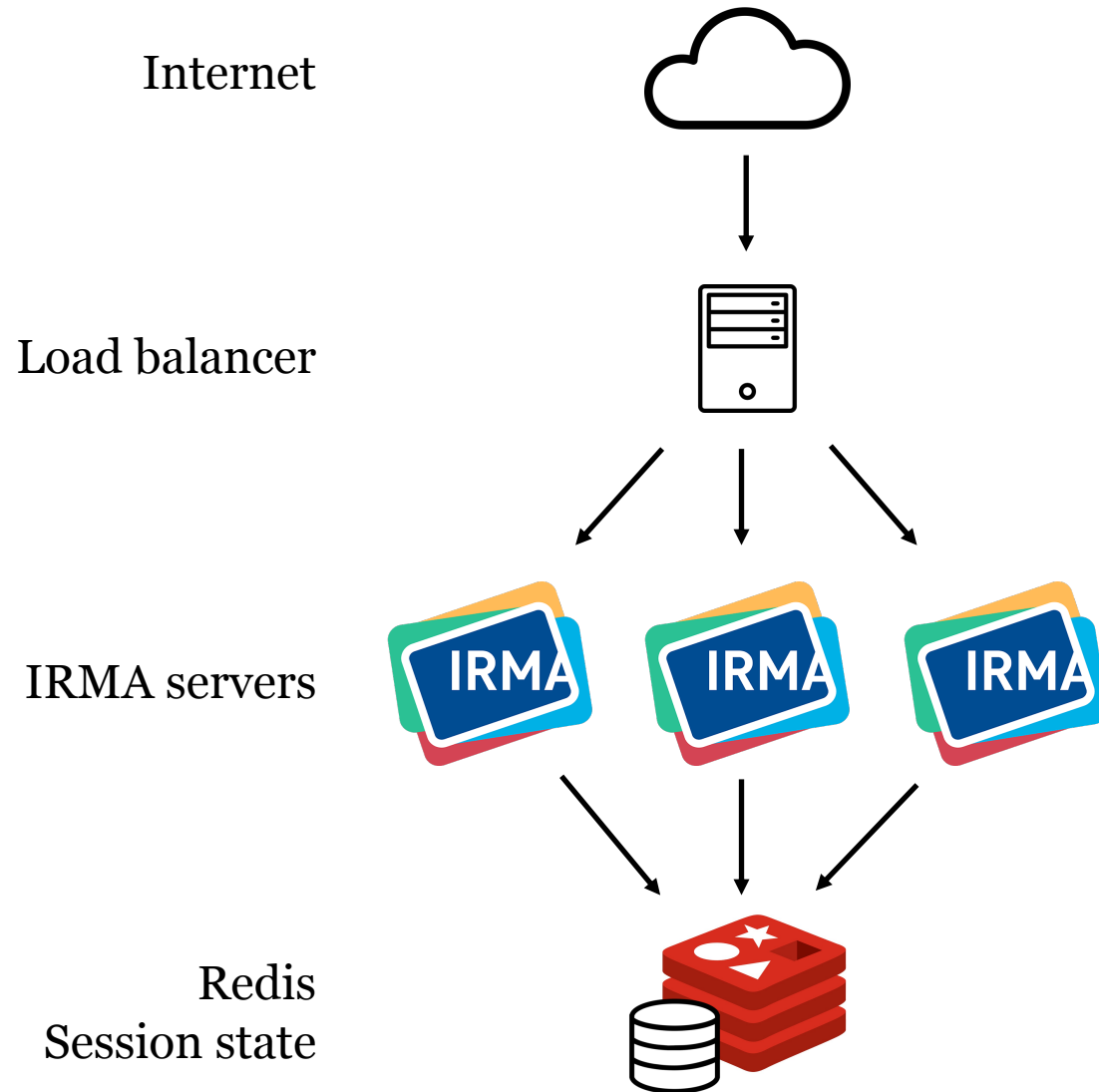
# Stateless IRMA server met Redis



- Performance-limiet: horizontaal schalen onmogelijk
- IRMA server is SPOF
- Upgraden kost downtime



# Stateless IRMA server met Redis



Vanaf v0.9.0:

```
irma server \  
  --store-type redis \  
  --redis-addr localhost:6379 \  
  --redis-pw p4ssw0rd
```

Voordelen

- IRMA servers horizontaal schalen
- Upgraden zonder downtime

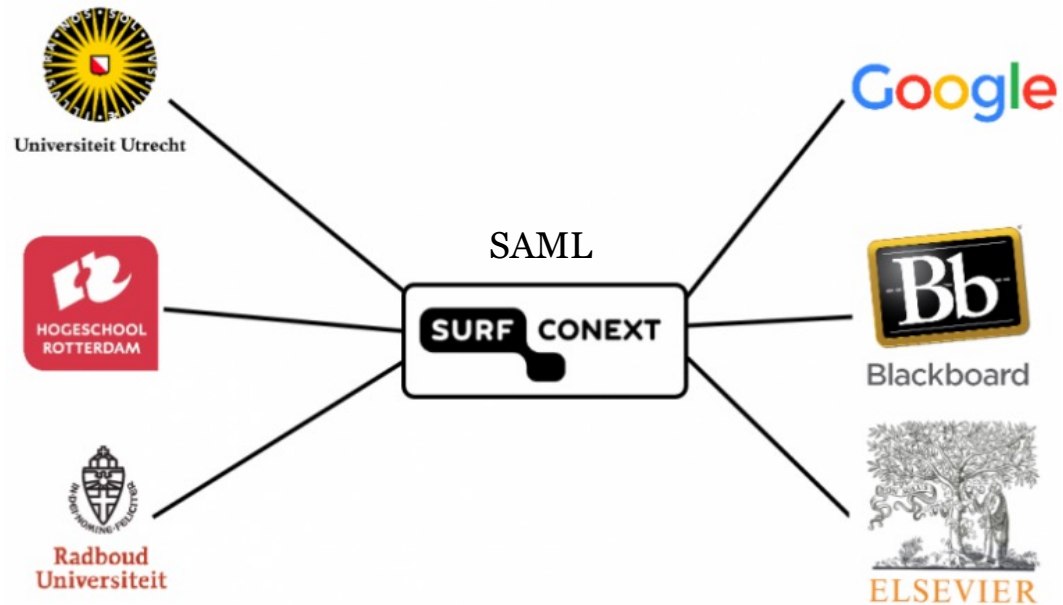
Later

- Support voor Redis clusters



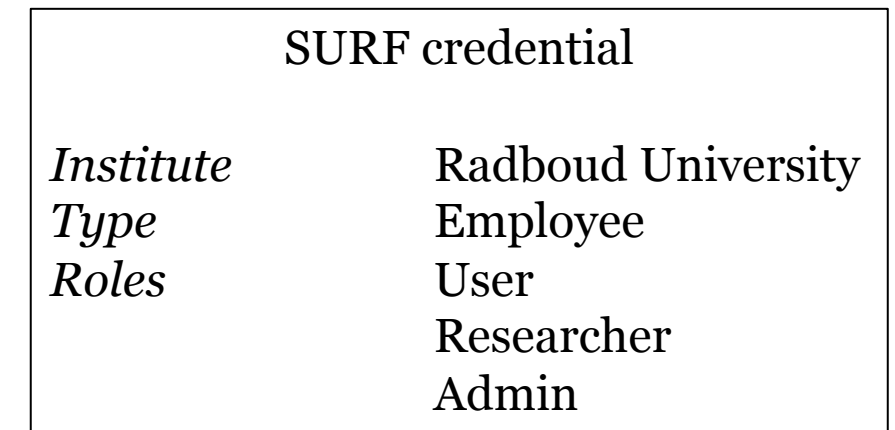
# Coming: multivalued attributen

## SURFconext



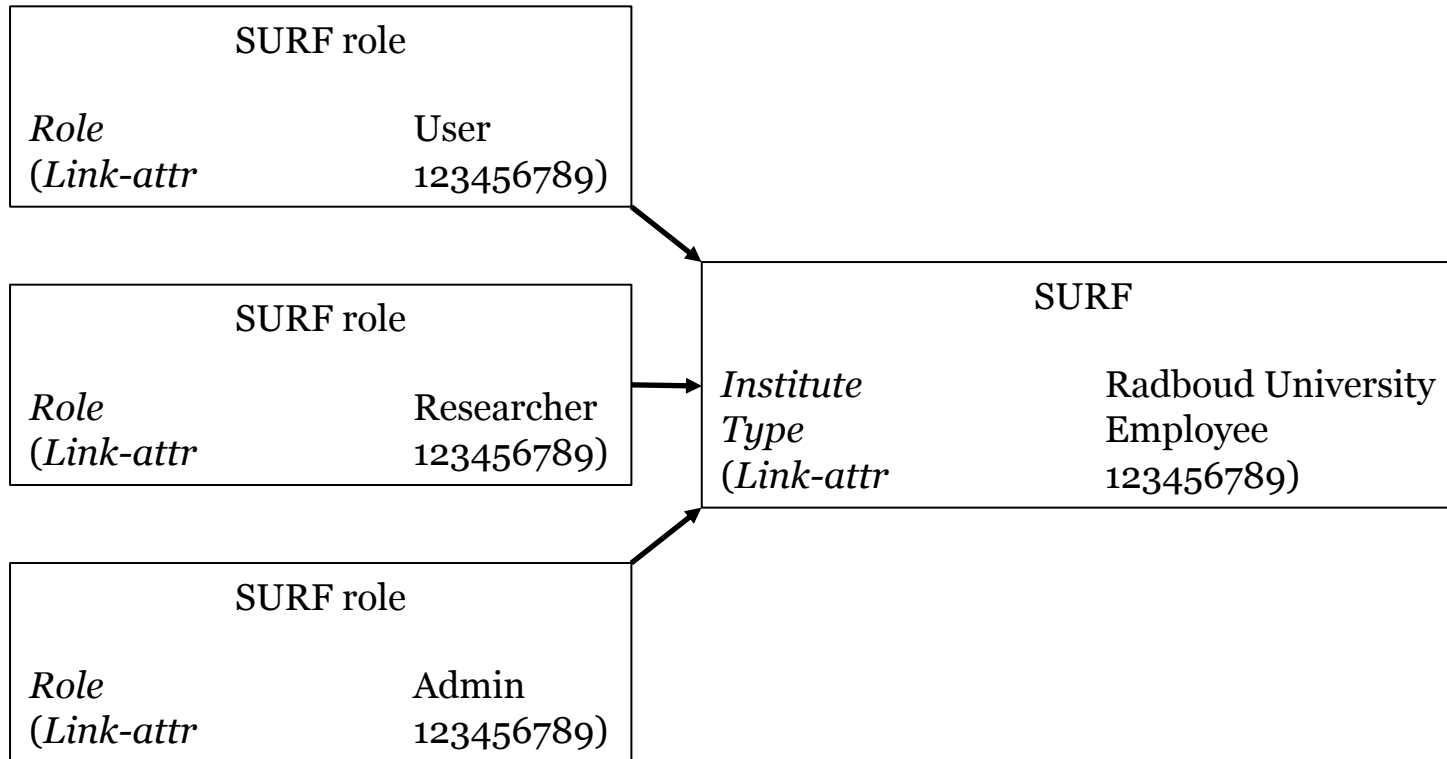
Externen?

## IRMA

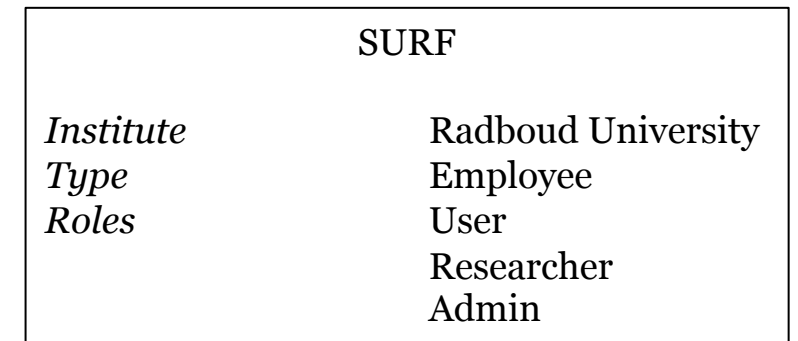


# Coming: dependent credentials

## Implementatie



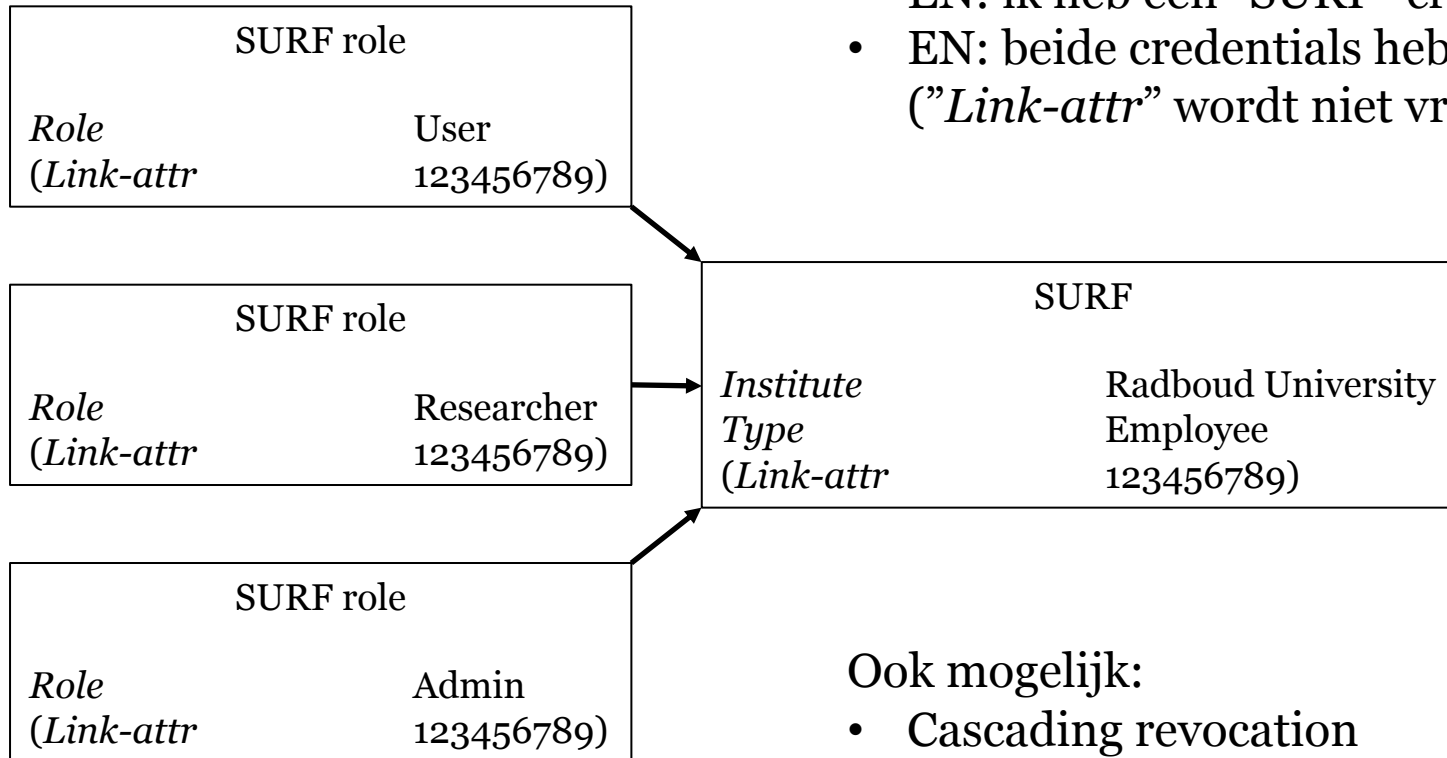
## IRMA app GUI



# Coming: dependent credentials

App bewijst in zero-knowledge:

- Ik heb een “SURF role” credential met “*Role: Researcher*”
- EN: ik heb een “SURF” credential
- EN: beide credentials hebben hetzelfde “*Link-attr*” (“*Link-attr*” wordt niet vrijgegeven)

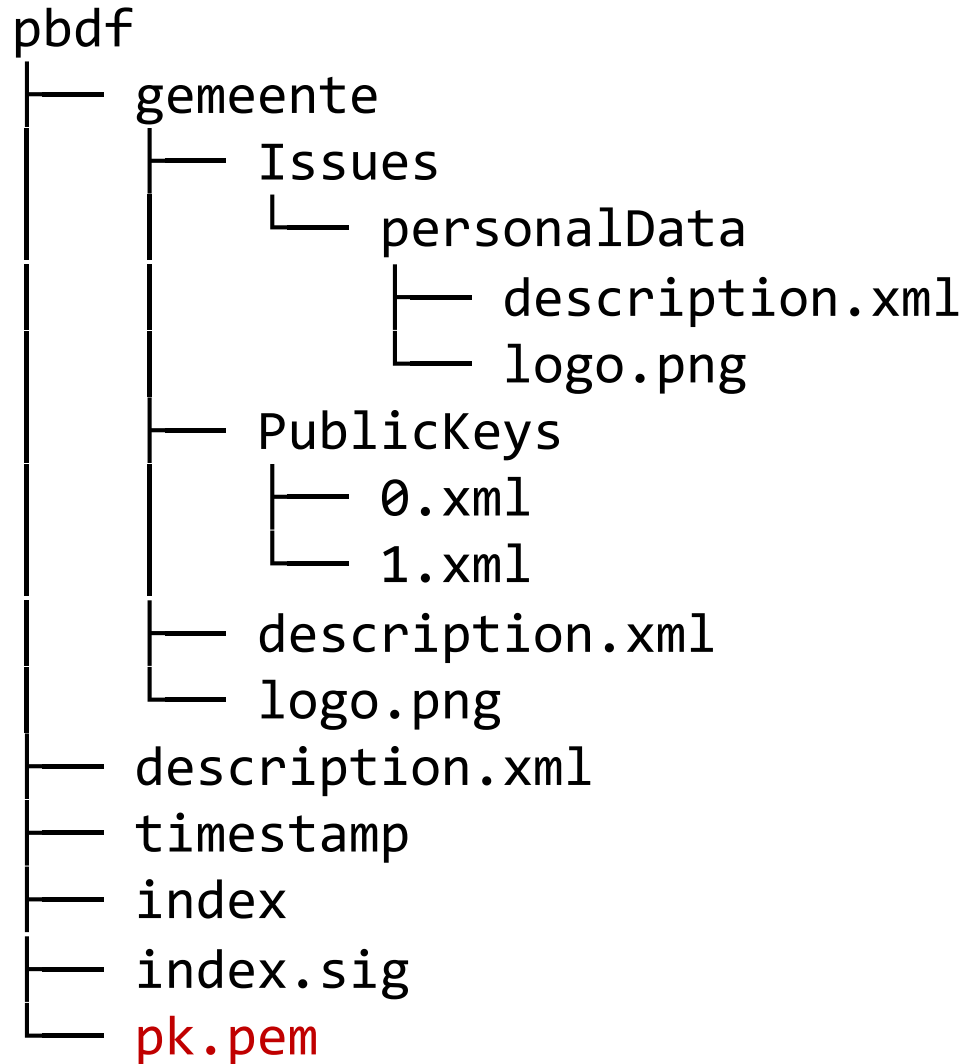


Ook mogelijk:

- Cascading revocation  
(“SURF” revoked → “SURF role” revoked)
- Splitsen van grote kaartjes  
(gemeentelijke persoonsgegevens-kaartje)



# Scheme key rollover





- IRMA apps + servers updaten vanaf online masterkopie
- pk.pem: public key tekent hele directory structuur
- Oorspronkelijke key sinds oprichting PBDF
- In ontwerp: rollover mechanisme
  - Scheme updates blijven werken, **als je IRMA server up-to-date is**
- Nieuwe private key in HSM (eIDAS)
- Verdere communicatie volgt tzt



# Huishoudelijke mededelingen

Pretty verifier en wizard zijn klaar voor gebruik

← Jezelf bekend maken

 Wil je dit aan  IRMA-meet doorgeven?

Naam  
A. J. Meijer

Leeftijd  
Ouder dan 18

Bron: Rijksoverheid

E-mail  
anouk.meijer@ziggo.nl

Bron: Stichting Privacy by design

• • • >  
3 keuzes

Nee, liever niet **Ja**

14:29

← Kaartjes ophalen



**Ivido PGO**

**Inloggen bij Ivido**

Je hebt een toegangsbewijs nodig om in te loggen bij Ivido. Hiervoor haal je jouw gegevens op in IRMA.

**Welke gegevens haal je op?** ^

Je haalt je persoonsgegevens op. Je hebt deze gegevens nodig om te laten zien wie je bent. Zo kan alleen jij inloggen op jouw account.

**Waar haal je de gegevens op?** v

**Hoe werkt het?** v

**Wat is Ivido?** v


Annuleer **Ophalen**


14:32

← Kaartjes ophalen



**Ivido PGO**

 Demo Persoonsgegevens

 **Demo Ivido Login**

Haal je toegangsbewijs op bij Ivido. Zo kun je makkelijk en veilig bij Ivido inloggen.

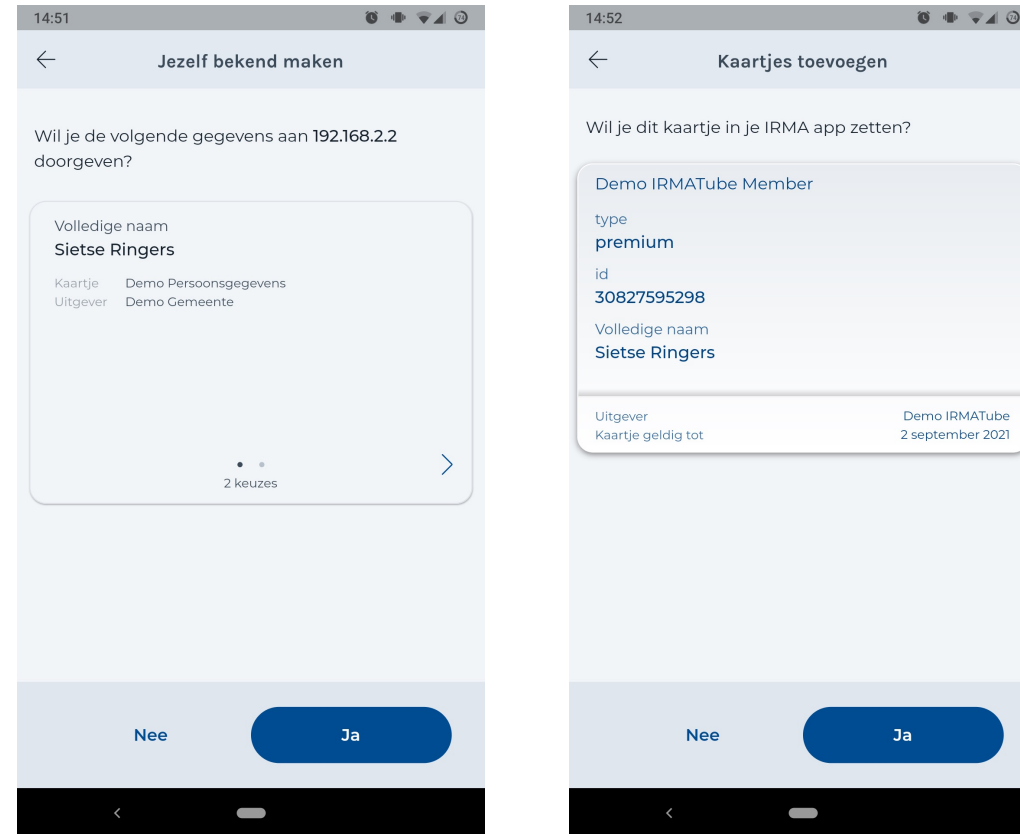
**Haal Demo Ivido Login op**

Interesse? Neem contact op!



# Huishoudelijke mededelingen

## Chained sessions: klaar voor gebruik

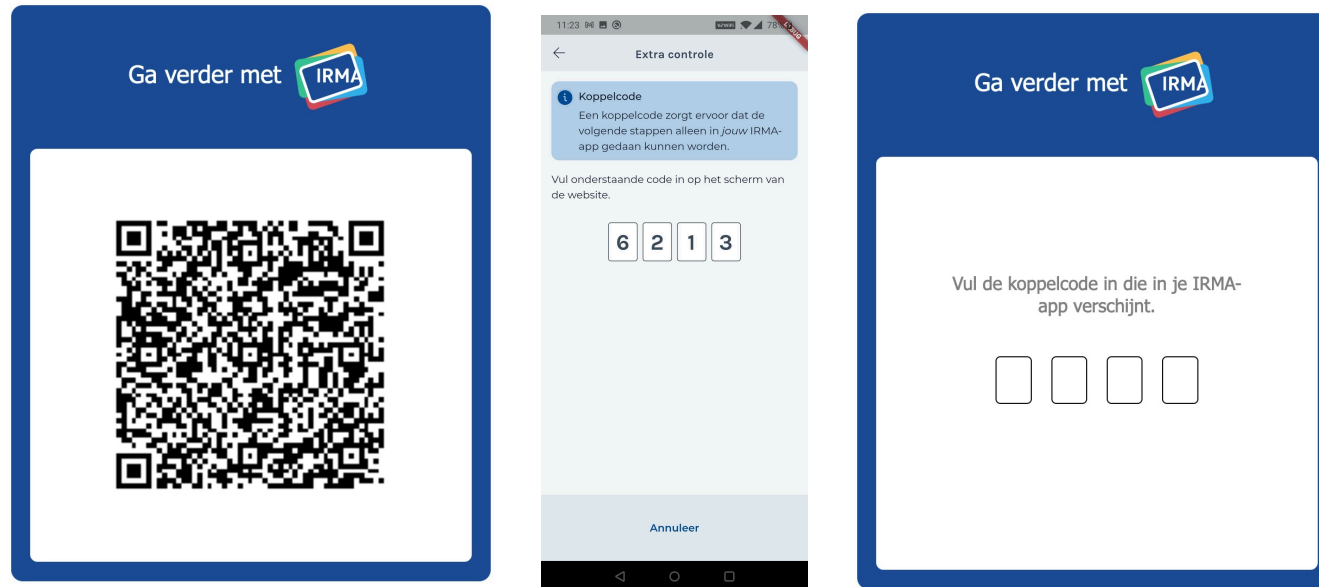


<https://irma.app/docs/chained-sessions/>



# Huishoudelijke mededelingen

- Device pairing: klaar voor gebruik → update irma-frontend



- 8 nov: SMS issuer migratie:  
pbf.pdf.mobilenumber.mobilenumber → pbf.sidn-pbf.mobilenumber.mobilenumber
- Bob Kronenburg tijdelijk uit roulatie





# Meer informatie

- Website  
<https://irma.app>  
<https://privacybydesign.foundation>
- Broncode  
<https://github.com/privacybydesign>
- Technische documentatie  
<https://irma.app/docs>
- Attribuut-index  
<https://privacybydesign.foundation/attribute-index/nl/>
- IRMA Slack

- Twitter  
[https://twitter.com/irma\\_privacy](https://twitter.com/irma_privacy)

