

“State of the IRMA”

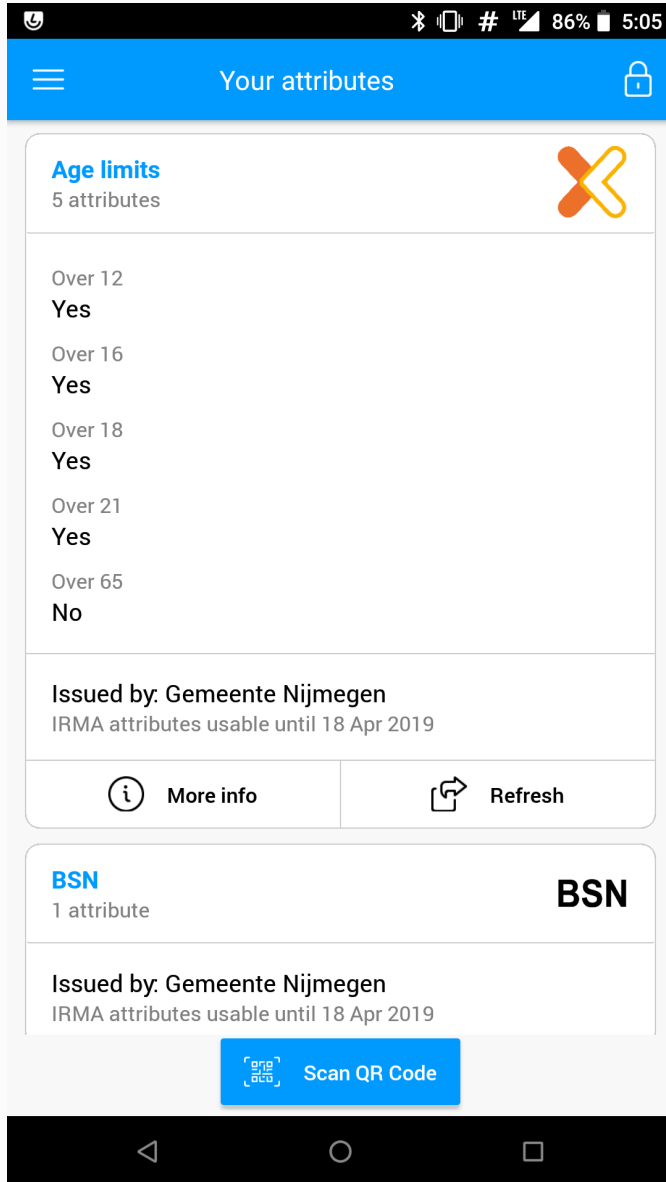
Latest IRMA developments

Sietse Ringers, Tomas Harreveld

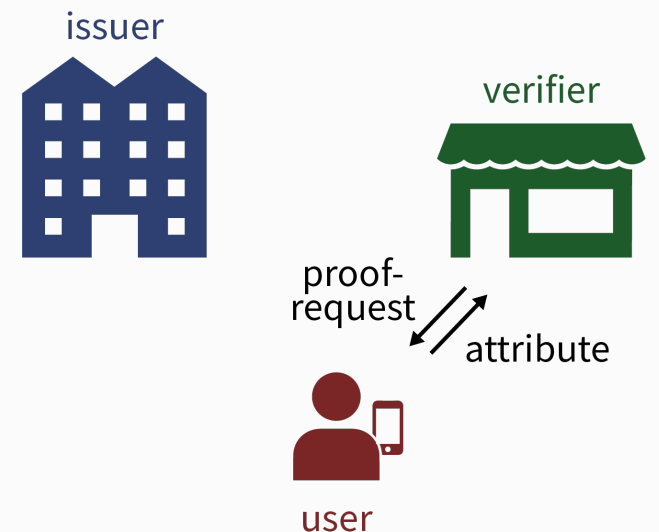
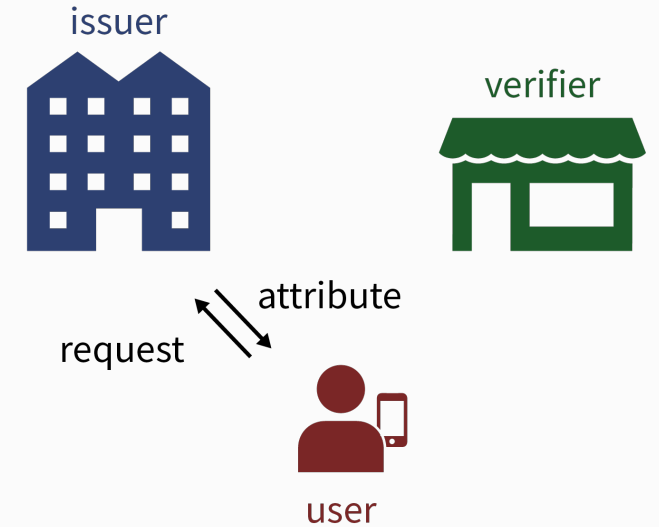
Privacy by Design Foundation

November 29, 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



Revocation



- Issuer can revoke individual previously issued credentials
- Effective instantaneously (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For each credential, the IRMA app includes a new zero-knowledge proof that the credential has not been revoked: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“This credential has not been revoked”

Revocation: how it works



- Issuance
 - Issuer gets 'nonrevocation public key'
 - Issuer gives 'nonrevocation witness' along with credential to IRMA app
- Disclosure
 - Verifier requests nonrevocation proof for a credential
 - App proves nonrevocation in zero knowledge using its witness against current nonrevocation public key
- Revocation
 - Issuer computes new nonrevocation public key & broadcasts update message
 - Apps update their nonrevocation witnesses
 - App with revoked credential cannot update its witness

Revocation: session requests



Issuance

```
{
  "@context": "https://irma.app/ld/request/issuance/v2",
  "credentials": [
    {
      "credential": "irma-demo.MijnOverheid.root",
      "attributes": { "BSN": "299792458" },
      "revocationKey": "12345"
    }
  ]
}
```

Revocation

```
{
  "@context": "https://irma.app/ld/request/revocation/v1",
  "type": "irma-demo.MijnOverheid.root",
  "key": "12345"
}
```

Disclosure

```
{
  "@context": "https://irma.app/ld/request/disclosure/v2",
  "disclose": [[[ "irma-demo.MijnOverheid.root.BSN" ]]],
  "revocation": [ "irma-demo.MijnOverheid.root" ]
}
```

Revocation: properties



Relatively expensive for app

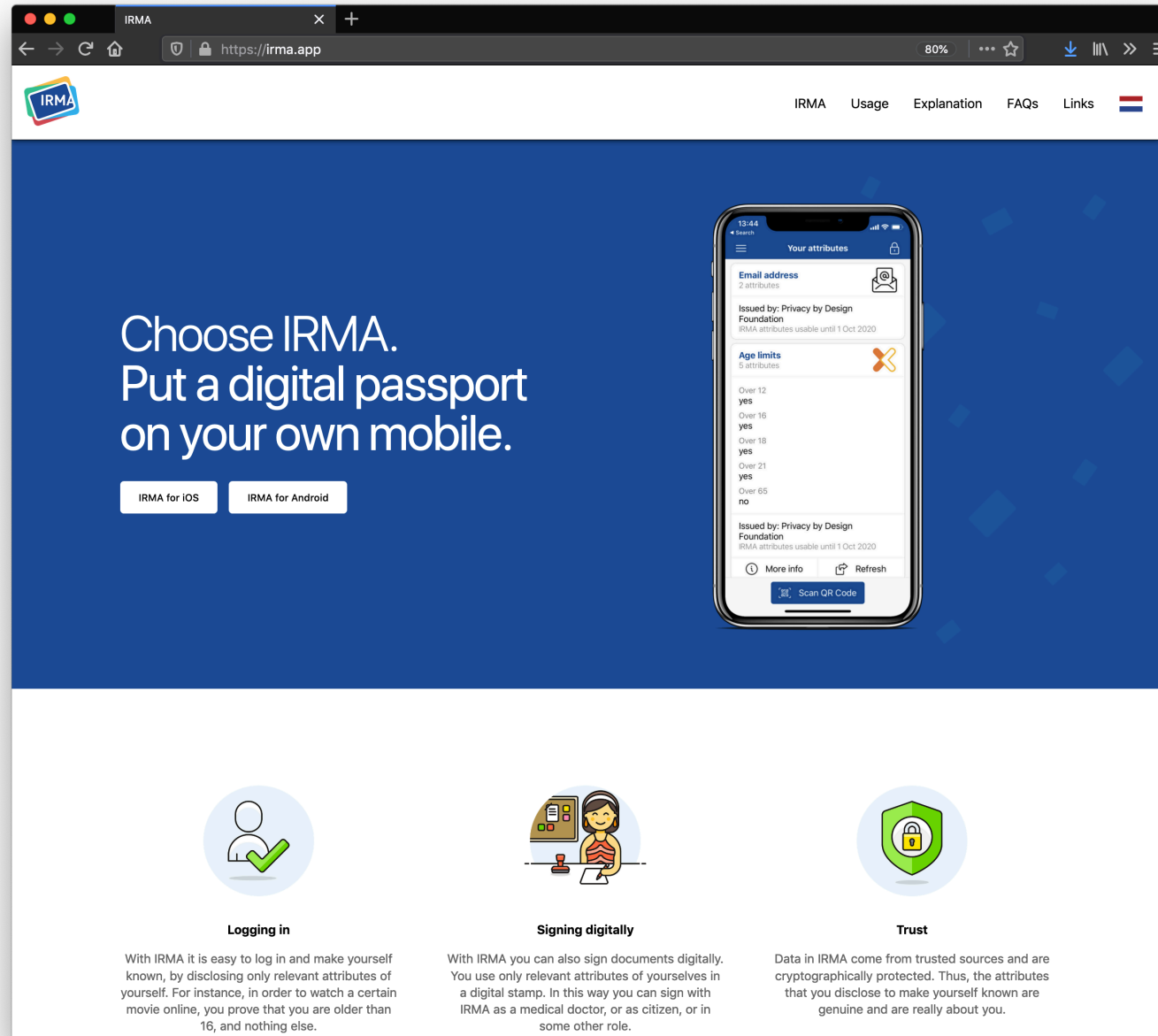
- Not enabled by default in credential types
- App proves nonrevocation only if verifier explicitly asks for it

App requires all update messages to update its witness

- Verifier includes latest update messages in session request

Consequences for:

- App → your credential can get revoked
- Verifiers → can ask for nonrevocation proofs
- Issuers → store revocation keys and update messages in database
→ must permanently host update messages



The screenshot shows the IRMA website in a browser. The main heading reads "Choose IRMA. Put a digital passport on your own mobile." Below this are buttons for "IRMA for iOS" and "IRMA for Android". A smartphone displays the app's "Your attributes" screen, which lists "Email address" (2 attributes), "Age limits" (5 attributes), and "Issued by: Privacy by Design Foundation". The age limits are: Over 12 (yes), Over 16 (yes), Over 18 (yes), Over 21 (yes), and Over 65 (no). At the bottom, three icons represent "Logging in", "Signing digitally", and "Trust", each with a short explanatory paragraph.

Logging in

With IRMA it is easy to log in and make yourself known, by disclosing only relevant attributes of yourself. For instance, in order to watch a certain movie online, you prove that you are older than 16, and nothing else.

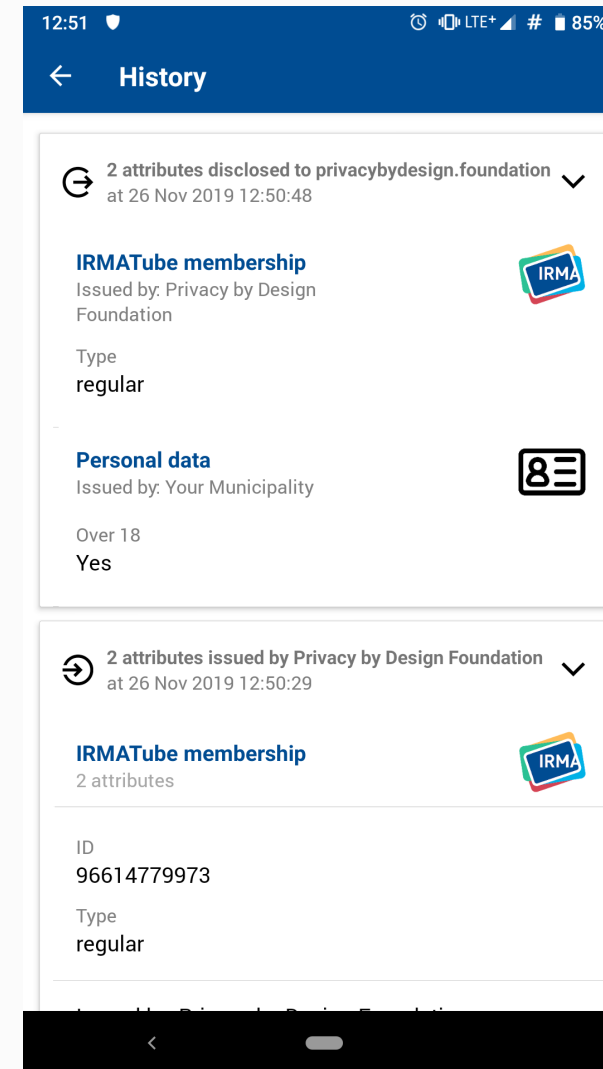
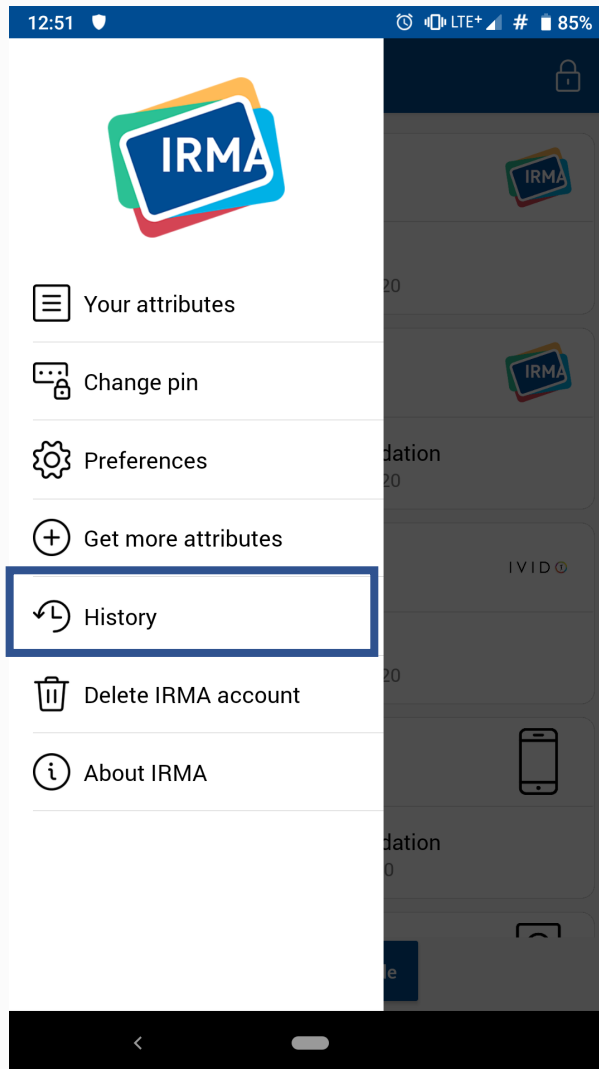
Signing digitally

With IRMA you can also sign documents digitally. You use only relevant attributes of yourselves in a digital stamp. In this way you can sign with IRMA as a medical doctor, or as citizen, or in some other role.

Trust

Data in IRMA come from trusted sources and are cryptographically protected. Thus, the attributes that you disclose to make yourself known are genuine and are really about you.

Attribute usage history in IRMA app



- Verifier authentication: pretty names in IRMA app
- iDEAL attribute issuer
- Keyshare server rewrite in Go
- New irmajs
- Verifiable credential standard
- Language bindings
 - Swift, C#, Ruby, Python

More information



- Website:
<https://irma.app>
<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

