Attribute-based Authentication and Signing with IRMA

Google SF

Bart Jacobs — Radboud University and Privacy by Design foundation
bart@cs.ru.nl
Dec. 14, 2017

Outline

Where we are, so far

Introduction

The IRMA system

Who is this guy?

- Professor of computer security at Nijmegen, NL
  - heading a broad group of 50+ security researchers, largest in NL
  - including top people like Joan Daemen (AES, Sha3), Peter Schwabe (New Hope)
  - own focus on privacy and identity management
- Several smart card vulnerabilities found in Nijmegen
  - e.g. in MIFARE Classic in 2008, and in Megamos in 2012
  - Both vulnerability disclosures were challenged in court, succesfully for Megamos in London
- Ranked most influential computer security expert in NL
  - by investigative journalism website *Follow the Money*
  - ranking based on appearances in the media
- Part of large medical study into Parkinson's disease, also with Verily
  - our own "PEP" technology forms a secure database
- PhD supervisor of Miguel (formally)

Fundamental form of payment: a check

A check is a written order directing a bank to pay money as instructed

A signed IOU

Or a digital equivalent

Requirements, for such checks

- it contains the amount and the account nr. of the payee (receiver)
- the payer's signature guarantees:
  - non-repudiation, the key security property of a digital signature
  - possession of the account from which the payment comes
  - the payer need not say: this is me, **but** this is my account
  - this account (number) is an attribute of the payer

Main ideas

Attributes instead of identities

A person's identity is given by a personal collection of attributes, like: gender, date-of-birth, home address, e-mail, phone nr., bank account nr., social security nr., profession, registration nr., membership, ...

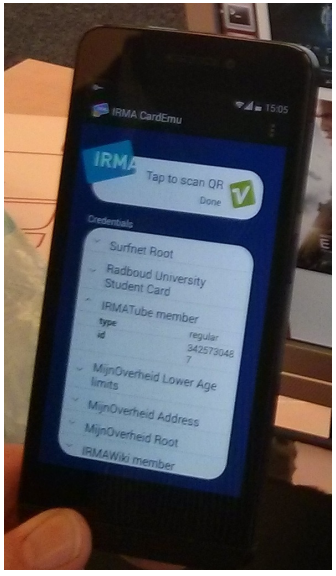
These attributes can be used for:

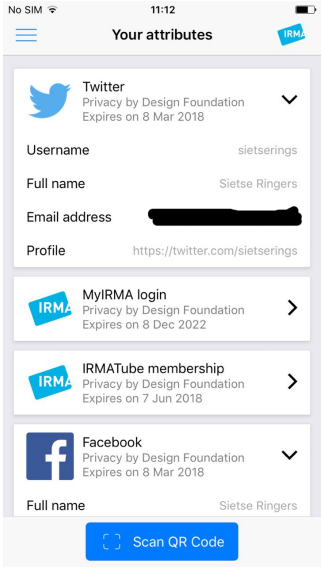
- **Authentication**
  - selective disclosure of attributes, depending on situation
  - "contextual authentication" realising different "personas"
- **Signing**
  - selective inclusion of attributes in signature
  - verifier learns: doc was signed by someone with these attributes
  - e.g. signed by medical doctor, lawyer, possibly with registration nr.
  - but also: signed with banck account nr as attribute

Excursion about signatures

- **Wet signatures**
  - traditional handwritten signature, produced with pen and ink
- **Electronic signatures**
  - the digitised equivalent of a hand written signature used to confirm content/terms in a document
  - e.g. digital scan of wet signature
- **Digital signatures**
  - cryptographically produced addition to a document that can be verified, assuring:
    - integrity of the document
    - signer authentication
    - sometimes also authenticity of the document (its source)

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)

Where we are, so far

Introduction

The IRMA system

IRMA history, in two phases

- **2008 – now**: scientific research project at Radboud University
  - active research line on attribute-based authentication
  - IBM's Idemix is cryptographic basis; extended to an ecosystem
  - 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 signing now added to the mix

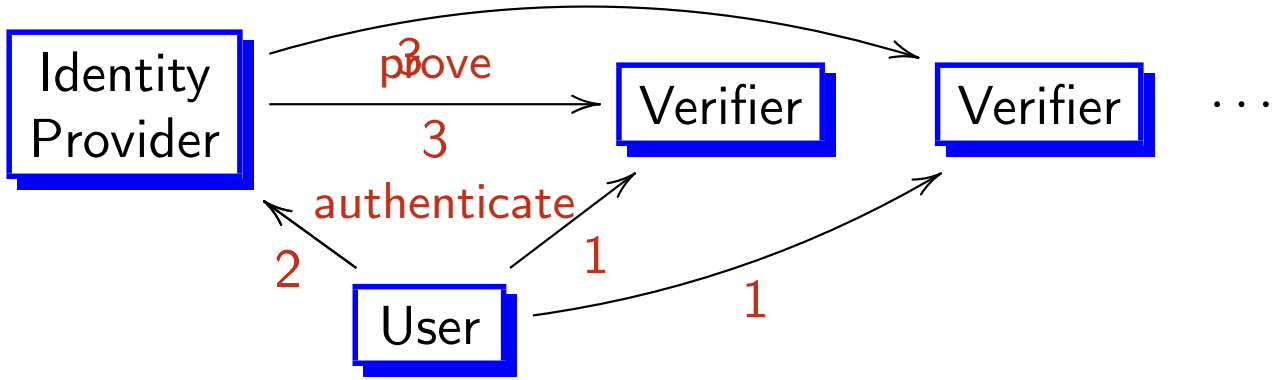
iCIS | Digital Security
Radboud University

Example identity services

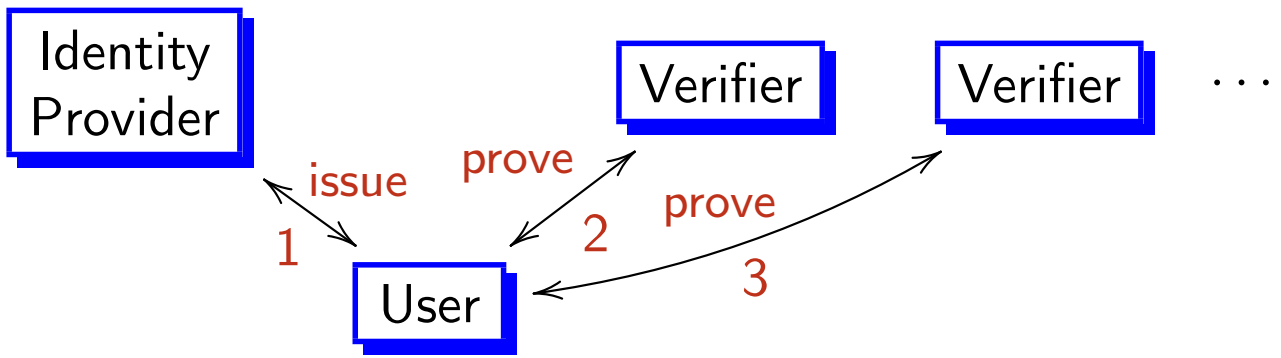
Public	Private	Non-profit
DigiD	Facebook login	SURFconext
~~iDensys~~		
iDIN		
		IRMA

Centralised versus decentralised, schematically

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



Decentralised: everyting goes via the User (think IRMA)



iCIS | Digital Security
Radboud University

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

iCIS | Digital Security
Radboud University

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

iCIS | Digital Security
Radboud University

Cryptographic basis: Schnorr's proof of knowledge

- Assume a generator $g \in G$ in a finite group of prime order q, with publicly given $h = g^x \in G$, where $x \in \mathbb{Z}_q^*$.
- Peggy (P) wants to prove to Victor (V) that she knows x, of course, without revealing it.

$$\begin{array}{lll} \mathbf{P} \longrightarrow \mathbf{V}: & a \stackrel{\text{def}}{=} g^w \in G & \text{with } w \in \mathbb{Z}_q^* \text{ random} \\ \mathbf{V} \longrightarrow \mathbf{P}: & c \in \mathbb{Z}_q & \text{a random challenge} \\ \mathbf{P} \longrightarrow \mathbf{V}: & r \stackrel{\text{def}}{=} c \cdot x + w & \end{array}$$

V now checks $g^r \stackrel{??}{=} h^c \cdot a$

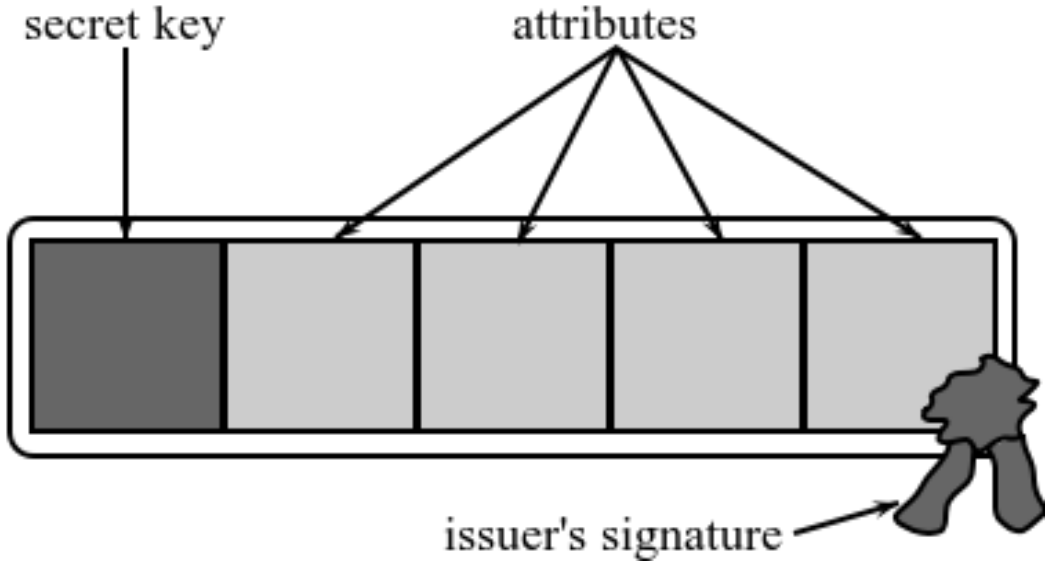
- Note that V can prove nothing to others: anyone can produce values r and a with $g^r = h^c \cdot a$.
- This proof-of-knowledge is turned into a signature by choosing the hash of a message as challenge c — the Fiat–Shamir heuristic.

iCIS | Digital Security
Radboud University

Credentials and attributes in IRMA context

A card contains multiple credentials, each with multiple attributes:

Credential =



- The secret key is securely stored (actually distributed, via key-splitting) making credentials non-transferable; required in "showing attributes"
- The issuer's signature guarantees authenticity and integrity
- Any subset of the attributes can be shown in transactions. This is called selective disclosure.

Attribute representation and disclosure

A 4-tuple (a_1, a_2, a_3, a_4) of attributes a_i is represented via a multi-exponent:

$$C = g_1^{a_1} \cdot g_2^{a_2} \cdot g_3^{a_3} \cdot g_4^{a_4} \in \mathbb{Z}_n$$

This multi-exponent must be *randomised* and *signed*, via a so-called Camenisch-Lysyanskaya signature (2002); this will be skipped here.

Assume I wish to disclose attributes a_1, a_3, but not a_2, a_4

- I send attribute values a_1, a_3 to the verifier
- the receiver divides C by $g_1^{a_1} \cdot g_3^{a_3}$, yielding $g_2^{a_2} \cdot g_4^{a_4}$
- Via a zero-knowledge proof I show that I know exponents a_2, a_4

iCIS | Digital Security
Radboud University

Authentication and signing

In IRMA authentication and signing follow the same protocol

- in authentication a challenge of the verifier is signed
- in signing the hash of a message is signed

The two are kept apart by domain separation

iCIS | Digital Security
Radboud University

Attribute-based signatures

General 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

Two procedures for signing a message M are being elaborated:

- **M is retrieved from a server via QR-code**
  - typical scenario online, eg. for payments (M = check)
  - can also be used to register important choices (e.g. being donor)
  - the webpage generates M; the QR-code tells where to find M

- **M is generated and sent by email**
  - a separate (desktop) app for forming a signature request:
    - via a text M, 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
  - many variations: pdf instead of text; multiple documents, or multiple signers, request itself is digitally signed

iCIS | Digital Security
Radboud University

IRMA pilots and rollout

- The IRMA app is freely available for everyone (Android + iOS)
- The foundation issues multiple attributes
  - from iDIN, SURFconext, BIG, email addresses, mobile numbers
  - recently: attributes from Facebook/Linkedin/Twitter accounts
  - soon also: bank account (IBAN+BIC)
  - the sky is the limit, depending on demand
- International challenge: finding trust anchors of appropriate levels
  - requires national efforts, in each country separately (like in NL)
  - e-passports have restrictions (NFC not on iOS, ownership?)
- Latest effort lies on verification, at merchants (relying parties)
  - since oct'17 available for all academic parties in NL (about 1M potential users); international extension planned (via eduGAIN)
  - pilot being set up in health care
  - strong authentication pilots with IRMA in preparation
- 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 from Big-IT is not likely;
  - tracking and profiling people is essential to their business model
  - but they might be interested in IRMA's signatures
- **Contra**: IRMA's business model is weak
- **Contra**: Some attribute management effort on user-side is required
- **Pro**: IRMA has superior technology, including digital signatures
- **Pro**: Private eID's have only limited trust, certainly in Europe
  - providing "source" identity is widely seen as public responsability
- **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: privacybydesign.foundation

Follow us on twitter.com/IRMA_privacy

iCIS | Digital Security
Radboud University