Attribute-based authentication and signing with IRMA

Kooy Symposium, Koot Kazerne

Bart Jacobs — Radboud University and Privacy by Design foundation
bart@cs.ru.nl
April 11, 2018

Tribute to Gen. Maj. Henri Koot (1883–1959)

- Probably the greatest cryptologist of the Netherlands
  - allegedly he broke German codes in WWI; archives were lost in 1940
  - he became *Directeur van het cijfer*, leading military cryptography
- He educated a whole generation of Dutch military cryptologists
  - esp. J.F.W. Nuboer and J.A. Verkuijl; they broke Japanese codes before WWII, and set-up NL intelligence after the war
- Koot is most well-known from WWII as *Commandant Binnenlandse Strijdkrachten* — and for introducing Greet Hofmans to the Palace

Overview

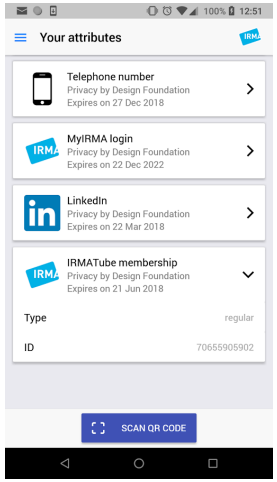
Attribute-based authentication & signing, via identity platform "IRMA"

- publicly available open source cryptographic functionality
- crypto comes from IBM Zürich — ecosystem is Dutch design
- basis is relatively mature
- functionality is still being extended — e.g. with strong authentication and digital signatures

IRMA's general picture

- value-driven design, connecting principles and solutions
- relevant values: self-sovereignty, transparancy, independence
- governance is an issue in itself — developed as we proceed

IRMA basics: reveal only relevant attributes



Authentication essentials:

- attributes instead of identities
- collected by user him/herself
- attributes are reliable (digitally signed by source)
- IRMA is free & open source
- decentralised architecture: attributes only on users own phone

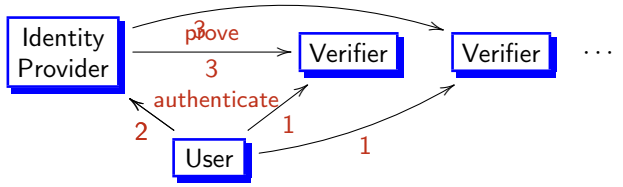
Demo !?!

IRMA history, in two phases

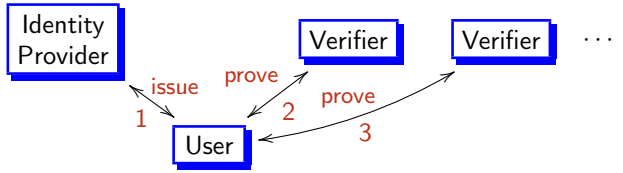
- **2008 – now**: scientific research project at Radboud University
  - active research line on attribute-based authentication (via Idemix)
  - 3 PhD theses so far, postdocs too, many publications
  - financial support from: NLnet, Translink, BZK, NWO, KPN
  - prototype implementations on:
    - smart 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
  - attribute-based signatures will be added soon

Centralised versus decentralised, schematically

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



Decentralised: everyting goes via the User (think IRMA)



First concern of the foundation: issuing attributes

Many attributes are already available — some of them only for NL

- via banks (iDIN): name-address-dob
- email and mobile nr.
- via social media (Facebook, LinkedIn, Twitter)
- via BIG: health professional registrations
- via SURFconext for education sector in NL
  - also internationally via eduGAIN — in experimental form
- and soon: IBAN & BIC attributes for bank account nr.

Chicken and egg problem, with "chicken" part solved

- At first: set-up infrastructure and issue attributes
- Now: getting usage of attributes off the ground

Ongoing activities/pilots

- Collaboration with SURF, for usage in educational sector
  - esp. strong authentication, with IRMA as second factor
  - exists in pilot environment; will be evaluated by Radboud
  - also joint project for access to new eduVPN service
- Experiments in municipalities
  - *huishoudboekje* of Utrecht, with signatures of participants
  - automatic form-filling by Nijmegen — and Alliander
  - issuing of attributes considered e.g. by Haarlem
  - many others are following with interest — including BZK
- Many options in healthcare, both professionals & patients
  - BIG-attributes are already being issued
  - *specifieke toestemming* is upcoming challenge
- Contacts with several companies

International expansion

- IRMA is globally available — see dashboard on website
  - the decentralised architecture is very suitable for international deployment
  - only public keys needed for verification
- Loading attributes into your IRMA app requires trusted sources
  - they are organised mostly at a national level — like now in NL
  - different "trust anchors" are needed per country
- Expansion will likely happen on country-by-country basis
  - identity management is culturally and historically determined
  - partner groups needed per country
  - we're open to collaboration, but it's not the current priority

Attribute-based signatures

General idea:

- selective inclusion of attributes of signer in a signature
- verifier learns: doc was signed by someone with these attributes
- signatures are transferrable and can be checked by others
- eg. a letter is signed by a doctor, lawyer, general, citizen, etc.
- opens up many new applications, like citizen requests signed with social security number, or digital cheques, signed with IBAN

IRMA realisation:

- exists, as prototype implementation of different components
- development of signature ecosystem currently under development, based on "requestor" model

Demos in the Workshop !!

Relevance of IRMA for the military

- The military world is full of attributes — like ranks, units and compartimentalisations, etc.
  - these attributes can be used for fine-grained access control
- IRMA is decentralised & robust & perfect for international usage
- IRMA's privacy-friendly character is also relevant
  - e.g. for special forces, who typically don't reveal their full identity
- IRMA's digital signatures guarantees authenticity and integrity of orders and reports
  - signing is the default technique for reliability of information

In short, the military is a great application domain!

Finally, why don't you use blockchains???

Blockchains are an exceptionally bad idea

especially in identity managment. For instance, it is against the law to:

- make personal data public on a (public, permissionless) blockchain
  - permissioned (private) blockchains offer little advantage
  - encrypting the data introduces huge key management problems
- not being able to delete personal data upon request
  - since data cannot be removed from blockchains

Blockchain believers now think the law (GDPR) should be changed.

- Good luck with that; better change/dump your technology!

Blockchains do require identity solutions

- but with authentication and signing solved, who needs blockchains?

Concluding remarks

- IRMA is about pushing the technology forward, and about creating impact, using real data, based on facts, not hypes
  - it is based on both privacy and security by design
- IRMA emphasises decentralised control: self-sovereignty
  - not just in words — like so many — but in architecture
- IRMA signatures may become the killer application
- IRMA is relatively mature, open source, non-profit, privacy-friendly, secure, globally available attribute-based identity management
  - the Google's and Facebook's don't want this
  - who will work for its adoption? Governments? Regulators? The public? Academics? Enlightened companies? The military?
  - IRMA is also a social experiment — and a community effort

For more info: privacybydesign.foundation
Follow us on: twitter.com/IRMA_privacy

iCIS | Digital Security
Radboud University