Manual

IRMA authentication PoC

for GIDS

Introduction

This short manual describes how to use the IRMA authentication Proof of Concept (PoC) in order for integration into your own platform.

Goal

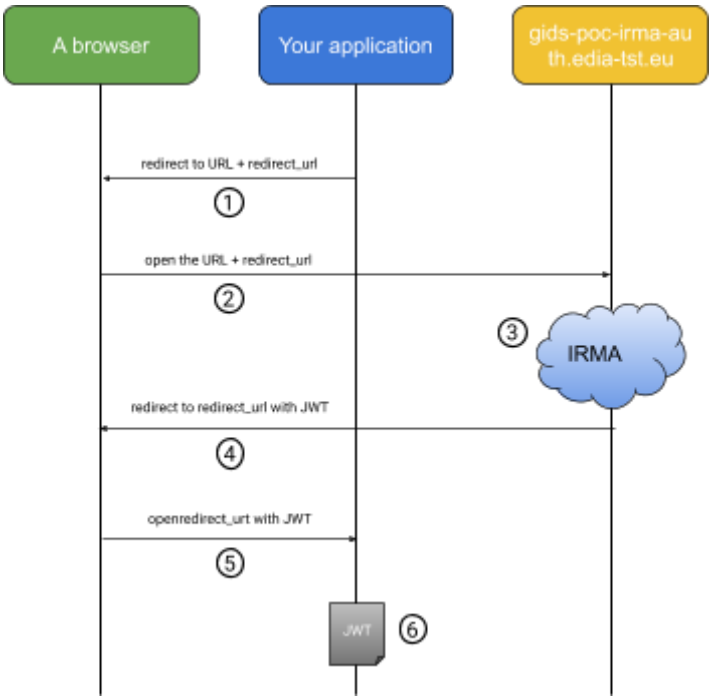
The goal of this component is to abstract the IRMA "implementation complexity" away from other applications in the PoC. I quote "implementation complexity" because in my experience integrating IRMA is not very complex, however, one need to understand some core concepts that demand some attention.

Architecture and workflow

The architecture is described in the figure below and consists of the following workflow:

1. Your application redirects the client browser to the GIDS IRMA PoC implementation with the redirect_uri parameter in an URL.
2. The browser opens the URL
3. The GIDS IRMA PoC does the IRMA magic
4. The GIDS IRMA PoC redirects the client browser to the redirect_uri with a JWT token in the parameters
5. The browser opens the redirect_uri with the JWT token
6. Your application decodes the JWT token and authenticates the user with the subject (sub) in

the JWT token.



The launch (step 1)

The launch has the following format:

`https://gids-irma-auth.edia-tst.eu/?redirect_uri=<REDIRECT_URL>`

Where REDIRECT_URL should be replaced with the URL the GIDS IRMA PoC should redirect to.

Example:

https://gids-poc-irma-auth.edia-tst.eu/?redirect_uri=https://www.minddistrict.com/auth/jwt

The IRMA authentication (step 3)

Prerequisites

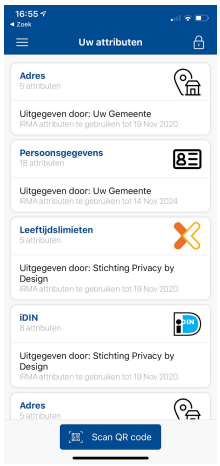
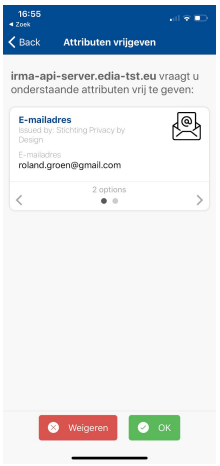
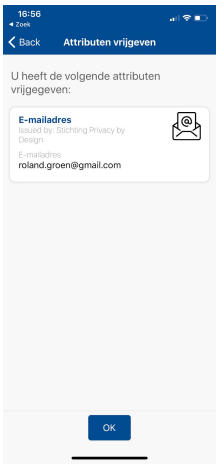
In order to identify yourself with the IRMA attribute, email in this case, you need install the IRMA application and add an email address to your IRMA app:

- Install the IRMA app on your mobile device. There are no desktop implementatins of IRMA.
- Navigate your browser to the following URL, this may be your desktop browser: https://privacybydesign.foundation/uitgifte/email and follow the steps to add the email attribute to your IRMA application

Steps to authenticate

Step a: Open the IRMA Application

Step 2b: scan the code:

Click on “QR code”	Scan the QR code	Accept the attribute	Confirmation
			

Step c: the browser application now automatically redirects to the redirect_uri with the JWT token.

The JWT Token (Step 6)

The JWT token you’ll receive with contain the following information

- The issuing date (iat)
- The expiry date (exp)
- The issuer (‘gids-irma-demo’)
- The subject (sub)

Example token:

On jwt.io

Encoded:

```
eyJhbGciOiJSUzI1NiJ9.eyJpYXQiOjE1Nzg2NzI0OTAsImV4cCI6MTU3ODY3Mjc5MCwiaXNzIjoiZ2lkcy1pcm1hLWRlbW8iLCJzdWIiOiJyb2xhbmQuZ3JvZW5AZ21haWwuY29tIn0.oJLfWqb6OpQfGwa_r9m4atMQI5XYl6ghEONTmkPhFvyJpp4UgxM3VAiUpzfmpQifLmfhi_K889pNYAQ1E8I-ZgJVZNWnO5JIu3NTL7qA6PruZTM2PWOvyAd3eU--xhgPjHEZgbXDVJwyzTuCn43RRx-gEgOM61GF18v5LsaZfki9Ww-A0EG9DPTzYFY3HR4kljEQcOGNgi_PJp9Le46huk_VAVia7H8SEc3Q9us6FdHjviVb18xHCwgIzRVF-VdsTMqQMlAJgcFywI-ZxPrzbrtQ9zMe654cbyOkkIrR3GvPFXhAxYWUYuAeTkY0IyNCN-a3IvmvmaCsGqkAog
```


Decoded:


```
{
  "iat": 1578672490,
  "exp": 1578672790,
  "iss": "gids-irma-demo",
  "sub": "roland.groen@gmail.com"
}
```


The JWT validation

In the case of a PoC the validation of the JWT might not have the highest priority, however, in some libraries it might be harder to implement JWT without validation. The public key of the JWT token encoded in BASE64 is displayed below.


```
-----BEGIN PUBLIC KEY-----
MIIBHjANBgkqhkiG9w0BAQEFAAOCAQsAMIIBBgKB/gC+0zqjfI2zKvvjwUwE4JiL
YyUqazpxWD+hmyLCEXgzfbHIWvwRD54M8PJqCt+9Iq3PBIvpZoJezQ5rztEWN6OI
7qoXq4ygZ4YTXGU+ErfqLlvyMv/PfbuHU7oRS+4W0iq2mPwQQXSKMDJz4qSORa75
p6xMMHd38xJgHQ6tBwPFMbwhpGsGpCFpxRqlMR735D8gRbhFbSexxMhbyqpQTro0
u6xPFoAecldiCJ8KNlp2/NNcRgMZKVIU3rwhp52JcnI90by8UZoD0ItlRoXdaBmm
QORWRrm2SC1rRu+KFidzjxe2cRiFVXqthqe1Ttm29atUeVftJhEgb7UpxKJPAgMB
AAE=
-----END PUBLIC KEY-----
```


Setting the attribute

By default, the email IRMA attribute is used (pbdf.pbdf.email.email). To experiment with other attributes, the service can request other attributes. This is can be done by setting the attribute in the initial URL.

`https://gids-poc-irma-auth.edia-tst.eu/?redirect_uri=<REDIRECT_URL>&attribute=<ATTRIBUTE>`

Example:

```
https://gids-poc-irma-auth.edia-tst.eu/?redirect_uri=https://www.minddistrict.com/auth/jwt&attribute=pbdf.pbdf.email.email
```

The full list of attributes is as follows.

```
pbdf.nuts.agb.agbcode
pbdf.ivido.login.identifier
pbdf.chipsoft.bsn.bsn
pbdf.chipsoft.bsn.initials
pbdf.chipsoft.bsn.firstnames
pbdf.chipsoft.bsn.prefix
pbdf.chipsoft.bsn.familyname
pbdf.chipsoft.bsn.dateofbirth
pbdf.chipsoft.testbsn.bsn
pbdf.chipsoft.testbsn.initials
pbdf.chipsoft.testbsn.firstnames
pbdf.chipsoft.testbsn.prefix
pbdf.chipsoft.testbsn.familyname
pbdf.chipsoft.testbsn.dateofbirth
pbdf.surf.secureid.secureid
pbdf.surf.secureid.environment
pbdf.surf.surfdrive.eppn
pbdf.surf.surfdrive.emailadres
pbdf.surf.surfdrive.displayname
pbdf.sidn-pbdf.irma.pseudonym
pbdf.gebiedonline.workingarea.zipcode
pbdf.gebiedonline.workingarea.district
pbdf.gebiedonline.workingarea.city
pbdf.gebiedonline.livingarea.zipcode
pbdf.gebiedonline.livingarea.district
pbdf.gebiedonline.livingarea.city
pbdf.gebiedonline.useridentification.logincode
pbdf.pbdf.twitter.username
pbdf.pbdf.twitter.fullname
pbdf.pbdf.twitter.email
pbdf.pbdf.twitter.profileurl
pbdf.pbdf.idin.initials
pbdf.pbdf.idin.familyname
pbdf.pbdf.idin.dateofbirth
pbdf.pbdf.idin.gender
pbdf.pbdf.idin.address
pbdf.pbdf.idin.zipcode
pbdf.pbdf.idin.city
pbdf.pbdf.idin.country
pbdf.pbdf.idin.over12
pbdf.pbdf.idin.over16
pbdf.pbdf.idin.over18
pbdf.pbdf.idin.over21
pbdf.pbdf.idin.over65
pbdf.pbdf.mijnirma.email
pbdf.pbdf.big.bignumber
pbdf.pbdf.big.startdate
pbdf.pbdf.big.profession
pbdf.pbdf.big.specialism
```

```
pbdf.pbdf.mobilenumber.mobilenumber
pbdf.pbdf.ideal.fullname
pbdf.pbdf.ideal.iban
pbdf.pbdf.ideal.bic
pbdf.pbdf.irmatube.type
pbdf.pbdf.irmatube.id
pbdf.pbdf.facebook.fullname
pbdf.pbdf.facebook.firstname
pbdf.pbdf.facebook.familyname
pbdf.pbdf.facebook.email
pbdf.pbdf.facebook.dateofbirth
pbdf.pbdf.ageLimits.over12
pbdf.pbdf.ageLimits.over16
pbdf.pbdf.ageLimits.over18
pbdf.pbdf.ageLimits.over21
pbdf.pbdf.ageLimits.over65
pbdf.pbdf.diploma.firstname
pbdf.pbdf.diploma.prefix
pbdf.pbdf.diploma.familyname
pbdf.pbdf.diploma.dateofbirth
pbdf.pbdf.diploma.gender
pbdf.pbdf.diploma.education
pbdf.pbdf.diploma.degree
pbdf.pbdf.diploma.profile
pbdf.pbdf.diploma.achieved
pbdf.pbdf.diploma.institute
pbdf.pbdf.diploma.city
pbdf.pbdf.surfnet.institute
pbdf.pbdf.surfnet.type
pbdf.pbdf.surfnet.id
pbdf.pbdf.surfnet.fullname
pbdf.pbdf.surfnet.firstname
pbdf.pbdf.surfnet.familyname
pbdf.pbdf.surfnet.email
pbdf.pbdf.surfnet-2.institute
pbdf.pbdf.surfnet-2.type
pbdf.pbdf.surfnet-2.id
pbdf.pbdf.surfnet-2.fullid
pbdf.pbdf.surfnet-2.fullname
pbdf.pbdf.surfnet-2.firstname
pbdf.pbdf.surfnet-2.familyname
pbdf.pbdf.surfnet-2.email
pbdf.pbdf.email.email
pbdf.pbdf.email.domain
pbdf.pbdf.linkedin.fullname
pbdf.pbdf.linkedin.firstname
pbdf.pbdf.linkedin.familyname
pbdf.pbdf.linkedin.email
pbdf.pbdf.linkedin.profileurl
pbdf.vgz.machtiging.clientnumber
pbdf.vgz.machtiging.clientfullname
pbdf.vgz.machtiging.mandateid
pbdf.gemeente.personalData.initials
pbdf.gemeente.personalData.firstnames
pbdf.gemeente.personalData.prefix
pbdf.gemeente.personalData.familyname
pbdf.gemeente.personalData.fullname
```

```
pbdf.gemeente.personalData.gender
pbdf.gemeente.personalData.nationality
pbdf.gemeente.personalData.surname
pbdf.gemeente.personalData.dateofbirth
pbdf.gemeente.personalData.cityofbirth
pbdf.gemeente.personalData.countryofbirth
pbdf.gemeente.personalData.over12
pbdf.gemeente.personalData.over16
pbdf.gemeente.personalData.over18
pbdf.gemeente.personalData.over21
pbdf.gemeente.personalData.over65
pbdf.gemeente.personalData.bsn
pbdf.gemeente.personalData.digidlevel
pbdf.gemeente.address.street
pbdf.gemeente.address.houseNumber
pbdf.gemeente.address.zipcode
pbdf.gemeente.address.municipality
pbdf.gemeente.address.city
```