

IRMA

I Reveal My Attributes

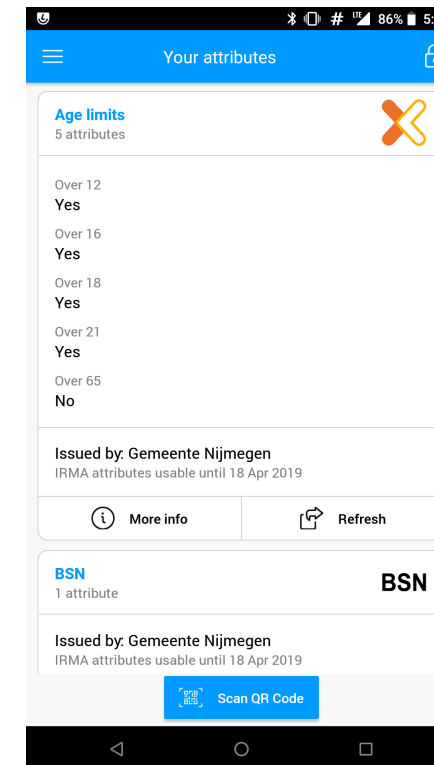
Attribuut-gebaseerde authenticatie

- Privacy en security
- Open source
- In de praktijk en in productie

Sietse Ringers

IRMA lead developer

Privacy by Design Foundation





“On the Internet, nobody knows you’re a dog.”

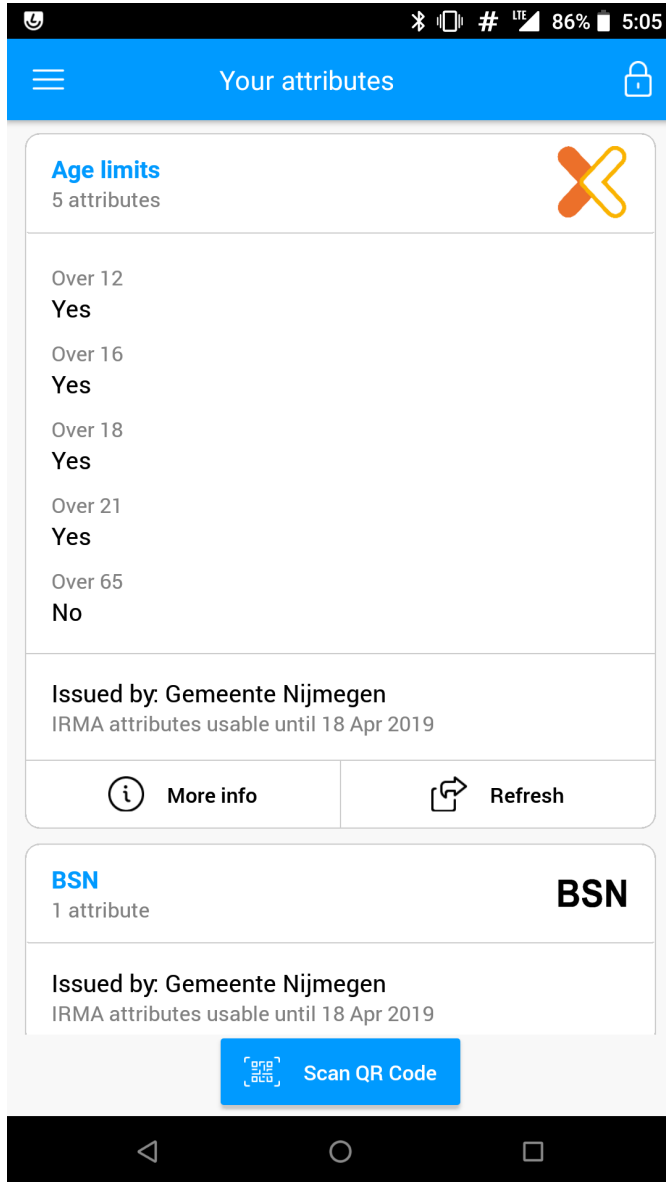
<https://privacybydesign.foundation>

- Opgericht in in 2016
- Voortgekomen uit onderzoek naar digitale identiteit @ Radboud universiteit
- Open source
- Stichting: geen winstoogmerk

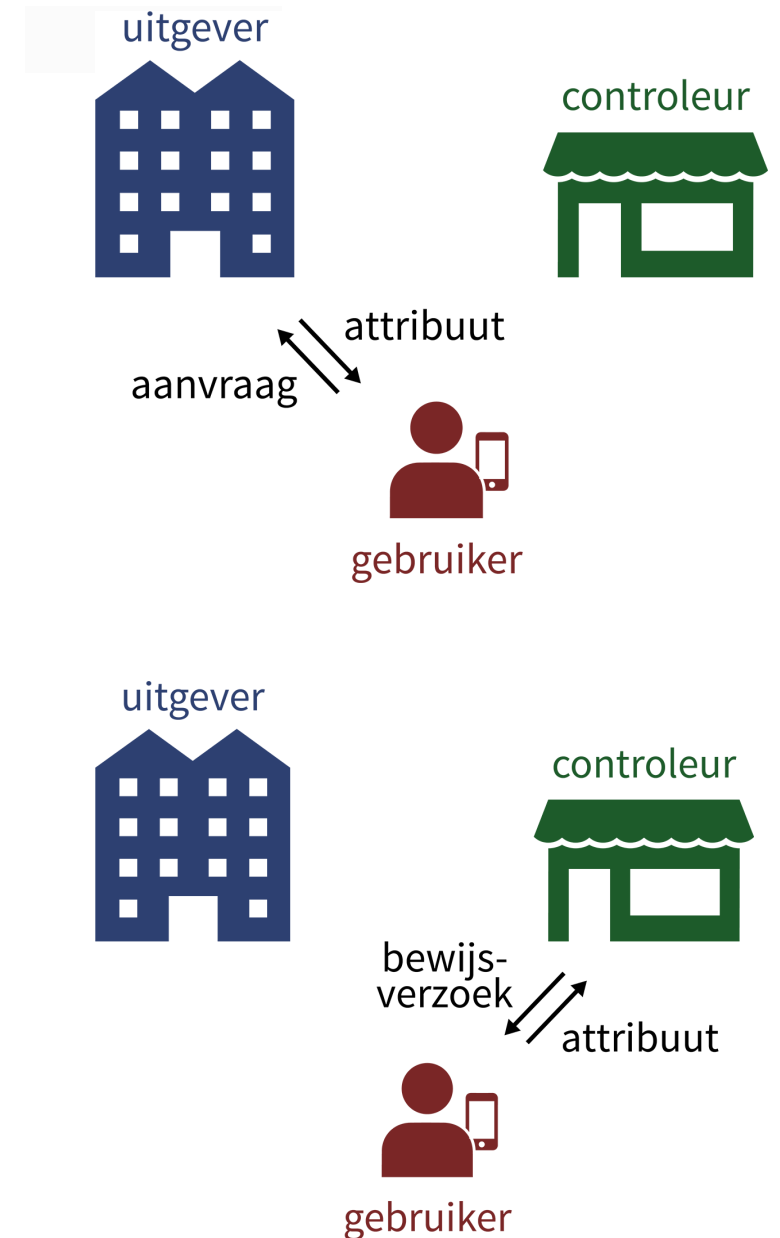


- Privacy Award 2018
- Brouwer prijs 2018
- ISOC.nl Internet Innovatie Award 2019

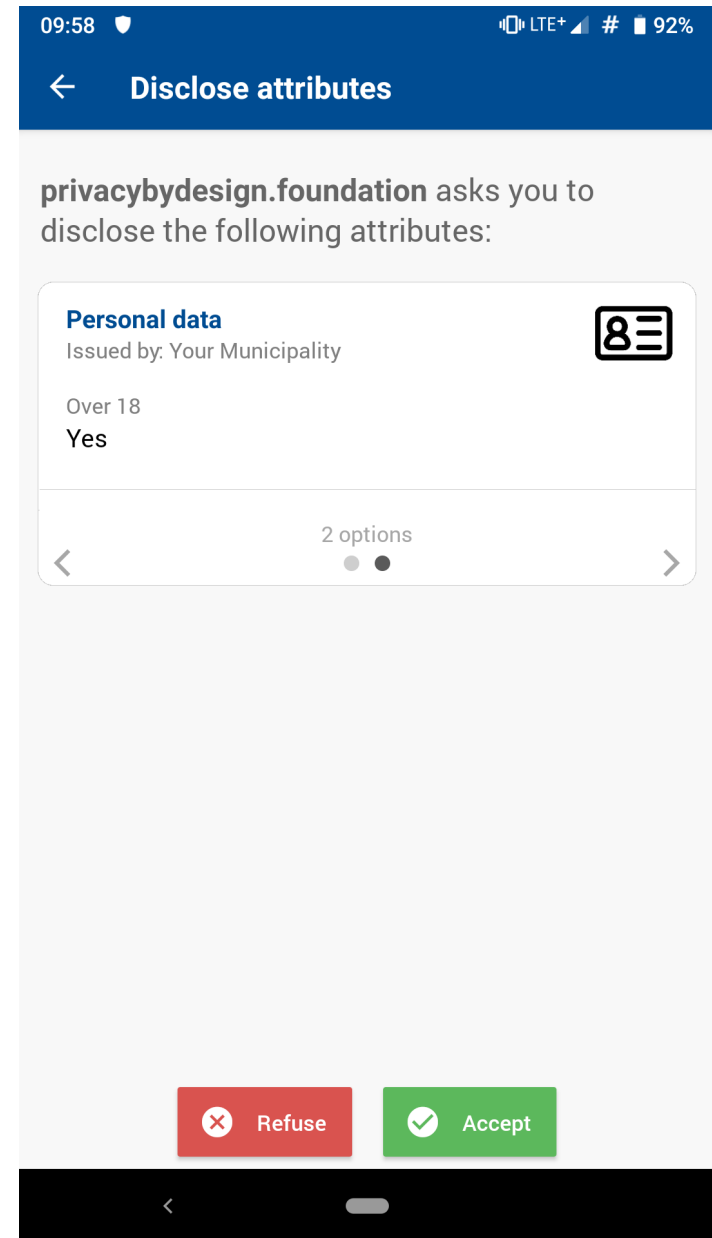
IRMA app



- Gebruiker verzamelt attributen in IRMA app
- Attributen zijn digitaal getekend door vertrouwde uitgever
- Identificerend (naam) of niet (> 18)
- Meerdere vrijgiftes zijn onlinkbaar
- Decentraal: attributen worden enkel op telefoon opgeslagen
- IRMA PIN unlockt app en attributen
- Gratis en open source



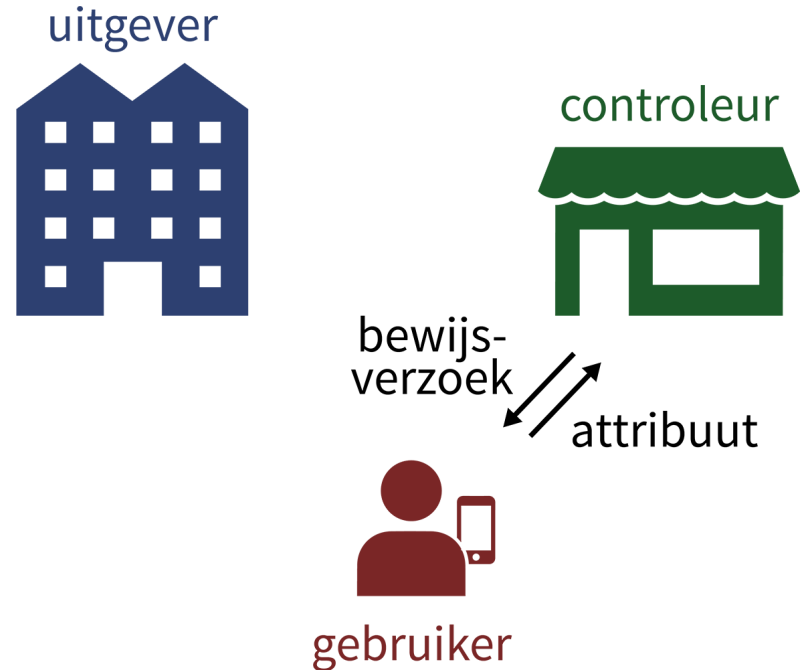
Demo
<https://angrygames.nl/>



Authenticatie vs. handtekeningen



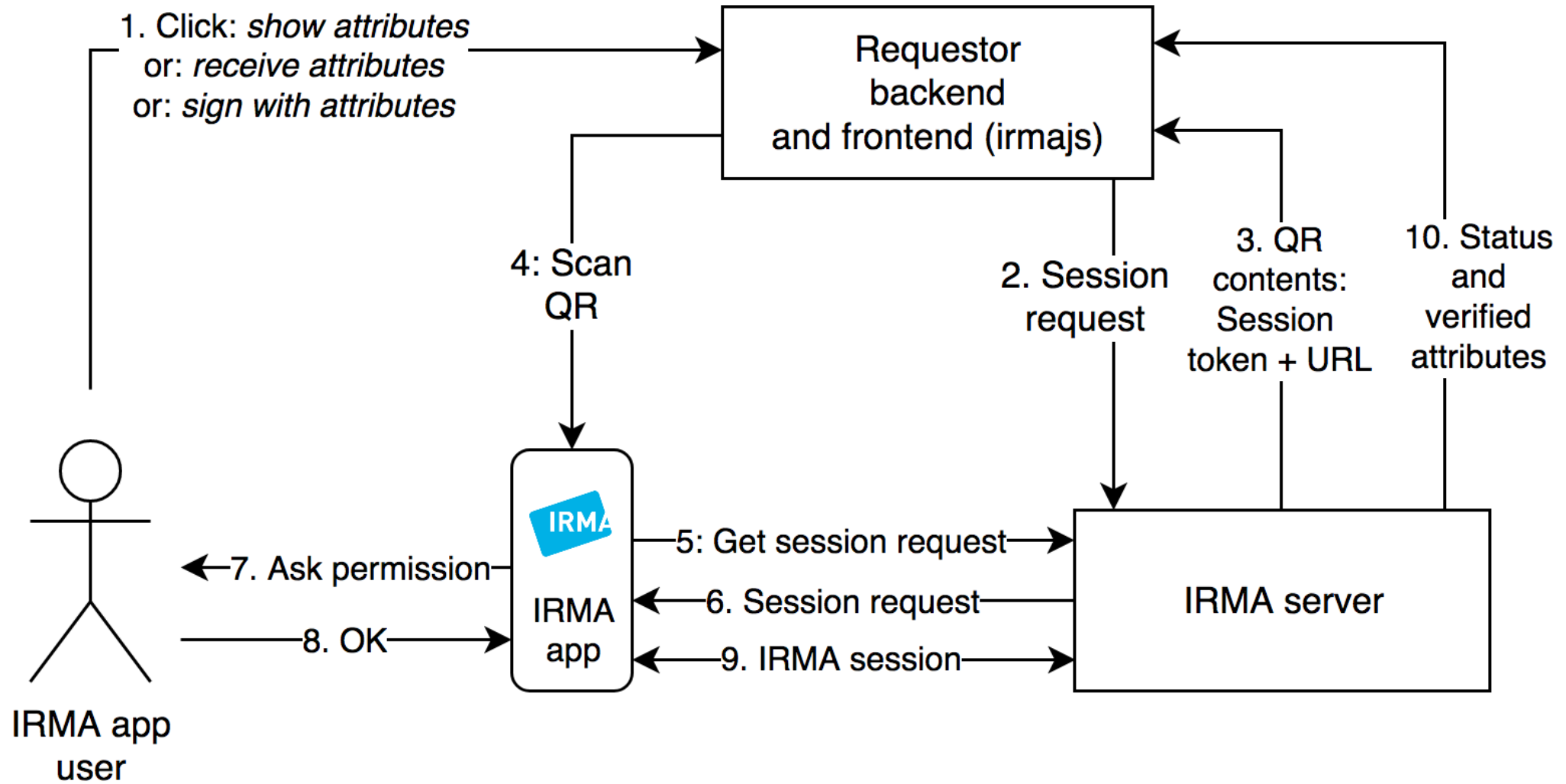
Authenticatie



Attribuut-gebaseerde handtekening

Ik geef toestemming om mijn data te delen met mijn huisarts.	
<i>Naam</i>	Eva
<i>MedMijID</i>	12345

Hoe werkt het?



Vorbereiding (zie irma.app/docs/getting-started):

- Installeer `irmajs` JavaScript library in je website voor IRMA QR
- Installeer `irma` binary op je server
- Start `irma server`

```
$ irma server -v
```

```
[2019-10-30T17:47:18+01:00] INFO irma server running mode=development verbosity=debug version=0.4.1
```

2. Start disclosure sessie

```
$ curl http://localhost:8088/session -X POST -H "Content-Type: application/json" -d \  
{  
  "@context": "https://irma.app/ld/request/disclosure/v2",  
  "disclose": [  
    [  
      [ "pddf.pddf.ageLimits.over18" ],  
      [ "pddf.gemeente.personalData.over18" ]  
    ]  
  ]  
}
```


3. Stuur sessionPtr naar irmajs in frontend

```
{
  "sessionPtr": {
    "u": "http://192.168.1.1:8088/irma/session/gr7R5Qf8PvJRaJgIo5H6",
    "irmaqr": "disclosing"
  },
  "token": "BtYi67NrjhCKsBTWfHNi"
}
```

10. Haal attributen op bij irma server

```
$ curl http://localhost:8088/session/BtYi67NrjhCKsBTWfHNi/result
```

```
{
  "status": "DONE",
  "proofStatus": "VALID",
  "disclosed": [
    [
      {
        "rawvalue": "Yes",
        "id": "pbdf.gemeente.personalData.over18"
      }
    ]
  ]
}
```

Software

- **irma** binary en server:
<https://github.com/privacybydesign/irmago>
- JavaScript library voor o.a. IRMA QR:
<https://github.com/privacybydesign/irmajs>
- Technische documentatie:
<https://irma.app/docs/>

Attributen

- BRP (naam, geslacht, leeftijd, adres, BSN)
- Email, 06
- Student
- Medisch professional (AGB)
- Demo: diploma

<https://privacybydesign.foundation/uitgifte/>

<https://privacybydesign.foundation/attribute-index/nl/>

Use cases

- Inloggen (met bv. e-mailadres)
 - 2FA: attribuut en PIN
 - Geen wachtwoordgedoe
- Verkrijg persoonsgegevens voor bv. aankopen of contracten
 - Geen privacy hotspots
 - Gevalideerde data door vertrouwde uitgevers
 - Automatische dataminimalisatie (AVG)
- Verifieerbare user consent
 - “Ik verleen toestemming om mijn data te delen met bedrijf X - Sietse Ringers”
- Jouw applicatie!

Wie gebruikt IRMA?



- <https://helder.health/>
 - Medisch dossier uitwisselingsstelsel voor oa. huisartsen
- Nijmegen, Amsterdam, Haarlem, Buren, 40+ gemeentes
 - BRP attriboot-uitgifte
 - Automatisch formulieren invullen met IRMA attributen
 - Inloggen op amsterdam.nl, haarlem.nl met IRMA (naast DigiD)
- Ivdo: PGO (Persoonlijke GezondheidsOmgeving)
 - Inloggen, emailadres
 - Naam, BSN van patiënt authenticeren
- SURFnet
 - IRMA als 2^e factor
 - Inloggen op SURFdrive

Meer informatie



- Websites:
<https://irma.app>
<https://privacybydesign.foundation>
- Source code:
<https://github.com/privacybydesign>
- Technische documentatie:
<https://irma.app/docs>
- IRMA Slack (vraag invite)

- Twitter:
https://twitter.com/irma_privacy

