

“State of the IRMA”

(Re-)introduction to IRMA
and new developments

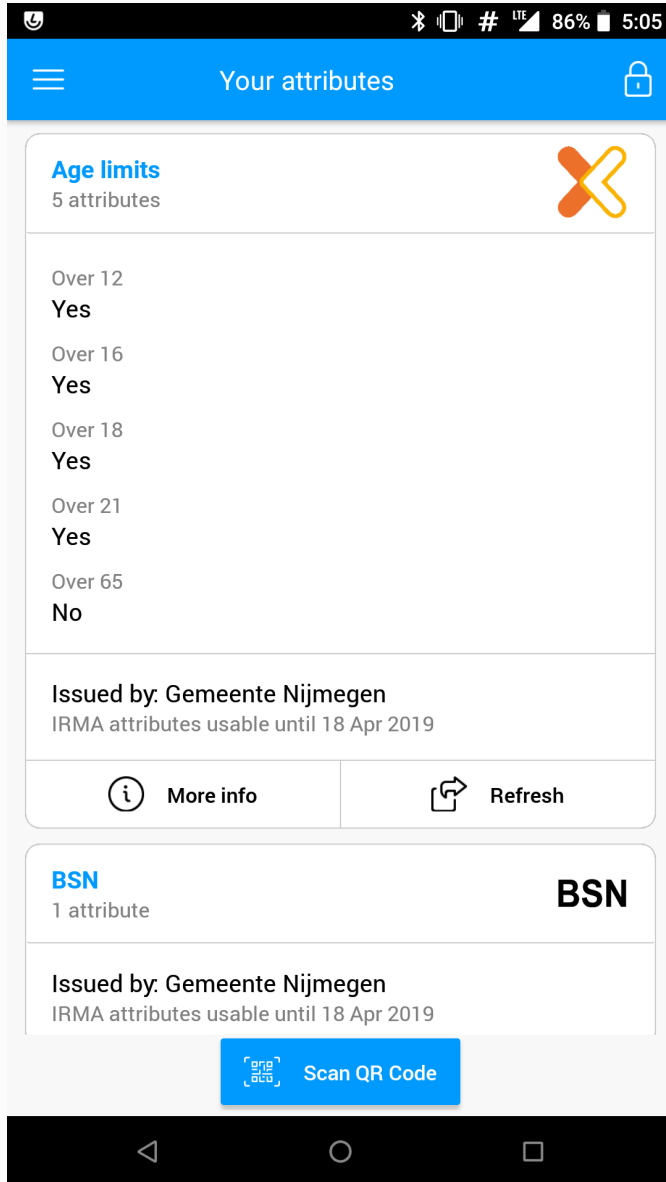
Sietse Ringers

Tomas Harreveld

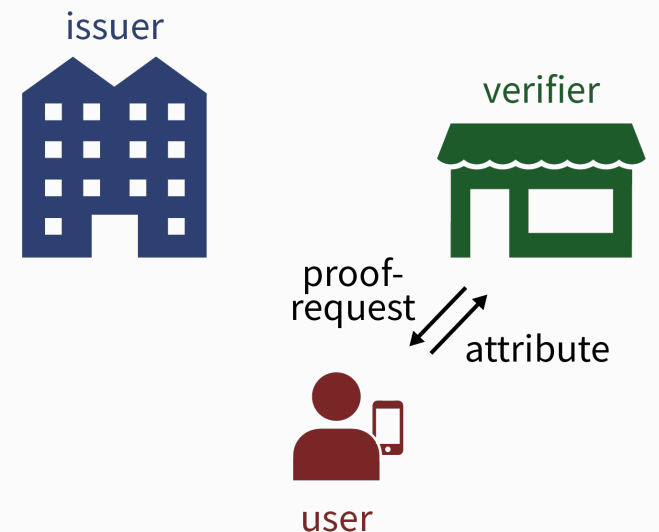
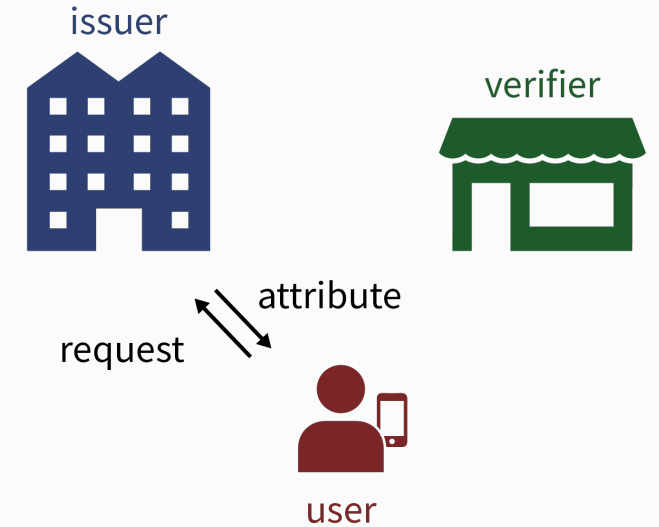
Privacy by Design Foundation

June 5, 2019

(Re-)introduction to IRMA



- User collects attributes
- 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



irma command line tool (including irma server)
deprecates Java irma_api_server

```
2. irma /Users/john (irma)

~ >>> irma version 15:05:50
IRMA toolkit
Documentation: https://irma.app/docs

Version: 0.3.0
OS/Arg: darwin/amd64

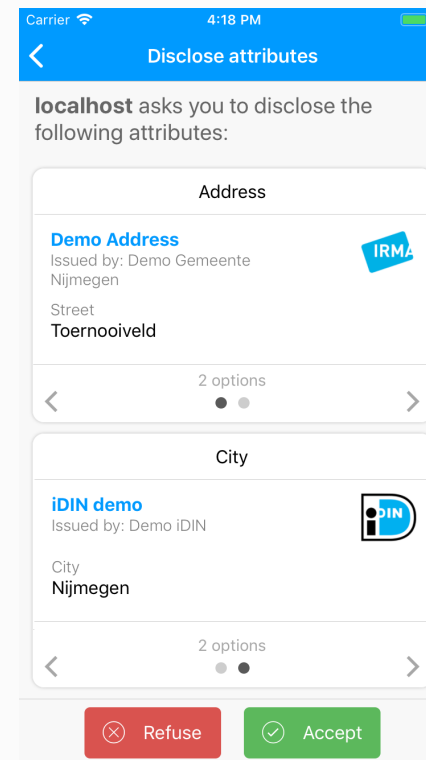
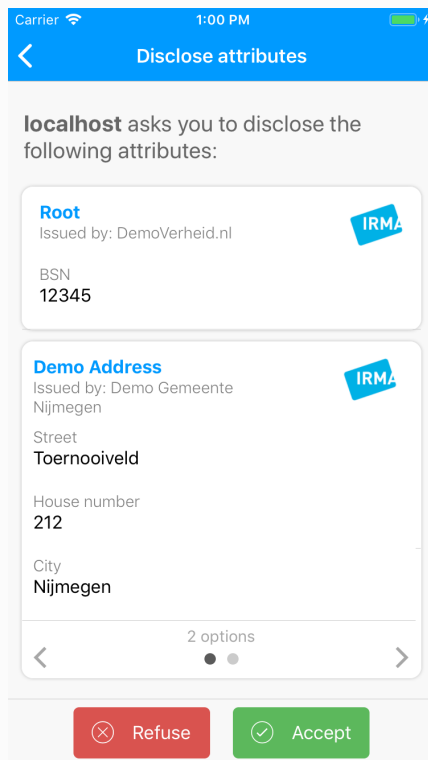
~ >>> irma server -v 15:05:52
[2019-07-03T15:06:08+02:00] INFO irma server running mode=d
velopment verbosity=debug version=0.3.0
[2019-07-03T15:06:08+02:00] INFO No configuration file found
```

Releasing 'condiscon'



More flexible attribute requests for IRMA verifiers

- For each requested attribute **set**, offer multiple choices
- Conjunction of disjunctions **of conjunctions** of attributes
- For each requested attribute, offer multiple choices
- Conjunction of disjunctions of attributes

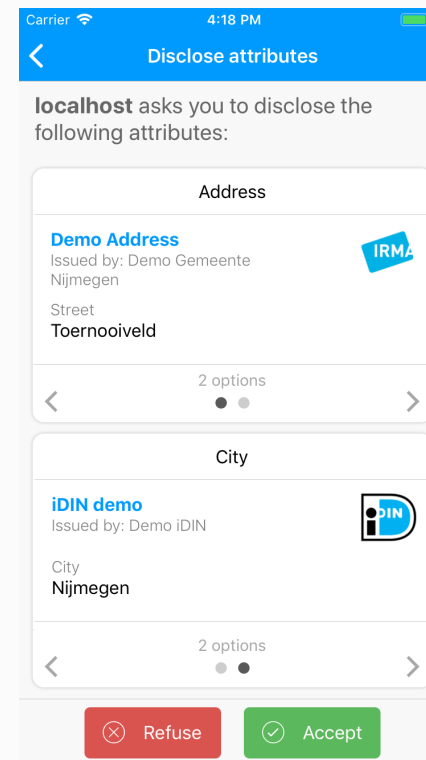
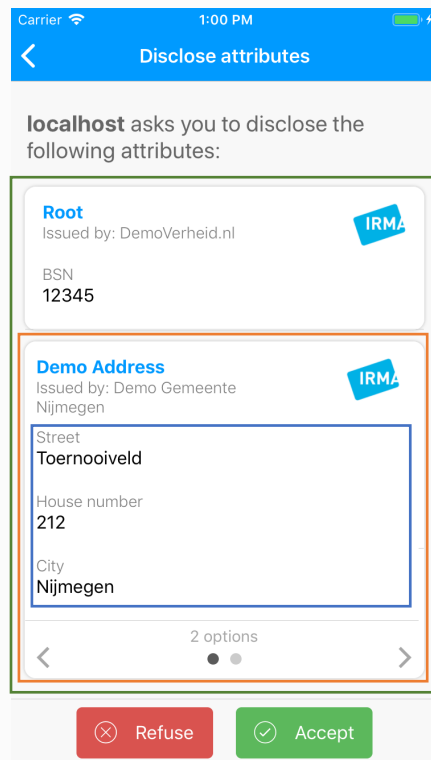


Releasing 'condiscon'



More flexible attribute requests for IRMA verifiers

- For each requested attribute **set**, offer multiple choices
- **Conjunction** of **disjunctions** of **conjunctions** of attributes
- For each requested attribute, offer multiple choices
- Conjunction of disjunctions of attributes

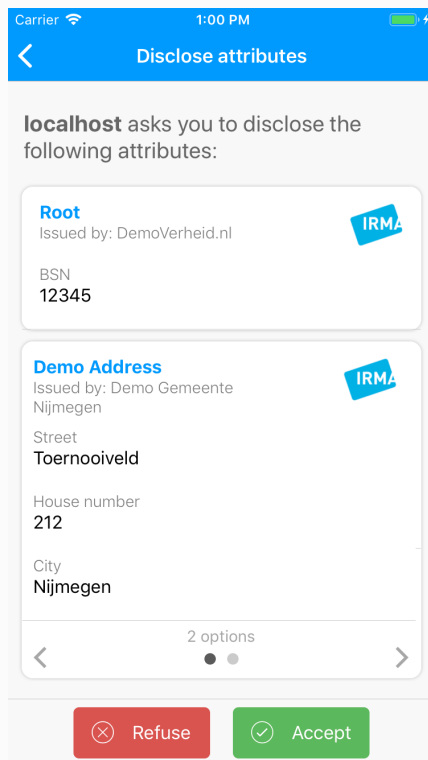


Releasing 'condiscon'

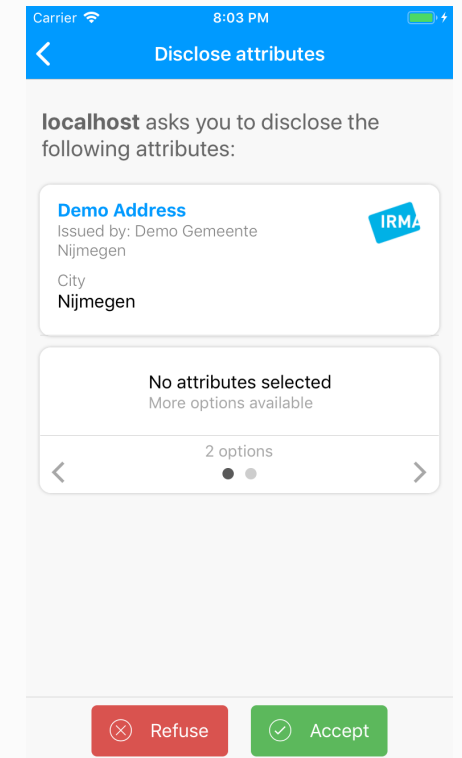


More flexible attribute requests for IRMA verifiers

- For each requested attribute set, offer multiple choices
- Conjunction of disjunctions of conjunctions of attributes



- Prevent cross-credential mixes
- IRMA app GUI: clearer relation between stored credentials and disclosed attributes
- Disclosure labels are optional and translatable
- Optional disjunctions: include empty candidate set
- Absent optional attributes (null attributes) no longer abort the session
- New IRMA apps, servers are backwards compatible with pre-condiscon
- New session request format (see updated documentation)



Coming: revocation



- Issuer can revoke individual previously issued credentials
- Revocation is instantaneous (as long as IRMA apps and servers keep up-to-date revocation state)
- Fully compatible with unlinkability

For each credential, the IRMA app includes a new zero-knowledge proof that the credential has not been revoked:

1. IRMA app sends disclosed attributes
2. IRMA app sends zero-knowledge proof:

“I have a valid credential containing these attributes”

AND

“This credential has not been revoked”

First use case: Gemeente BRP attributes

Roadmap and issue tracker



The screenshot displays a Jira issue tracker interface. At the top, there is a search bar and navigation buttons. The main area is a grid of issue cards, each representing a task or feature. Each card includes a title, a progress bar with colored segments (yellow, red, green, purple), and a status indicator (e.g., 'In Progress', 'Done', 'Blocked'). The issues are organized into columns, likely representing different teams or project phases. The interface is clean and modern, with a dark blue header and a light gray background for the issue cards.

Continuous integration met Gitlab



- Richting:
 - Signed commits en releases
 - Reproducible builds

GitLab Projects Groups More Search or jump

IRMA > Github mirrors > irmago > Pipelines

All 60 Pending 0 Running 0 Finished 60 Branches Tags

Status	Pipeline	Triggerer	Commit	Stages
passed	#26426 latest		master -> 9e10ae11 feat: link to documenta...	✓ ✓
passed	#23316 latest		signingtime -> 63eb5f54 hack: Added SigningTi...	✓ ✓

Intro

[What is IRMA?](#)

[Getting started](#)

New

["Condiscon" session requests](#)

Guides

[irma command line tool](#)

[irma server](#)

[irma server library](#)

[irmajs JavaScript library](#)

[IRMA schemes](#)

[Session requests](#)

[Email address](#)

API reference

[Go libraries](#)

[irmajs](#)

Getting started

This page shows how to get started with verifying or issuing IRMA attributes, using the following components:

- [irma server](#), a server that verifies or issues IRMA attributes to [IRMA apps](#),
- [irmajs](#), a JavaScript library for drawing the IRMA QR in your website, and handling IRMA session with the [irma server](#).

You should have the IRMA app installed ([Android](#), [iOS](#)). If you want to compile from source instead of using prebuilt binaries, you should additionally have [Git](#), [Go](#), [dep](#), and [npm](#) installed.

Installing and running [irma server](#)

You can install the [irma](#) command line tool in the following two ways.

Installing and running [irma server](#)

Perform a command line IRMA session

Installing [irmajs](#) and an example webpage

Perform browser IRMA session



IRMA BRP attributen laden

Via deze pagina kunt u uw gegevens uit de basisregistratie personen (BRP) laden als attributen in IRMA. Klik op 'inloggen' om in te loggen met DigiD en het laden van de IRMA attributen te starten.



[Inloggen met DigiD](#)

Landelijke BRP uitgifte

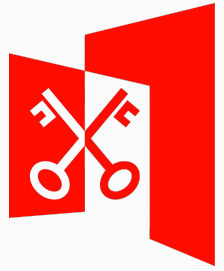


- Te gebruiken vanaf aankomende maandag 8 juli
- Verifiers kunnen (moeten) nu al hun requests aanpassen:

```
{
  "type": "disclosing",
  "content": [{
    "label": "Volledige naam",
    "attributes": [
      "pbdn.nijmegen.personalData.fullName"
    ]
  }]
}
```



```
{
  "type": "disclosing",
  "content": [{
    "label": "Volledige naam",
    "attributes": [
      "pbdn.nijmegen.personalData.fullName",
      "pbdn.gemeente.personalData.fullName"
    ]
  }]
}
```



Leiden

Gemeente Almere



Haarlem

× Gemeente
× Amsterdam

- Voortgekomen uit het Digitale Identiteitslab
- Binnen de pilot gegevens uit identiteitskaart, paspoort of rijbewijs (inclusief pasfoto)



- Uitbreidbaar naar hogere mate van controle, stadspas, balie
- Peer to peer verificatie vanuit de IRMA app
- Open source kaartlezer, ook te gebruiken op Android en iOS



Lokale Digitale Democratie met Consul



Log in

Log in via:





Home > Bewoners > Milieustations

Milieustations

U kunt uw afval ook zelf wegbrengen naar een van de twee milieustations in 's-Hertogenbosch. Let op: zorg dat u uw pas bij u hebt!

Waar?

- Milieustation Treurenburg, Galliumstraat 9 in 's-Hertogenbosch. Open van maandag tot en met vrijdag van 8.30 tot 17.00 uur. Op zaterdag van 8.30 tot 16.00 uur. Hier vindt u een afvalstation van Milieuwilt/Kreisloopbedrijf





[Home](#) > IRMA-formulier

IRMA-formulier



Haal IRMA attributen op

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

