Attribute-based Authentication and Signatures

Dcypher, Utrecht

Bart Jacobs — Radboud University and Privacy by Design foundation
bart@cs.ru.nl
4 oct. 2017

IRMA Demo

Two key aspects:
▶ attributes instead of identities
▶ decentralised architecture: attributes on users own phone

IRMA history, in two phases

▶ 2008–now: scientific research project at Radboud University
  • active research line on attribute-based authentication
  • 3 PhD theses so far, postdocs too, many publications
  • financial support from: NLnet, Translink, BZK, NWO, KPN
  • prototype implementations on:
    ▶ smart card — at first, but no longer supported
    ▶ smart phone — prototype for Android only

▶ 2016–now: technology deployment via non-profit Foundation
  • https://privacybydesign.foundation set up in fall 2016
  • foundation runs infrastructure, and issues attributes
  • currently from: iDIN (banks), Surfconext (academia), BIG (health)
  • both Android and iOS apps, with common code-base in Go
  • attribute verification pilots are emerging
Example identity services

<table>
<thead>
<tr>
<th>Public</th>
<th>Private</th>
<th>Non-profit</th>
</tr>
</thead>
<tbody>
<tr>
<td>DigiD</td>
<td>Facebook login</td>
<td>SURFconext</td>
</tr>
<tr>
<td>iDensys</td>
<td>iDIN</td>
<td>IRMA</td>
</tr>
</tbody>
</table>

Centralised versus decentralised, schematically

**Centralised**: everything goes via the Identity Provider (think iDIN)

1. User authenticates
2. Identity Provider proves
3. Verifier authenticates

**Decentralised**: everything goes via the User (think IRMA)

1. User issues
2. User proves
3. Verifier proves

Comparing iDIN and IRMA

- **iDIN**
  - operated jointly by banks in NL, based on iDeal
  - wide coverage, based on existing e-banking authentication
  - centralised architecture, with associated privacy concerns
  - payment per authentication (attribute delivery) — expensive
  - fixed number of attributes: name, date-of-birth, address, possibly BSN, but e.g. not bank account nr, email, phone nr ...

- **IRMA**
  - Operated by Privacy by Design foundation
  - decentralised architecture, emphasising self-sovereignty
  - app deployment very limited so far — but may increase quickly
  - verification is free of costs; issuance currently too
  - maximal flexibility of attributes, supporting “persona” concept
  - soon also attribute-based digital signatures, via subscription

Attribute-based signatures

**Idea**:
- personal attributes can be included in digital signature
- eg. a letter is signed by a doctor, lawyer, minister, citizen, etc.
- opens up many new applications, like new digital cheques, with bank account attribute in signature

**IRMA realisation**:
- exists, as prototype implementation “on the command line”
- development of signature ecosystem foreseen in late 2017
- based on ‘signature requests’ that can be sent to someone’s IRMA app for signing
- at first only for “flat text”, later also for “pdf”
IRMA pilots and rollout

- The IRMA app is freely available for everyone
- The foundation issues multiple attributes
  - from iDIN, SURFconext, BIG, email
  - soon also: mobile phone nr, bank account (IBAN+BIC)
  - other options: from Facebook/Google+/Linkedin account
  - the sky is the limit, depending on demand

- Latest effort lies on verification, at merchants (relying parties)
  - since oct’17 available for all SURFconext parties
  - (about 0.5M potential users)
  - pilot being set up in health care, with additional AGB codes
  - strong authentication pilot in preparation at Radboud
  - (your project?)

- Publicity effort is starting only now.

IRMA as societal experiment

Big questions (about situation in NL)

Will IRMA reach broad usage? Which forces work Pro and Contra?

- Contra: support Google’s and Facebook’s etc. not likely
  - they may even fight/obstruct IRMA, when it grows a bigger

- Contra: IRMA’s business model is weak

- Contra: Some attribute management effort on user-side is required

- Pro: Private eID’s have only limited trust
  - providing “source” identity is widely seen as public responsibility

- Pro: NL-Government lacks vision and fails to defend public values

- Pro: IRMA has superior technology, including digital signatures

- Pro: Foundations, like SIDN, can play a trusted strategic IT-role

- Pro: GDPR-regulators could enforce privacy-friendly technology

Main points

- Information flows and authentication requirements determine power relations in modern societies
  - IRMA provides privacy-friendly empowerment of users
  - now organised and run by non-profit foundation

- The choice of authentication architecture is extremely sensitive
  - substantial differences exist between central and decentral
  - power and (financial) control are key in the central approach
  - privacy and autonomy are leading values in the decentralized one
  - What kind of society do we prefer to live in?

- IRMA is a decentralized, open source, non-profit, flexible system that is up and running, and being tested by various parties

- Attribute-based signatures are really cool & innovative
  - strategy: use paid signatures to provide authentication for free

We live in interesting times; thanks for your attention