Attribute-based authentication and signing with IRMA

Towards Trustworthy Digital Identities in Europe
Brussels, July 3, 2019

Bart Jacobs — Radboud University and Privacy by Design foundation
bart@cs.ru.nl

Where we are, so far

Introduction

Platforms

IRMA usage

Conclusions

Overview

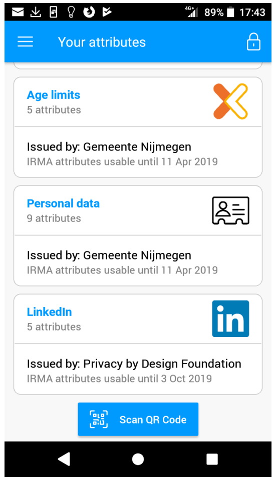
Attribute-based authentication & signing, via identity platform “IRMA”

- up-and-running, freely available, gaining traction in NL
- esp. in local government & healthcare
- IRMA is an open source Swiss army knife for digital identity

IRMA’s general picture

- value-driven design, connecting principles and solutions
- relevant values: self-sovereignty, transparancy, independence
- innovative approach, operated by non-profit foundation
- it’s a grassroot ecosystem, via a community effort,

IRMA app, for revealing only relevant attributes



89% 17:43

Your attributes

Age limits
5 attributes

Issued by: Gemeente Nijmegen
IRMA attributes usable until 11 Apr 2019

Personal data
9 attributes

Issued by: Gemeente Nijmegen
IRMA attributes usable until 11 Apr 2019

LinkedIn
5 attributes

Issued by: Privacy by Design Foundation
IRMA attributes usable until 3 Oct 2019

Scan QR Code

Essentials:

- attributes instead of identities
- collected by user him/herself
- attributes are reliable (digitally signed by source)
- decentralised architecture: attributes only on users own phone
- IRMA is free & open source

IRMA history, in two phases

- **2008 – now**: scientific research project at Radboud University
  - active research line on attribute-based authentication
  - 3 PhD theses so far, postdocs too, many publications
  - prototype implementations on:
    - smart card — at first, but no longer supported
    - smart phone — for Android only
- **2016 – now**: technology deployment via non-profit foundation
  - `https://privacybydesign.foundation` set up in fall 2016
  - foundation runs infrastructure, and issues some attributes
  - both Android and iOS apps, with common code-base in **Go**
  - strategic cooperation established with SIDN: larger foundation that issues domain-names in NL

Prizes for IRMA (in 2018 en 2019)

Privacy award
from Privacy First

KONINKLIJKE
HOLLANDSCHE MAATSCHAPPIJ
DER WETENSCHAPPEN

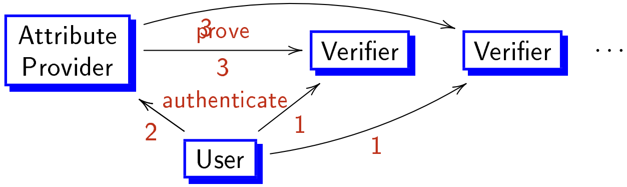
Brouwer prize
from KHMW

Internet Innovation
award from ISOC

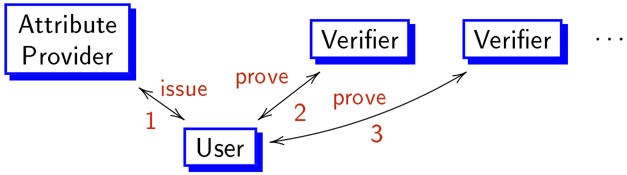
Juries appreciate the combination of a solid scientific basis and potentially big societal impact.

Centralised versus decentralised, schematically

Centralised: everything goes via the Attribute Provider (think Facebook)



Decentralised: everyting goes via the User (think IRMA)



Where we are, so far

Introduction

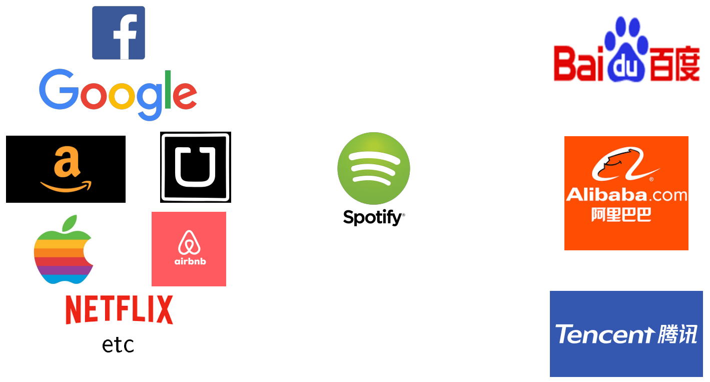
Platforms

IRMA usage

Conclusions

The world's platforms

US	Europe	China



etc

The shared US-CN agenda

- Both US and CN platforms wish to control digital identities
  - they wish to precisely register who is doing what & when online
  - goal: build up detailed profiles
- The US platforms have mostly commercial motives
  - but they have been used for political manipulation too
- The CN platforms are instrumental in maintaining state control
  - see e.g. their role in "social credit scores"

These systems work on the basis of a unique identifier (number), per individual, that is used everywhere — very unlike attributes

Maybe we should do things differently in Europe!

After the Cambridge Analytica scandal . . .

- Widely shared sentiment: we need another kind of IT-infrastructure
- one in which European values are embedded
  - arising through "value-driven design"
- ultimately this is a geopolitical matter
  - developments are driven by the commercial sector in the US
  - by the state in China
  - by civil society in Europe?

Where we are, so far

Introduction

Platforms

IRMA usage

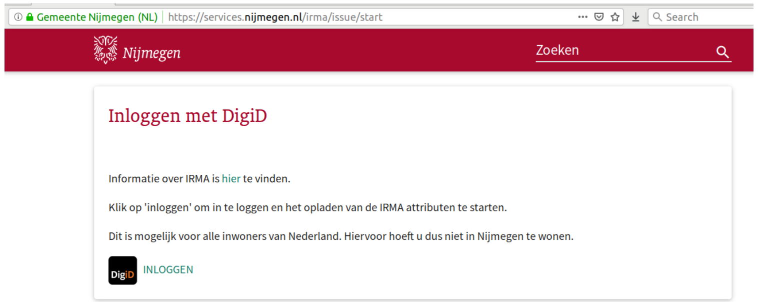
Conclusions

Which sectors are leading?

- **Local** government
  - it has established an IRMA-BRP connection with the official national registry of citizens
  - legal checks have been performed
  - this provides all Dutch citizens with reliable attributes in IRMA — including the sensitive citizen number BSN
  - local government is much better than national government in operating in a networked society
- e-health sector
  - IRMA is used in portals, both for patients & doctors
  - availability of BSN is crucial
- Other sectors are joining, e.g. insurance

Main point: an IRMA ecosystem is emerging, in which parties benefit from each other's efforts.

Illustration: Nijmegen city's IRMA page


Gemeente Nijmegen (NL) https://services.nijmegen.nl/irma/issue/start
Search
Nijmegen
Zoeken

Inloggen met DigiD

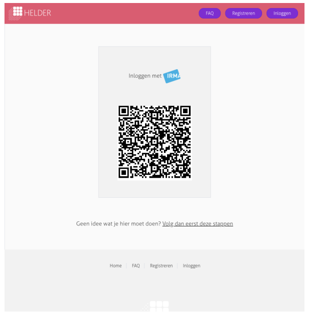
Informatie over IRMA is hier te vinden.

Klik op 'inloggen' om in te loggen en het opladen van de IRMA attributen te starten.

Dit is mogelijk voor alle inwoners van Nederland. Hiervoor hoeft u dus niet in Nijmegen te wonen.

- Citizens can login, and then obtain IRMA attributes from the government's citizen administration
- This is available for everyone in NL

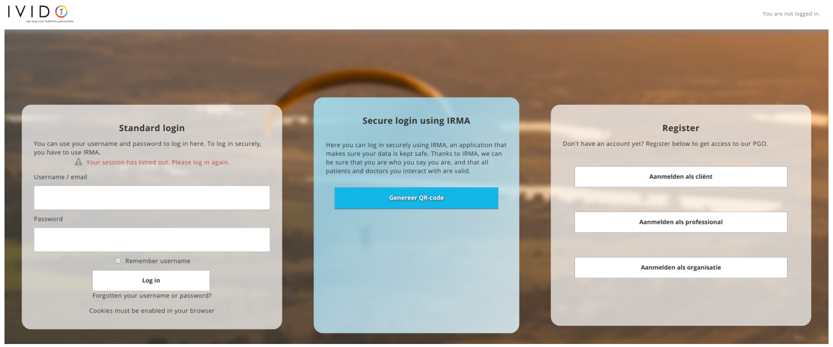
Doctor's portal Helder: login exclusively with IRMA



Geen idee wat je hier moet doen? Volg dan eerst deze stappen

- Several e-health companies in NL are joining forces to set-up an open standard, including IRMA-based authentication & signing
- This consortium nuts.nl issues special IRMA attributes to health care professionals — contributing to an IRMA ecosystem

Login to patient portal with IRMA



Standard login

You can use your username and password to log in here. To log in securely, you have to use IRMA.

Your session has timed out. Please log in again.

Username / email

Password

□ Remember username

Forgotten your username or password?

Cookies must be enabled in your browser

Secure login using IRMA

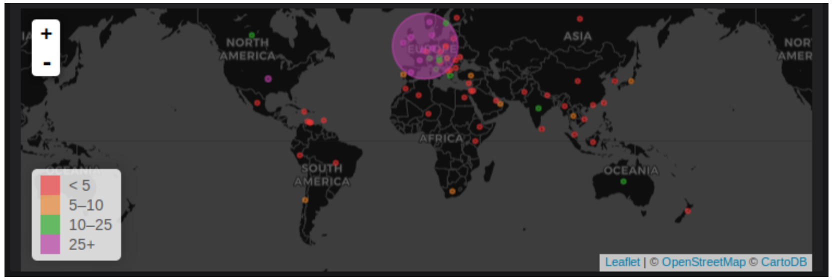
Here you can log in securely using IRMA, an application that makes sure your data is kept safe. Thanks to IRMA, we can be sure that you are who you say you are, and that all patients and doctors you interact with are valid.

Register

Don't have an account yet? Register below to get access to our PGO.

International dimension of IRMA

IRMA is globally available, with now ±90% of > 7500 registrations in NL



The decentralised set-up makes IRMA ideal for international usage

- only public keys needed for verification — and open source software
- bottom-up approach; no eIDAS-style connectors between countries

International expansion of IRMA

- Current focus is on NL, to get it widely used there
  - international expansion is not a priority now
- Expansion will go step-by-step, since national trust anchors are needed, per country, as reliable sources of attributes
  - attributes can reflect existing national authentication cultures
  - IRMA is made for diversity
- International partnerships are being developed.

Where we are, so far

Introduction

Platforms

IRMA usage

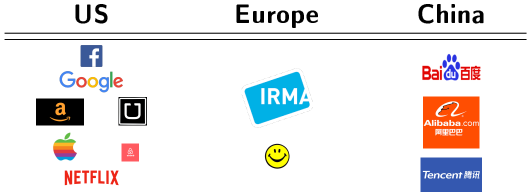
Conclusions

Near future plans, very briefly

- Extend IRMA with identity-base encryption (with a bit of NGI funding)
- Use IRMA signatures against fakenews / deep fakes

Concluding remarks

- Information flows and authentication requirements determine power relations in modern societies
  - what kind of society do we wish to live in?



- IRMA is a decentralised, open source, non-profit, flexible identity platform that is up and running, and being used & tested
  - it integrates attribute-based authentication and signing
  - it provides privacy-friendly empowerment of users
  - it's well on the way, on a long road
  - it's a community effort, not aiming to monopolise