IRMA - I Reveal My Attributes

Attribute-based Authentication and Signatures in Practice

Joost van Dijk, Bart Jacobs, Sietse Ringers - TNC 2018
Contents

• IRMA intro
• IRMA vs SAML vs X.509
• From smart card to smart phone
• Demo
• Attribute-based electronic signatures
• Obtaining attributes
What is IRMA?
IRMA is about Attributes

- IRMA: *I reveal my attributes*
- Attributes can be identifying (*name, SSN*) or not (*over 18, citizen of Trondheim*)
- Decentralised
  - Digitally signed by *issuers*
  - Collected by user
  - Disclosed to *verifiers*
eduTEAMS Membership Management Service | GÉANT requires your information before logging in.

The service needs the following information to function properly. These data will be transmitted securely from your institution towards eduTEAMS Membership Management Service | GÉANT.

The following information will be shared with eduTEAMS Membership Management Service | GÉANT:

- **Display Name**: Joost van Dijk
- **Full Name**: Joost van Dijk
- **First name**: Joost
- **Surname**: van Dijk
- **Email address**: joost.vandijk@surfnet.nl
- **Institution user ID**: joi@surfnet.nl

Do you agree with sharing this data?

- **Yes, proceed to eduTEAMS Membership Management Service | GÉANT**
- **No, I do not agree**

You are using 139 services via SURFconext. View the list of services and your groups.
LET'S SEE SOME I.D.

PLEASE TELL US YOUR LOCATION & DATE OF BIRTH

NETHERLANDS  DD  MM  YY

LOG IN WITH FACEBOOK

BY SUBMITTING THIS FORM, YOU AGREE TO THE PRIVACY AND COOKIE POLICY OF THIS WEBSITE. THIS WEBSITE WILL MAKE USE OF COOKIES. TO LEARN MORE, PLEASE READ OUR PRIVACY AND COOKIE POLICY.
Heineken Social Connect will receive:
your public profile and birthday.

Edit This

Continue as Joost

Cancel

This doesn't let the app post to Facebook

App Terms · Privacy Policy
IRMA is about privacy

- Based on Idemix (IBM Research Zürich)
- Uses advanced crypto to achieve desirable privacy properties:
  - Selective disclosure
  - Non-transferability
  - Issuer unlinkability
  - Multi-show unlinkability
J.P. van Dijk

Issued by: TERENA Personal CA 3
Expires: Monday, 9 September 2019 at 14:00:00 Central European Summer Time
✔ This certificate is valid

Trust

Details

Subject Name
Country NL
State/Province Noord Holland
Locality Amsterdam
Organization Stichting Hogeschool Van Amsterdam
Common Name J.P. van Dijk

Issuer Name
Country NL
State/Province Noord-Holland
Locality Amsterdam
Organization TERENA
Common Name TERENA Personal CA 3

Serial Number 0D E3 C6 D9 DC EF 9F A5 3C F7 68 CC 89 16 95 F6
Version 3
Extension Authority Key Identifier (2.5.29.35)
Critical NO

Key ID F0 21 E9 49 77 73 9F 85 AE 18 3B E8 52 70 14 06 ED 42 EE CA

Extension Subject Alternative Name (2.5.29.17)
Critical NO
RFC 822 Name j.p.van.dijk@hva.nl

Extension Certificate Policies (2.5.29.32)
Critical NO
Policy ID #1 2.16.840.1.114412.4.1.2
Qualifier ID #1 Certification Practice Statement (1.3.6.1.5.5.7.2.1)
CPS URI https://www.digicert.com/CPS

Extension CRL Distribution Points (2.5.29.31)
Critical NO
URI http://crl3.digicert.com/TERENAPersonal/CA3.crl
URI http://crl4.digicert.com/TERENAPersonal/CA3.crl
IdP-centric:

![Diagram showing the IdP-centric model](image)

User-centric:

![Diagram showing the User-centric model](image)
Decentral

- No central IdP
- Attributes stored in app, not with an IdP
- Attributes tied to mobile phone and to one another through personal secret key

To achieve these properties, the technologies rely on novel cryptographic techniques such as blind signatures and zero-knowledge proofs. The most important concept in IRMA is that of credentials. Credentials form a set of coherent attributes released by a single issuer. The structure of a credential is shown in Figure 1.

Figure 1 - IRMA credential

As the figure shows, a credential consists of three key elements:

- A secret key that is used to ensure that credentials are non-transferable (cannot be copied from the card)
- The attributes associated with the credential
- A digital signature by the issuer of the credential, vouching for the authenticity of the attributes

Examples of credentials are:

- An address credential, containing attributes for the country, city, street number, and postal code of the card holder
- An age verification credential, containing attributes that certify that the user is, e.g., over 16, over 18, over 21, and under 30.

Any subset of attributes from a credential can be released upon approval by the user (this is called “selective disclosure”). Also, attributes from multiple credentials can be released simultaneously, for instance, the “country” attribute from the first example above could be combined with the “over 18” attribute from the other example to create a privacy-friendly “wijtpas” under the condition that the country is “NL.”

Two more important properties of the IRMA card are issuer-unlinkability (the issuer of a credential cannot track where, when, and which attributes were released by a user) and multi-show-unlinkability (service providers cannot collude to build a profile on the user by comparing attributes released by the user to trace them).

We are currently (Fall of 2012) working on a pilot of this technology, where students of a research master track in Digital Security (called the Kerckhoffs’ Master) are issued a smart card with the IRMA application installed. The smart card is issued with a base credential on it with attributes from our identity federation (SURFconext) and the students can obtain additional attributes from, for example, the Kerckhoffs’ Master program to indicate that they are a student of said program. The physical smart card body will not contain any identifying information other than a photo printed on the front to prove that the person using the card is the legitimate owner when the card is used in an offline scenario (see Figure 2 below for an example of what the card looks like).

Figure 2 - Example IRMA card with user photo printed on the front

1 The “wijtpas” is an ID that allows Dutch citizens over 18 to legally purchase soft drugs from the infamous “Coffee Shops.”
## Comparison

<table>
<thead>
<tr>
<th></th>
<th>SAML/OIDC</th>
<th>X.509</th>
<th>IRMA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Centricity</strong></td>
<td>IdP centric</td>
<td>User centric</td>
<td>User centric</td>
</tr>
<tr>
<td><strong>Attribute Disclosure</strong></td>
<td>Selective</td>
<td>All-or-nothing</td>
<td>Selective</td>
</tr>
<tr>
<td><strong>Identifier Scope</strong></td>
<td>Directed Identity</td>
<td>Global Identity</td>
<td>Directed Identity</td>
</tr>
</tbody>
</table>
From smart card to smart phone
Keeping secrets

- Split secret between app and Keyshare server
- Multiparty computation using Keyshare protocol
- MyIRMA (revocation)

- Keyshare server
  - never sees any attributes
  - never sees to whom attributes are disclosed
Please enter your IRMA PIN

To use your attributes, you need to enter your IRMA PIN.
Attribute-based electronic signatures
• Idea: In the challenge/response mechanism, let the (hash of a) message be the challenge

• Attach your IBAN attribute to “I donate €10,- to Privacy by Design Foundation”

• Signature demo application https://github.com/privacybydesign/irma_signature_app
Getting attributes

• Overview of all attributes: https://privacybydesign.foundation/attribute-index/en/
• Issuers:
  – PrivacyByDesign Foundation https://privacybydesign.foundation/issuance/
  – SURFnet (multi-factor authentication)
  – Municipality of Nijmegen (soon)
• Attribute sources:
  – iDIN (Bank ID),
  – Social IDs (Facebook, LinkedIn, etc)
  – BIG (register of professionals in individual health care)
  – Edugain
Disclosing attributes

– SURFconext IRMA Guest IdP
– SURFsecureID 2nd factor authentication
– <your application here>
DIY

- **irma_mobile**
  IRMA mobile app (iOS/Android)

- **irma_js**
  IRMA JS library for website integration

- **irma_api_server**
  IRMA API server for issuing/verification of attributes
Getting attributes: Edugain

https://technical.edugain.org/status
Available eduGAIN attributes

The attributes below can be added to your IRMA app:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Institute</td>
<td>surfnet.nl</td>
</tr>
<tr>
<td>Type</td>
<td>employee</td>
</tr>
<tr>
<td>User ID</td>
<td>jodi</td>
</tr>
<tr>
<td>Full ID</td>
<td><a href="mailto:jodi@surfnet.nl">jodi@surfnet.nl</a></td>
</tr>
<tr>
<td>Full name</td>
<td>Joost van Dijk</td>
</tr>
<tr>
<td>First name</td>
<td>Joost</td>
</tr>
<tr>
<td>Family name</td>
<td>van Dijk</td>
</tr>
<tr>
<td>Email address</td>
<td><a href="mailto:joost.vandijk@surfnet.nl">joost.vandijk@surfnet.nl</a></td>
</tr>
</tbody>
</table>

Click here to add this attributes to your IRMA app.

Load attributes in IRMA app

You are logged in as Joost van Dijk (Log out)
Questions?
Remarks?

Joost.vanDijk@surfnet.nl
http://nl.linkedin.com/in/Joostd

www.creativecommons.org/licenses/by/3.0/nl/deed.en