

# IRMA Ontwikkelingen

Een kijkje achter de schermen

---

Dr. Hanna Schraffenberger

October 29, 2019

Privacy by Design Foundation, iHub Radboud University

1. IRMA geschiedenis
2. IRMA nu
3. IRMA toekomst
4. IRMA demo

IRMA geschiedenis

IRMA nu

IRMA toekomst

IRMA demo

**FASE 1 (2008-NU):** wetenschappelijk onderzoeksproject aan de Radboud University

- active onderzoekslijn over attribuut-gebaseerde authenticatie (via Idemix)
- 4 proefschriften, veel publicaties
- financiële steun van: NLnet, Translink, BZK, NWO, KPN
- prototype implementaties op
  - smart card – niet langer ondersteund
  - smart phone – alleen voor Android

FASE 2 (2016-NU): technologie **uitrol** via non-profit stichting Privacy by Design

- <https://privacybydesign.foundation>
- mobile app voor iOS en Android
- strategische samenwerking met SIDN sinds 2019
- stabiliteit en continuïteit daarmee gegarandeerd



IRMA geschiedenis

IRMA nu

IRMA toekomst

IRMA demo

## Wie werkt met IRMA? Twee sleutelgebieden...

- **Gemeenten** geven IRMA attributen uit, en maken nieuwe toepassingen mogelijk
  - zie presentaties vandaag
- **Zorg**, voor nieuwe online omgevingen
  - doorbraaktechnologie voor persoonlijke gezondheidsomgevingen
  - zowel voor zorgverleners als voor patiënten
  - zowel inloggen als ondertekening (bijv. van recepten)
  - koplopers: Ivido, Nedap Healthcare, Chipsoft, VGZ, en VZVZ
  - samenwerking van  $\geq 20$  zorg-ICT bedrijven via [nuts.nl](#)
  - **Voorbeelden** medisch gebruik:
    - groep [huisartspraktijken](#) (Medipark, Chipsoft pilot)
    - Artsenportaal [Helder](#)
    - Declaraties voor zaakwaarnemers bij [VGZ](#)

IRMA geschiedenis

IRMA nu

IRMA toekomst

IRMA demo

IRMA Ontwikkelingen

## Ontwikkelingen (selectie)

- roadmap
- keyshare server
- machtigingen
- fraude
- revocatie
- geschiedenis
- website
- terminologie
- IRMAbellen
- IRMAseal
- IRMA bijenkomst
- **IRMA UX**

# IRMA toekomst ► Roadmap



## Inspiratie: Unreal Engine Roadmap

The screenshot shows the Unreal Engine 4 Roadmap board on Trello. The board has several lists:

- Future Releases**:
  - Delta Color Compression (DCC) on Consoles
  - Switch Optimizations
  - Animation Streaming
  - New Physically-Based Atmospheric Sky Model
  - Bury Subsurface Scattering
  - Screen Space Global Illumination
  - New Audio Mixer
  - Virtual Texturing (coming out of beta)
  - High End Only Hair Rendering and Simulation (Experimental)
  - Ray Tracing Updates
  - USD "Univeral" Workflow Beta
  - Landscape tools improvements
  - GTAO SSSD on Consoles and Windows
  - Chaos Physics (production ready)
- Done for 4.24**:
  - Initial Blending
  - Anim Blueprint Linking (beta)
  - Chaos - Destruction (beta)
  - Blurry Subsurface Scattering
  - Screen Space Global Illumination
  - New Audio Mixer
  - Virtual Texturing (beta)
  - High End Only Hair Rendering and Simulation (Experimental)
  - Ray Tracing Updates
  - USD "Univeral" Workflow Beta
  - Niagara: Switch Support
  - Geographically Accurate Sun Positioning (beta)
  - Visual Studio 2019
  - Niagara Integration Into Chaos Physics
  - Animation Shading Hugin
  - Animation Sequence Framerate
  - Mixed Reality Capture (beta)
  - Digital Human Improvements
- Shipped with 4.23**:
  - Real-Time Ray Tracing and Path Tracing
- Shipped with 4.22**:
  - Geographic: Depth of Field
  - ProxyLOD Improvements
  - New Post Processing
- Shipped with 4.21**:
  - Geographic: Switch Support
- Shipped with 4.20**:
  - Geographic: Depth of Field
  - ProxyLOD Improvements
  - New Post Processing
- Shipped with 4.19**:
  - Landscape

## Herimplementatie keyshare server:

- voornamelijk van intern belang
- doelen:
  - beter onderhoudbaar maken keyshare
  - beter testbaar maken infrastructuur
  - beter upgradebaar maken
  - veiligheid opslag verhogen met encryptie
  - communicatie met MijnIrma webinterface robuuster maken
- loopt vermoedelijk tot december/januari

## Machtigingen met IRMA:

- **generiek**: niet alleen voor VGZ
- **specifiek**: niet machtigen voor alles, zoals bij DigiD, maar voor specifieke taken

## Proces voor fraudegevallen en vermoedens van fraude

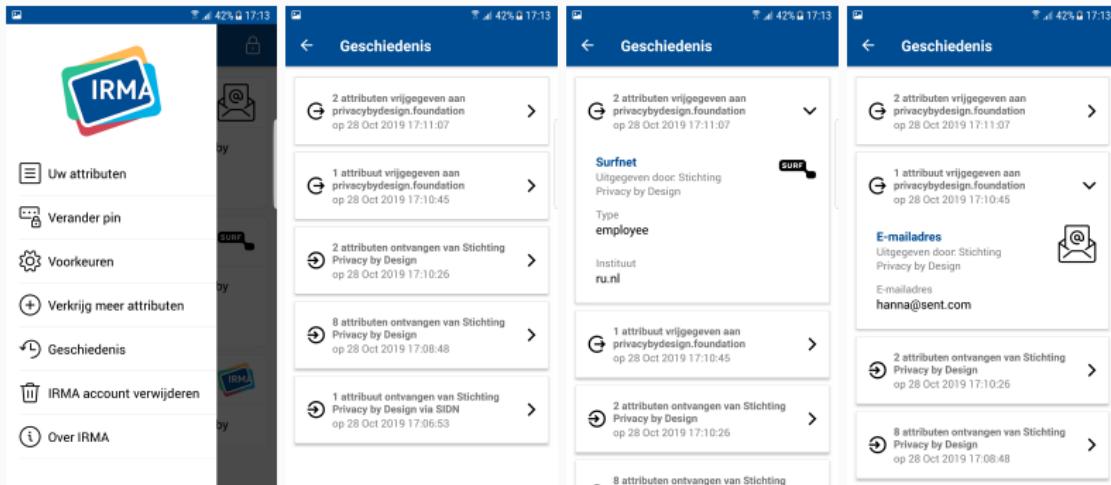
- wij kunnen fraude maar beperkt detecteren (bij de keyshare server)
- goed proces is nodig voor als mensen fraude vermoeden
- revocatie (mogelijkheid om credentials te kunnen blokkeren bij de issuer) is noodzakelijk

Mogelijkheid om specifieke attributen snel te blokkeren

- blokkeren van alle attributen mogelijk via MijnIRMA
- blokkeren van specifieke attributen nog niet mogelijk
- verlopen/verversen proces wordt gebruikt om te voorkomen dat mensen attributen gebruiken die niet langer geldig zijn
- dit is in sommige gevallen niet snel genoeg
- doel: revocatie door *issuer* (binnen 24 uur)
- vereist: infrastructuur (zwarte lijst) bij *issuer*
- vereist: privacy-vriendelijke controle van attributen door *verifiers* met zero-knowledge proofs

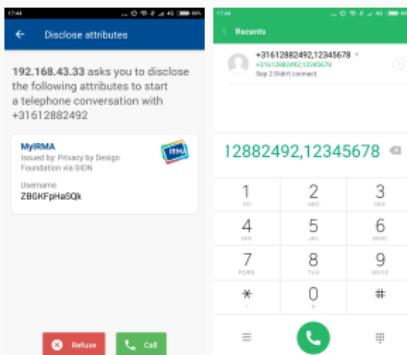
## Geschiedenis in Android beta

- Uitbreidingen mogelijk (verkennend stadium)



Hoe kunnen we de identiteit van iemand aan de telefoon vaststellen?

- Bloqzone heeft hiervoor een methode ontworpen via IRMA
- zie presentatie van Alexander Blom (11.30 – 11.50)
- binnen IRMA opgezet als **generieke feature** die door iedereen gebruikt kan worden



# IRMA toekomst ► Website



Uitbreiden en verbeteren van [www.irma.app](http://www.irma.app)

The screenshot shows a web browser window with the URL [127.0.0.1](http://127.0.0.1). The page has a dark blue header with the IRMA logo and navigation links: IRMA, Usage, Explanation, FAQs, Links, and a flag icon. The main content area features a large blue background with white text: "Choose IRMA. Put a digital passport on your own mobile." Below this are download buttons for "IRMA for iOS" and "IRMA for Android". To the right is a smartphone displaying the IRMA mobile application interface, which includes fields for "Email address" (2 addresses), "Age limits" (Over 12, Over 16, etc.), and a QR code section. At the bottom of the phone screen is a button labeled "Scan QR Code". At the bottom of the page are three circular icons: "Logging in" (user profile with a checkmark), "Signing digitally" (person at a desk with a laptop), and "Trust" (shield with a lock).

Uitbreiden en verbeteren van [www.irma.app](http://www.irma.app)

- internationalisatie
- toegankelijkheid
- tutorials
- details
- gezamenlijke terminologie

Gezamenlijke en consistente terminologie (“IRMA woordenboek”)



## I. IRMA is...

- een **digitaal paspoort** op je mobiel (bron irma.app)
- jouw **gepersonaliseerde paspoort opgeslagen in je telefoon** (bron appstore)
- een **digitale portemonnee** (bron prototype > Hoe werkt het > bullet 3)
- een **systeem waarmee je kunt bewijzen wie je bent, of welke eigenschappen je hebt** (bron <https://helder.health/register>)
- een **privacyvriendelijk authenticatie systeem** (bron VGZ)
- **distributed, attribute-based authentication platform** (bron tech intro <https://credentials.github.io>)
- een **digitale identiteitsmanager / een tool voor het makkelijk en veilig gebruiken van je online en offline identiteit** (bron presentatie AMS)

## Versleuteling met IRMA

- nog niet mogelijk
- V in AVO, zie [IRMA manifest](#)
- prototype voor email versleuteling, zie [NLnet project](#)
- demo op IRMA bijenkomst op 29 november
- nieuw projectvoorstel ingediend om versleuteling productie-klaar te maken
- zie video

### [AVO: Authenticatie, Versleuteling en Ondertekening](#)

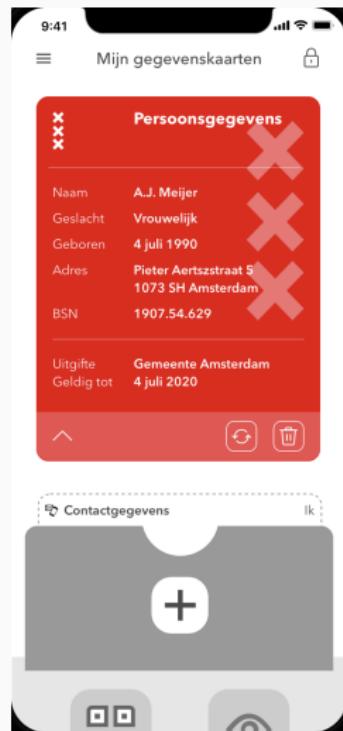
De zekerheden die met deze vijf toe's gepaard gaan hangen samen met de identiteiten van de betrokkenen: het moet duidelijk zijn *wie* toegang krijgt, voor *wie* iets wel of niet toegedekt wordt, *wie* toestemt of iets toeegt, en aan *wie* iets toegeschreven kan worden. De realisatie van die zekerheden maakt gebruik van de volgende drie technische basisbegrippen: authenticatie, versleuteling, en ondertekening. Ze worden hier gezamenlijk met de afkorting AVO aangeduid.

## Volgende IRMA bijeenkomst

- vrijdagmiddag 29 november
- van 13:30 tot 17:30
- op een locatie van de gemeente Amsterdam (Weesperstraat 113)

## IRMA app krijgt nieuwe user experience (UX)

- implementatie van open source UX ontwerp van Amsterdam's UX team
- samenwerking van Almere, Amsterdam, Drechtsteden, Groningen, Haarlem, Leiden en Nijmegen
- zie presentatie van Mark Fonds over NL DIGIbeter project (10.35 – 10.55)
- **doel:** release 1 eind 2019
- **release 1:** functionaliteit van huidige IRMA app met nieuwe UX
- **demo** van Mike Alders (UX lead)



IRMA geschiedenis

IRMA nu

IRMA toekomst

IRMA demo



# Vragen?