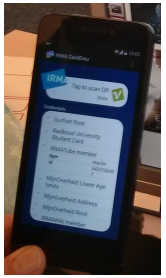
Attribute-based Authentication with IRMA

FJG, Leeuwarden

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

IRMA Demo



Key aspects:

- attributes instead of identities (for user empowerment)
- decentralised architecture: attributes on users own phone (privacy)
- attributes are digitally signed by issuing source (security)

IRMA history, in two phases

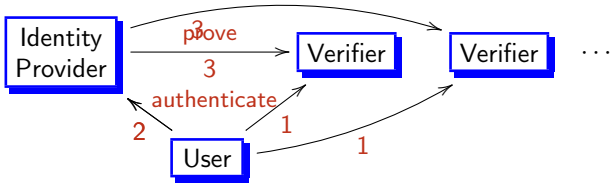
- **2008 – now**: scientific research project at Radboud University
  - active research line on attribute-based authentication
  - 3 PhD theses so far, postdocs too, many publications
  - financial support from: NLnet, Translink, BZK, NWO, KPN
  - prototype implementations on:
    - smart card — at first,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

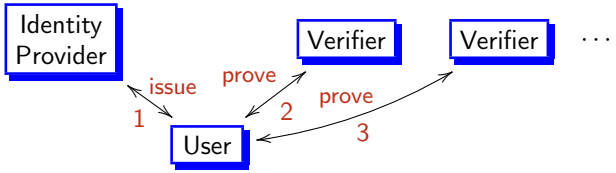
Public	Private	Non-profit
DigiD	Facebook login	SURFconext
~~iDensys~~		
iDIN		
		IRMA

Centralised versus decentralised, schematically

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



Decentralised: everyting goes via the User (think IRMA)



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

Key idea in attribute-based IdM

- Each transaction only requires a **subset** of your attributes for authentication
  - the subset should be small & proportional: data minimisation
  - this also offers some protection against identity fraud
- Typical transactions involve a combination of attributes
  - address + bank account, for online shopping
  - minimal age + bank account for online gambling / XXX / ...
  - "doctor" status + medical registration number for write-access to medical record
- (Pseudonyms are useless for this kind of functionality)
- Attributes give proportional authentication
  - authentication is context-dependent
  - contextual view on privacy, after Helen Nissenbaum
- Very suitable for international deployment
  - abroad they only need to download public keys for verification

Requirements for attribute-based systems

- Non-transferability: my little nephew should not be able to get my "over 18" attribute (and go to XXX sites)
  - realised in IRMA via binding to my private key
- Issuer-unlinkability: the issuers should not be able to track where I use which attribute
  - realised via blind(able) signature
- Multi-show unlinkability: service providers should not be able to connect usage (at different providers)
  - realised via zero-knowledge proofs
- Revocation: rogue attributes (via stolen/lost tokens) should be blockable — or tokens themselves
  - most difficult, partly in conflict with previous requirements
  - possible via short *epochs*, or via external monitor
  - alternative, app itself or device can be blocked
  - attributes expiry & freshness requirements offer some protection

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 citizen requests signed with BSN, or digital cheques, signed with IBAN

IRMA realisation:

- exists, as prototype implementation "on the command line"
- development of signature ecosystem currently under development

IRMA signature ecosystem

Basic set-up:

- a separate (desktop) app for forming a signature request:
  - a text, to be signed — flat text at first
  - a list of attributes for the signer — to be included
- the request is sent, as email attachment, to the signer
- clicking on the attachement opens the IRMA app for signing
- the requester gets a copy, and the signer retains one

This basic set-up will be evaluated first

- later on, many extensions/variations will be added
  - pdf instead of flat text
  - multiple documents signed at once
  - multiple people signing
  - signature request signed itself, by the requester
- Long term strategy: authentication for free, signing via subscription

IRMA pilots and rollout

- The IRMA app is freely available for everyone
- The foundation issues multiple attributes
  - from iDIN, SURFconext, BIG, email addresses, mobile numbers
  - soon also: bank account (IBAN+BIC)
  - also coming: attributes 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
- 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 responsability
- **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 requires privacy-friendly technology — which could be enforced by regulators

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 decentral one

  What kind of society do we prefer to live in?
- IRMA is a decentralised, 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 authenation for free

For more info: https://privacybydesign.foundation

Follow us on twitter.com/IRMA_privacy

iCIS | Digital Security
Radboud University