

Quick introduction to IRMA and overview of new developments

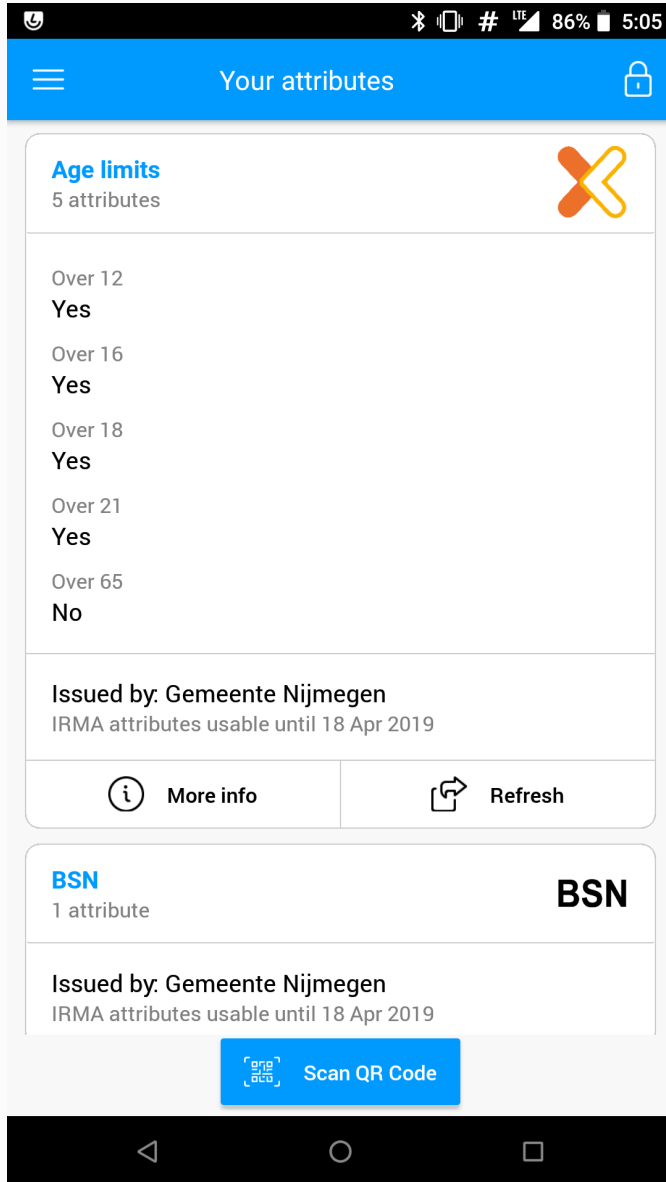
Sietse Ringers

IRMA lead developer

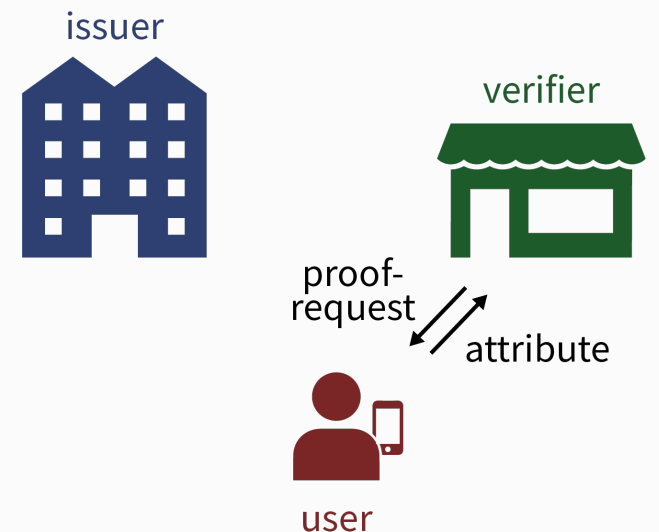
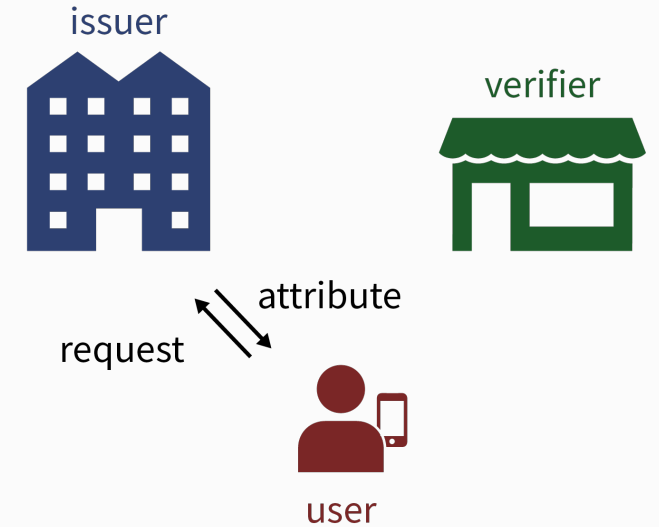
Privacy by Design Foundation

March 8, 2019

(Re-)introduction to IRMA



- Attributes instead of identity
- Collected by user
- Attributes are digitally signed by trusted issuer
- Identifying (name) or not (> 18)
- Multiple disclosures are unlinkable
- Decentral: attributes are stored only on phone
- IRMA PIN to unlock app & attributes
- Free and open source



Awards

- Dutch Privacy award 2018
- Stichting Privacy First



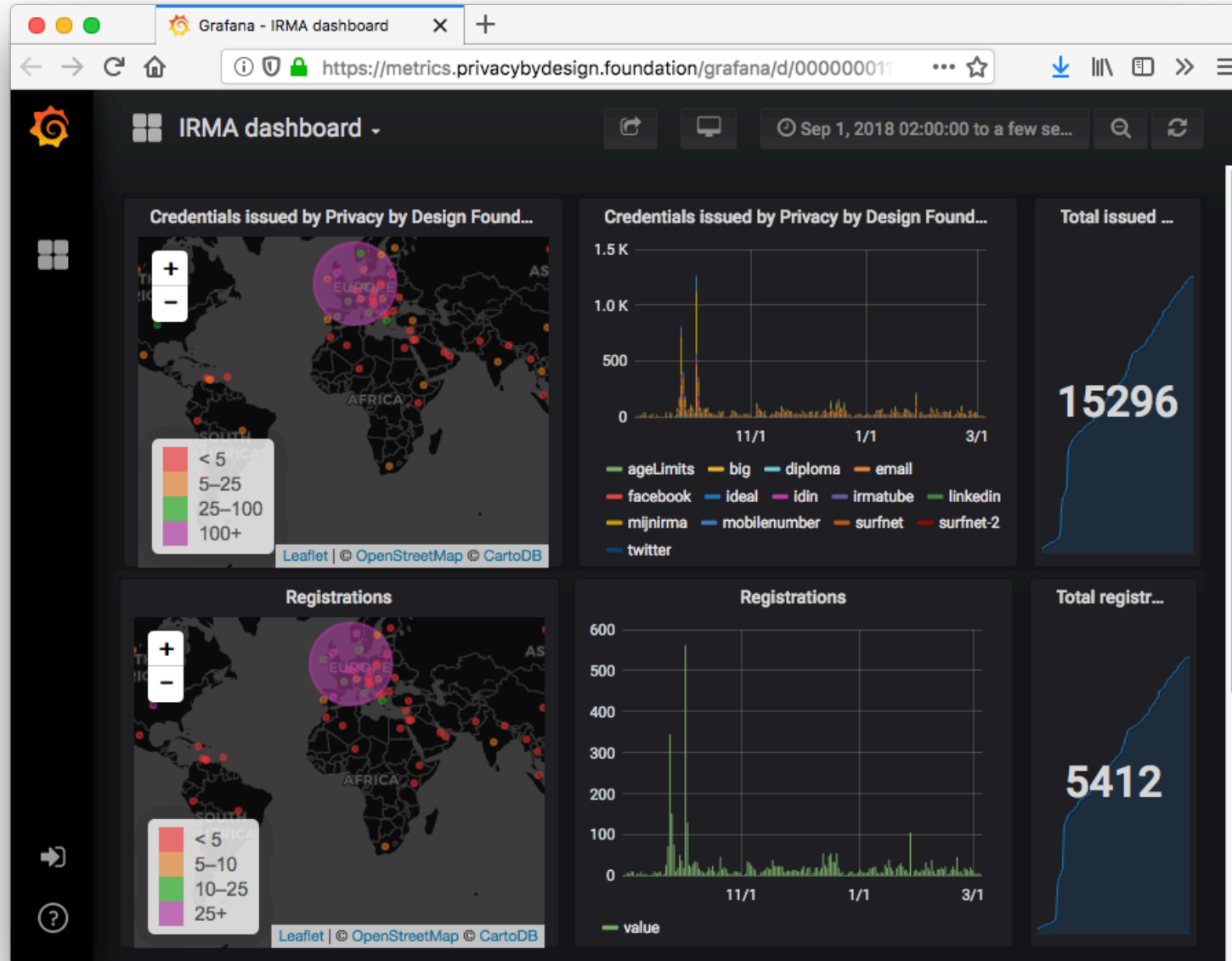
- Brouwer award 2018
- Koninklijke Hollandse Maatschappij der Wetenschappen



- Internet Innovation Award 2019
- Internet Society Nederland



IRMA usage



IRMA for developers



- Releasing new IRMA server, related software, and documentation
- Focus on developer friendliness
 - Easy to understand and use
 - Conventional and modern API familiar to developers
 - Dropping legacy
 - Accompanying technical documentation:
<https://irma.app/docs>

The screenshot shows a web browser window displaying the IRMA documentation website. The page title is "What is IRMA? · IRMA docs" and the URL is "https://irma.app/docs/what-is-irma/". The navigation bar includes "IRMA docs", "Docs", "Attribute index", "About", and "Privacy by Design Foundation".

Intro

- [What is IRMA?](#)
- [Getting started](#)

Guides

- [irma command line tool](#)
- [irma server](#)
- [irma server library](#)
- [irmajs JavaScript library](#)
- [IRMA schemes](#)
- [Session requests](#)
- [Email address](#)

API reference

- [Go libraries](#)
- [irmajs](#)
- [irma server](#)

Documentation

- [Technical overview](#)
- [Zero-knowledge proofs](#)
- [Keyshare protocol](#)

What is IRMA?

IRMA is a set of software projects implementing the Idemix attribute-based credential scheme, allowing users to safely and securely authenticate themselves as privacy-preserving as the situation permits. Users receive digitally signed attributes from trusted issuer, storing them in their IRMA app, after which the user can selectively disclose attributes to others.

Schematically:

Using the issuer's digital signature over the attributes the verifier can verify that the attributes were given to the user in the past, and that they have not been modified since.

IRMA session flow

A typical IRMA session is depicted schematically below.

```
graph TD; A[1. Click: show attributes  
or: receive attributes  
or: sign with attributes] --> B[Requestor  
backend  
and frontend (irmajs)]; B --> A;
```

New IRMA software



- `irma`: a single command line tool IRMA scheme mgmt, key generation, session testing, and more
- `irma server`: IRMA server subcommand
 - Easy to install (single binary) and experiment with
 - Easy to configure; default configuration immediately usable
 - More versatile; developer-friendly API
 - Better and more logging
 - More efficient/scalable
 - Also available as Go library; other languages will follow
- New JavaScript library `irmajs`
 - Modern JavaScript with smaller/simpler API
- IRMA developer documentation: <https://irma.app/docs>

- Healthcare sector:
 - Ivido
 - Nuts
 - VGZ
- Municipalities:
 - Whitelabel BRP attribute issuance
 - Nijmegen: fill form with attributes & call-me-back IRMA signatures
 - Haarlem, Almere, Leiden: dashboard in city hall issuing passport attributes (eIDAS high)
 - Haarlem: log in with IRMA
- SIDN

More information



- Website:
<https://privacybydesign.foundation>
- Source code:
<https://github.com/privacybydesign>
- Technical documentation:
<https://irma.app/docs>
- IRMA Slack (ask for invite)

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

