

“State of the IRMA”

Nieuwe en komende IRMA ontwikkelingen

Sietse Ringers | IRMA meeting

5 maart 2021



Agenda

- Online verkiezingen met randomblind attributen
- Pretty verifier names
- Issuance wizards
- Chained sessions
- QR diefstal bescherming

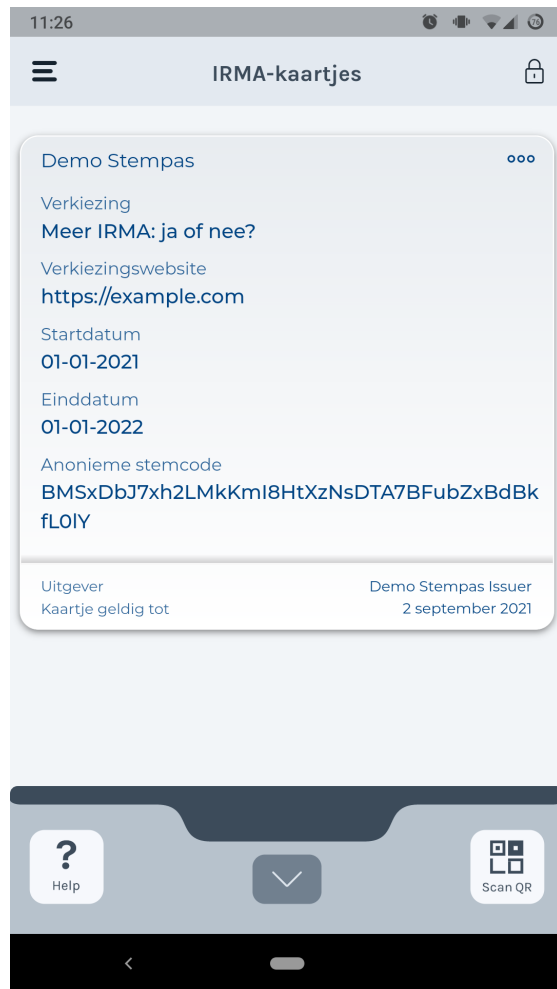


Overgang naar SIDN

- Ivar, Sietse verhuisd naar SIDN in nieuw IRMA team
- Nieuwe teamleden:
 - Maja Reißner (programmeur)
 - Kia Esmailykia (tester)
 - Dick ten Haaft (technisch applicatiebeheer)
 - Martijn Sanders (PO)
 - Esau Boen (scrummaster)
- Meer ontwikkelcapaciteit
- ISO27001
- Meer focus op testen & stabiliteit



Online verkiezingen met randomblind attributen





- Attribuut wordt als “randomblind” gemarkeerd in scheme
- Waardes zijn willekeurig en onzichtbaar voor issuer
- Stem use case:
 1. Issue stempas aan user met stemcode: randomblind attribuut
 2. User brengt stem uit met attribuut-gebaseerde handtekening:
 - Stem: “Ja, meer IRMA!”
 - Stemcode: BMSxDb...
- Dubbel stemmen detecteerbaar dmv stemcode
- Issuer van stempas ziet niet wat je stemt
- Documentatie: <https://irma.app/docs/randomblind/>



Pretty verificer names

← 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 >

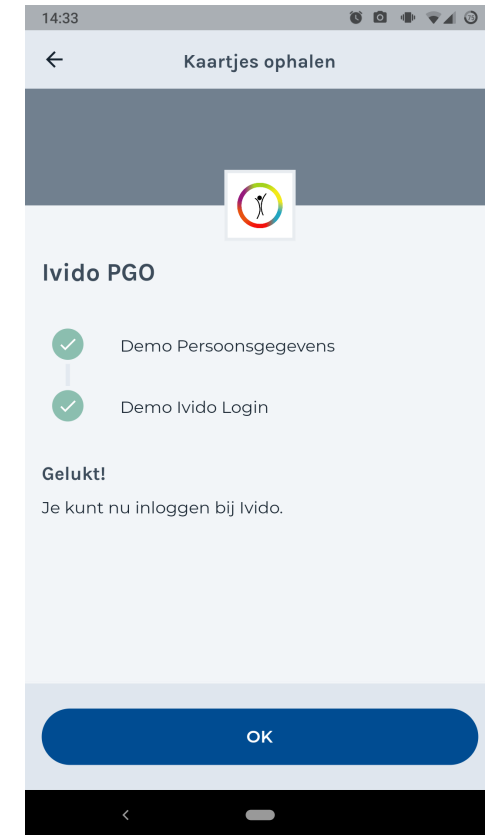
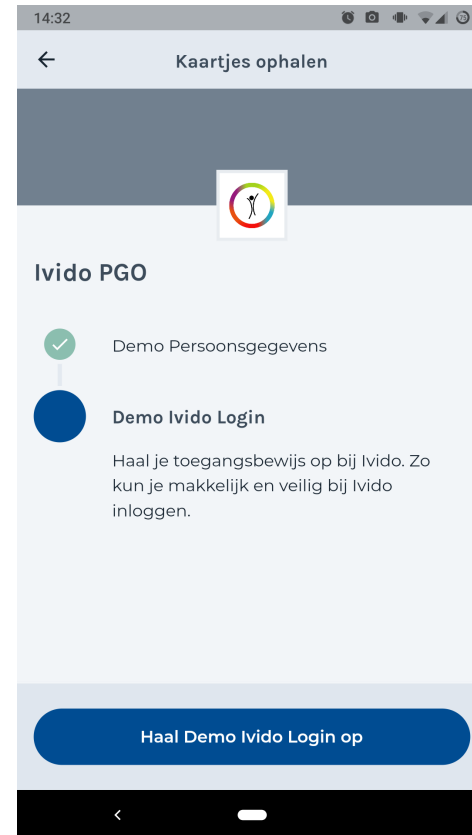
Nee, liever niet

- Domeinnaam → naam (+ logo)
irma-meet.nl → IRMA-meet
- Human-readable en vertaalbaar
- Controle vooralsnog handmatig
- Geregistreerd door PBDF
- (Op termijn) aan te vragen bij Bob Kronenburg
bob.kronenburg@sidn.nl

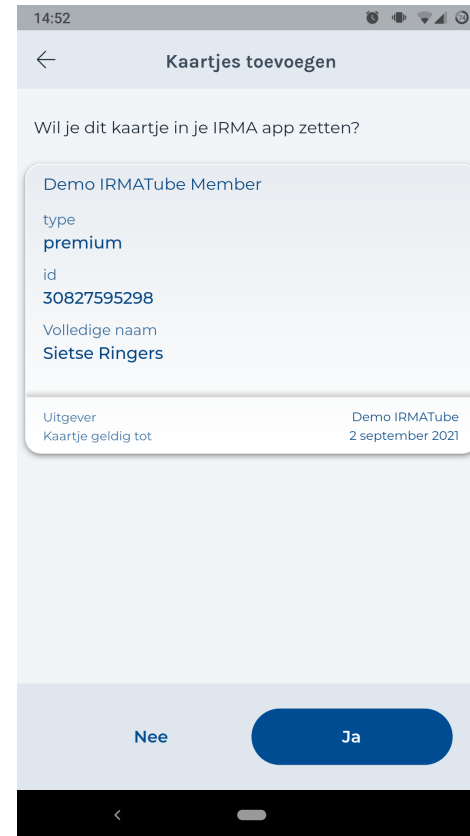
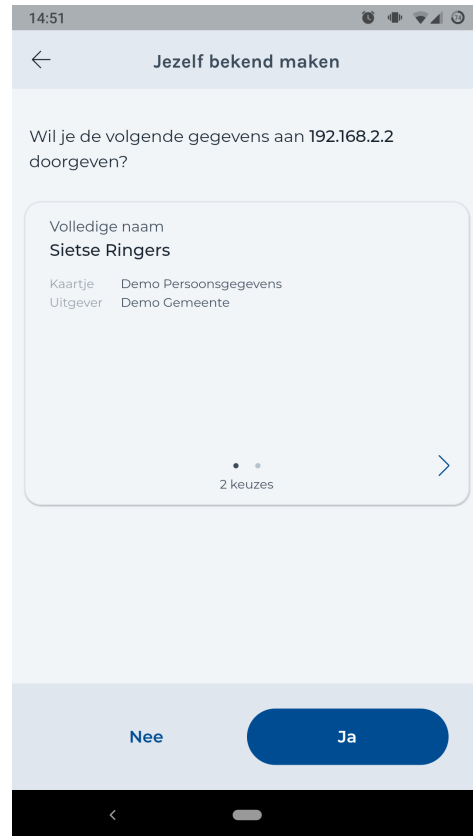


Issuance wizards

- Begeleid IRMA app gebruikers bij complexe registratieflows met meerdere kaartjes
- Met/voor Ivido ontwikkeld, maar algemeen bruikbaar (op aanvraag)
- (Op termijn) aan te vragen bij Bob Kronenburg, bob.kronenburg@sidn.nl

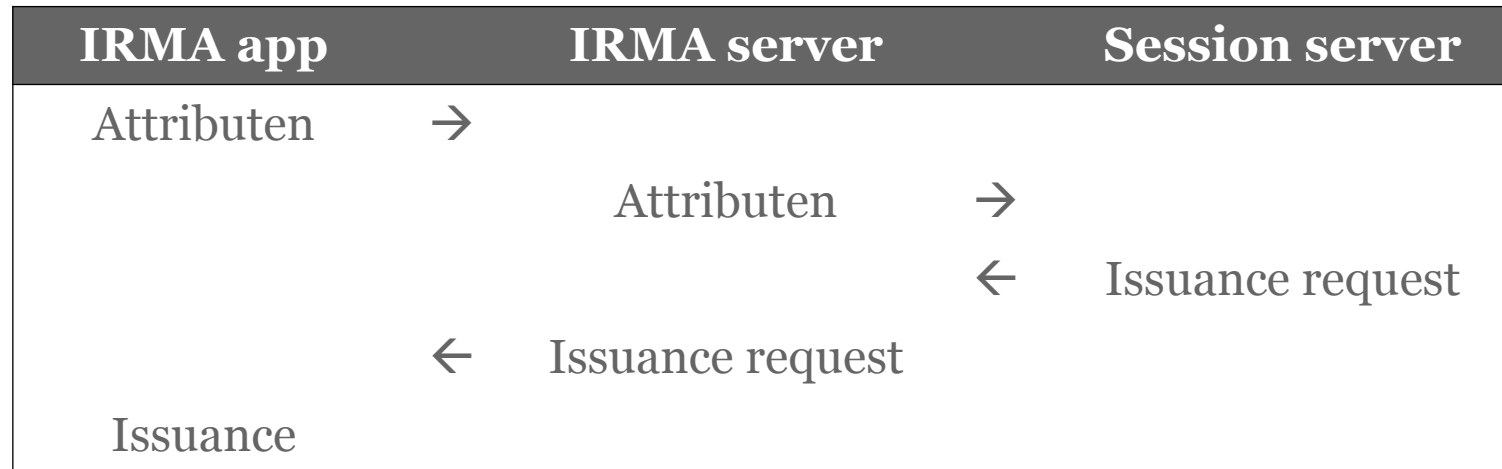


Chained sessions



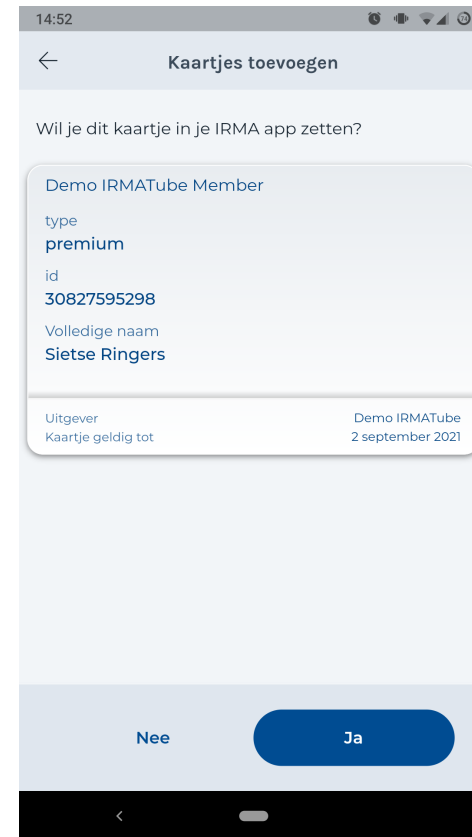
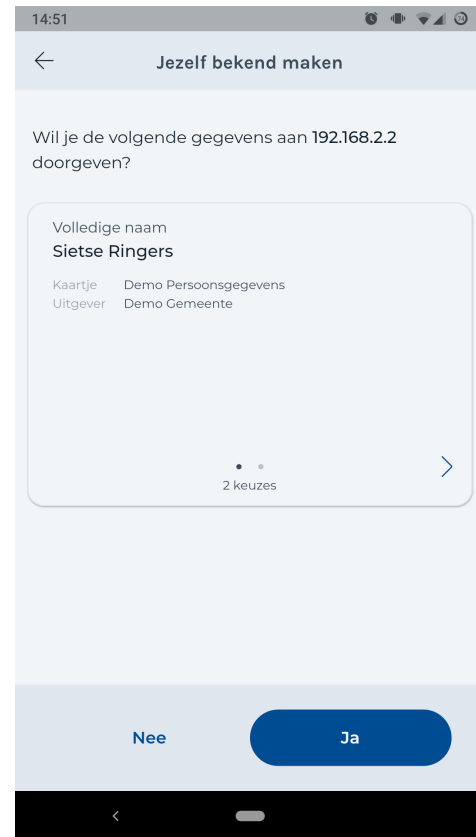
Chained sessions

- Sessie n mag afhangen van resultaat van sessie $n - 1$
- *Session server* ontvangt sessieresultaat en antwoordt met volgende session request
- Voorbeeld: toon BRP attributen → haal AGB code → issue AGB code



Chained sessions

- Demo: toon naam → issue naam in “IRMATube premium” kaartje



QR diefstal bescherming

- Voor issuance sessies, of disclosure sessies die gevoelige gegevens bevatten
- Alleen voor desktop flow
- Sessie vindt pas plaats nadat gebruiker code uit app overtypt in browser



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

