

“State of the IRMA”

(Re-)introduction to IRMA
and new developments

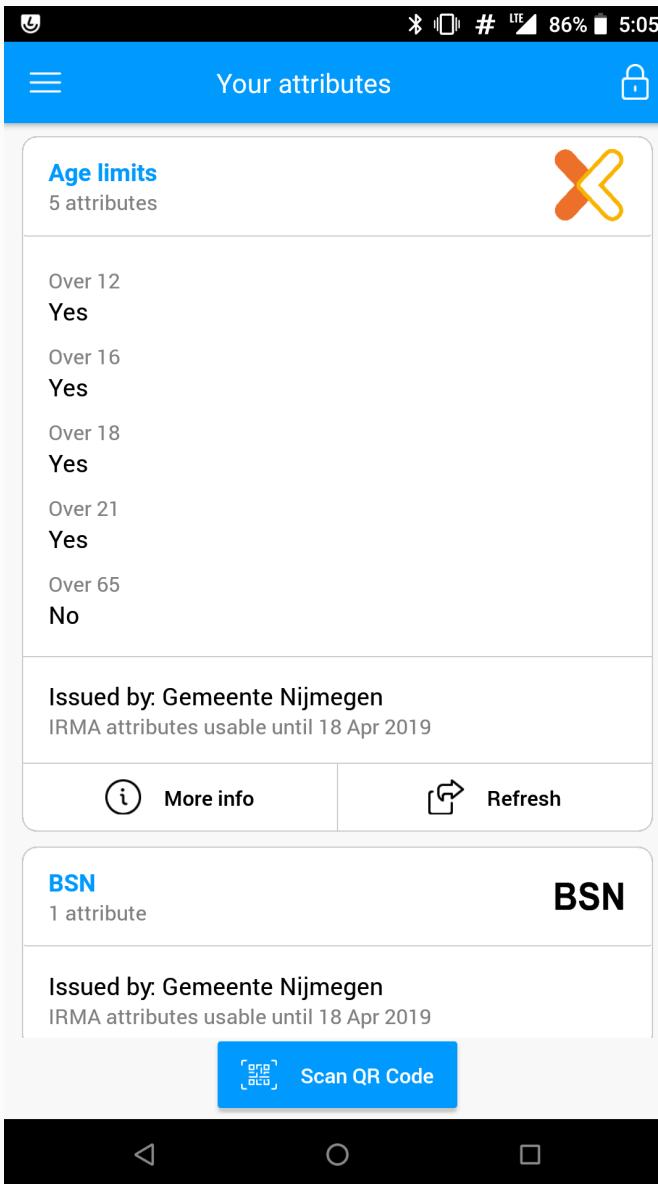
Sietse Ringers

Tomas Harreveld

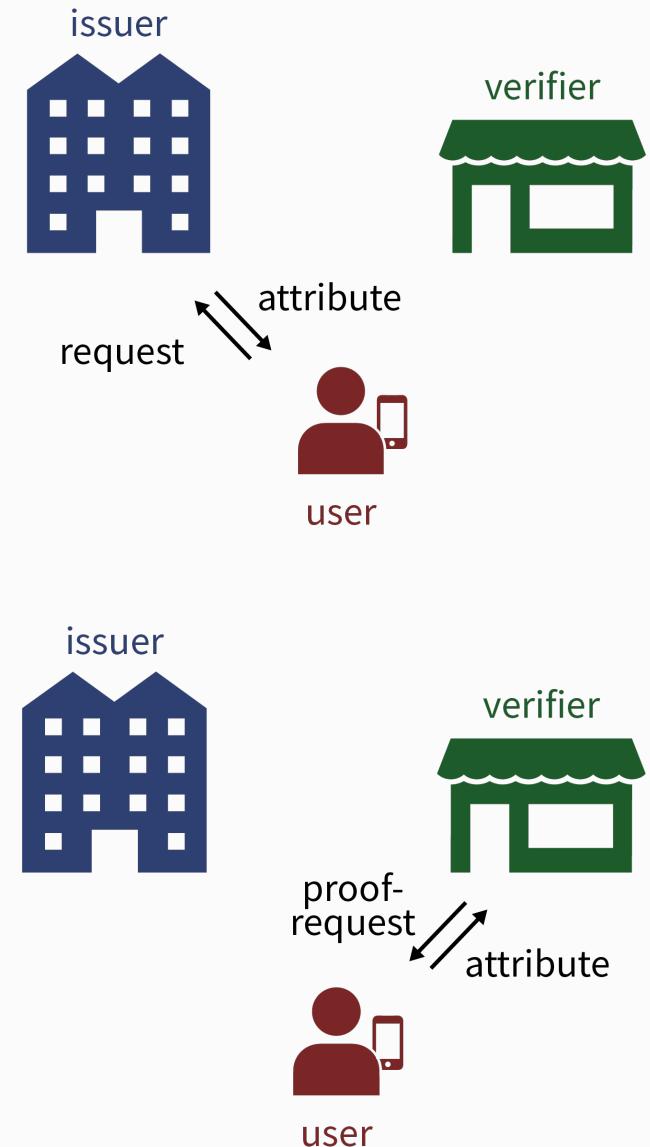
Privacy by Design Foundation

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 software



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
evelopment verbosity=debug version=0.3.0
[2019-07-03T15:06:08+02:00] INFO No configuration file foun
d
```

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

The image displays two screenshots of the IRMA mobile application interface, illustrating the evolution of attribute disclosure options.

Screenshot 1 (Left): Shows a list of attributes under the heading "localhost asks you to disclose the following attributes:". It includes:

- Root**: Issued by: DemoVerheid.nl. Options: BSN (12345) and Demo Address.
- Demo Address**: Issued by: Demo Gemeente Nijmegen. Options: Street (Toernooiveld), House number (212), and City (Nijmegen).

At the bottom are "Refuse" and "Accept" buttons.

Screenshot 2 (Right): Shows a more detailed view of the "Demo Address" disclosure screen. It includes:

- Address**:
 - Demo Address**: Issued by: Demo Gemeente Nijmegen. Options: Street (Toernooiveld).
- City**:
 - iDIN demo**: Issued by: Demo iDIN. Options: City (Nijmegen).

At the bottom are "Refuse" and "Accept" buttons.

A blue arrow points from the left screenshot to the right screenshot, indicating the progression from a general set of attributes to a detailed 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

The image displays two screenshots of the IRMA mobile application interface, connected by a blue arrow pointing from the left screen to the right screen.

Left Screen (1:00 PM): The title is "Disclose attributes". It shows a message: "localhost asks you to disclose the following attributes:". Below this, there is a "Root" node with "BSN 12345" and an "IRMA" logo. A "Demo Address" node is expanded, showing "Street Toernooiveld", "House number 212", and "City Nijmegen". This node also has an "IRMA" logo. At the bottom, there are "Refuse" and "Accept" buttons.

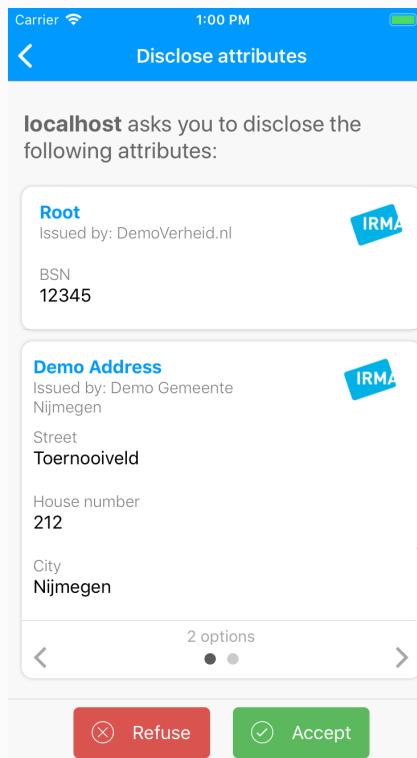
Right Screen (4:18 PM): The title is "Disclose attributes". It shows a message: "localhost asks you to disclose the following attributes:". Below this, there are two sections: "Address" and "City". The "Address" section contains a "Demo Address" node with "Street Toernooiveld", "House number 212", and "City Nijmegen", along with an "IRMA" logo. The "City" section contains an "iDIN demo" node with "City Nijmegen" and an "iDIN" logo. Both sections have "2 options" indicated at the bottom. At the bottom, there are "Refuse" and "Accept" buttons.

Releasing ‘condiscon’

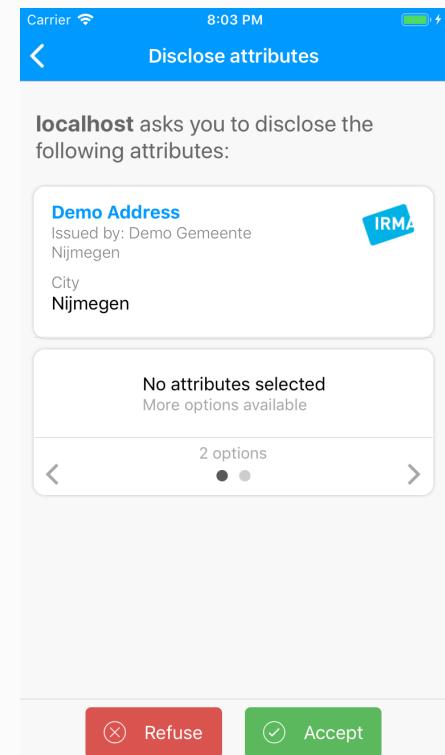


More flexible attribute requests for IRMA verifiers

- 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



This image shows a screenshot of a software application interface for managing a roadmap and issue tracker. The interface is divided into several sections: a top navigation bar, a search/filter bar, a left sidebar with a tree view, and a main content area with a grid of cards.

The top navigation bar includes links for 'Dashboard', 'Issues', 'Stories', 'Merge', 'Planning', 'Reports', and 'Search'. The search/filter bar contains fields for 'Search or filter results...' and 'Status' (with options 'Open', 'In Progress', 'Completed', and 'Blocked'). On the right side of the search bar are 'REFRESH' and 'SEARCH' buttons.

The left sidebar features a tree view with nodes like 'Roadmap', 'Issues', 'Stories', 'Merge', 'Planning', 'Reports', and 'Search'. Below this is a section titled 'Planning' with a tree view of 'Planning' categories.

The main content area displays a grid of cards, each representing a task or feature. The cards are organized into columns by status: Open (orange), In Progress (blue), Completed (green), and Blocked (red). Each card includes a title, a brief description, and a progress bar indicating completion status. The cards are arranged in a grid format, with some cards having a larger height than others.

Category	Task Description	Status	Progress (%)
Planning	Refactor codebase and migrate legacy parts	Open	20%
	Integrate AI-powered forecasting module	In Progress	40%
	Optimize user interface for mobile devices	Completed	100%
	Develop real-time reporting system for stakeholders	Blocked	0%
	Introduce AI-driven prediction models for market trends	Open	10%
	Refactor database schema to support new requirements	In Progress	30%
	Enhance security protocols for sensitive data	Completed	100%
	Implement AI-based recommendation engine	Blocked	0%
	Develop machine learning model for fraud detection	Open	5%
	Refactor codebase for better readability and maintainability	In Progress	25%
Issues	Fix critical bug in production environment	Open	10%
	Address performance issues in legacy system	In Progress	30%
	Integrate AI-powered monitoring tool	Completed	100%
	Refactor codebase for better readability and maintainability	Blocked	0%
	Address performance issues in legacy system	Open	5%
	Integrate AI-powered monitoring tool	In Progress	25%
	Refactor codebase for better readability and maintainability	Completed	100%
	Address performance issues in legacy system	Blocked	0%
	Integrate AI-powered monitoring tool	Open	10%
	Refactor codebase for better readability and maintainability	In Progress	30%
Stories	Refactor codebase and migrate legacy parts	Open	20%
	Integrate AI-powered forecasting module	In Progress	40%
	Optimize user interface for mobile devices	Completed	100%
	Develop real-time reporting system for stakeholders	Blocked	0%
	Introduce AI-driven prediction models for market trends	Open	10%
	Refactor database schema to support new requirements	In Progress	30%
	Enhance security protocols for sensitive data	Completed	100%
	Implement AI-based recommendation engine	Blocked	0%
	Develop machine learning model for fraud detection	Open	5%
	Refactor codebase for better readability and maintainability	In Progress	25%
Merge	Refactor codebase and migrate legacy parts	Open	20%
	Integrate AI-powered forecasting module	In Progress	40%
	Optimize user interface for mobile devices	Completed	100%
	Develop real-time reporting system for stakeholders	Blocked	0%
	Introduce AI-driven prediction models for market trends	Open	10%
	Refactor database schema to support new requirements	In Progress	30%
	Enhance security protocols for sensitive data	Completed	100%
	Implement AI-based recommendation engine	Blocked	0%
	Develop machine learning model for fraud detection	Open	5%
	Refactor codebase for better readability and maintainability	In Progress	25%
Reports	Refactor codebase and migrate legacy parts	Open	20%
	Integrate AI-powered forecasting module	In Progress	40%
	Optimize user interface for mobile devices	Completed	100%
	Develop real-time reporting system for stakeholders	Blocked	0%
	Introduce AI-driven prediction models for market trends	Open	10%
	Refactor database schema to support new requirements	In Progress	30%
	Enhance security protocols for sensitive data	Completed	100%
	Implement AI-based recommendation engine	Blocked	0%
	Develop machine learning model for fraud detection	Open	5%
	Refactor codebase for better readability and maintainability	In Progress	25%
Search	Refactor codebase and migrate legacy parts	Open	20%
	Integrate AI-powered forecasting module	In Progress	40%
	Optimize user interface for mobile devices	Completed	100%
	Develop real-time reporting system for stakeholders	Blocked	0%
	Introduce AI-driven prediction models for market trends	Open	10%
	Refactor database schema to support new requirements	In Progress	30%
	Enhance security protocols for sensitive data	Completed	100%
	Implement AI-based recommendation engine	Blocked	0%
	Develop machine learning model for fraud detection	Open	5%
	Refactor codebase for better readability and maintainability	In Progress	25%

Continuous integration met Gitlab



- Richting:
 - Signed commits en releases
 - Reproducible builds

The screenshot shows the GitLab Pipelines interface for the project 'irmao'. The top navigation bar includes links for Projects, Groups, More, and a search bar. The sidebar on the left has icons for Home, Pipeline, Triggerer, Commit, and Settings.

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 Laden

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": [  
      "pbdf.nijmegen.personalData.fullname"  
    ]  
  }]
```



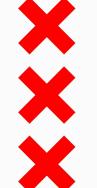
```
{  
  "type": "disclosing",  
  "content": [{  
    "label": "Volledige naam",  
    "attributes": [  
      "pbdf.nijmegen.personalData.fullname",  
      "pbdf.gemeente.personalData.fullname",  
    ]  
  }]
```



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



„CONSUL

Free software for citizen participation.

The background features a stylized illustration of a city skyline with various buildings, trees, and clouds. In the foreground, there is a group of diverse people standing together. The word "CONSUL" is repeated at the bottom of the slide.



Log in

Log in via:



Toegang milieustation Gemeente Den Bosch



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



Gemeente Buren IRMA Wordpress-plugin



Gemeente Buren

Home Nieuws De gemeente Contact



14 0344

[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

