Attribute-based Authentication and Signing with IRMA

Summer School on real-world crypto and privacy

Bart Jacobs — Radboud University and Privacy by Design foundation
bart@cs.ru.nl
Šibenik, Croatia, 15 June 2018

Where we are, so far

IRMA overview

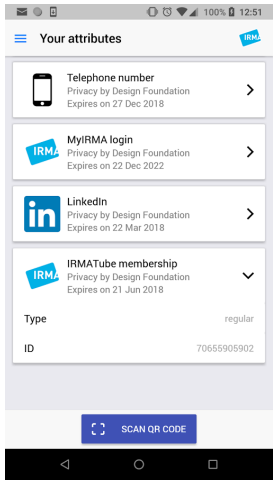
Cryptographic essentials

IRMA in action

Conclusions

iCIS | Digital Security
Radboud University

IRMA Demo: authenticate/sign with relevant attributes only



Essentials:

- attributes instead of identities, on user's phone
- collected by user him/herself
- attributes are reliable (digitally signed by source)
- both authentication and signing
- decentralised architecture: attributes only on phone
- Cryptographic basis: Idemix
- IRMA is free & open source

iCIS | Digital Security
Radboud University

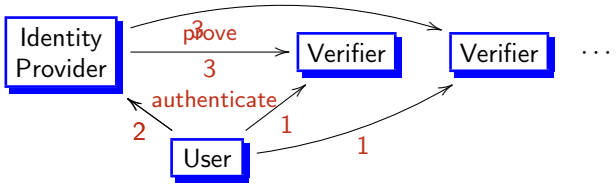
IRMA history, in two phases

- **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 some attributes
  - eg. from: iDIN (banks), EduGain (academia), BIG (health)
  - both Android and iOS apps, with common code-base in **Go**
  - attribute verification pilots are emerging
  - attribute-based signatures added recently

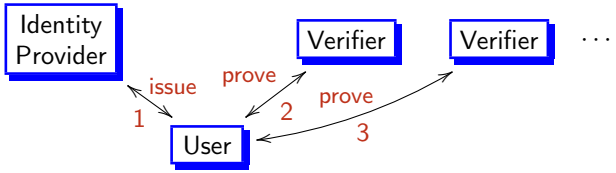
iCIS | Digital Security
Radboud University

Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider (eg. FB Connect)



Decentralised: everyting goes via the User (think IRMA)



Bigger picture: open identity platform

- The internet was designed without security or identity guarantees
  - understandable, at the time
  - increasingly a problem: identity fraud, lack of trust, missed opportunities
  - many ad hoc solutions, often harming privacy
- IRMA has the grand ambition to be such identity add-on
  - it's globally available, see dashboard page with metrics
  - **not**: one size fits all, like Facebook connect
  - **but**: different attributes, depending on national traditions
  - identity management is culturally sensitive
  - it requires national 'trust anchors', see later

Bigger picture: General Data Protection Regulation

GDPR has identity management requirements in two places:

- **Inspection rights**
  - people can ask organisations what data they have on them, for which purpose, from which sources, etc.
  - also: right of correction & deletion
  - only possible with (strong) authentication of the requestor
- **Consent obligations**
  - each form of data processing requires a legal ground (art. 6)
  - one such ground is consent, for a specific purpose
  - consent requirements are in art. 7: free, separate, clear, etc.
  - processor must keep "proof" of consent; what is it?
  - best realisation: digital signatures
  - they can be stored, and shown to others — like regulators

IRMA is the unique platform with integrated authentication & signing

Bigger picture: non-profit sector realisation

- Identity management is a strategic and sensitive topic
  - it's all about regulating who has access to what & who checks
- Public authorities often do a bad/mediocre job
  - they fail altogether: NL (partly), UK, US, ...
  - or they come up with privacy-unfriendly (always identifying, centralised) solutions: Estonia, Belgium, India, ...
- Corporations have too many side-interests
  - either making it expensive or forcing user profiling
  - also centralised solutions
  - typically they are not universally trusted by citizens — certainly not when they monopolise
- Maybe non-profit organisations can do **IT** better
  - eg. Let's Encrypt in US, or SIDN in NL (for domain names)
  - IRMA is also a social experiment
  - its decentralised architecture requires alternative funding

Bigger picture: value-driven design

- After Cambridge-Analytica scandal one reaction was that our ICT-infrastructure needs to better reflect moral values
  - esp. 'public' and/or 'European' values should be better reflected
  - not only 'code as legal order' but also 'code as moral order'
- value-driven (or value-sensitive) design exists as academic strand
  - much of this work remains rather theoretical
- IRMA tries to bring this into practice. Emphasis on:
  - self-sovereignty — terminology nicked from blockchain believers
  - transparancy and openness (e.g. of code and designs)
  - independent, non-for-profit and non-monopolising
  - decentralised
  - both security and privacy — not just one of them
  - catch-phrase: contextual authentication & signing — after Helen Nissenbaum's contextual privacy/integrity

Where we are, so far

IRMA overview

Cryptographic essentials

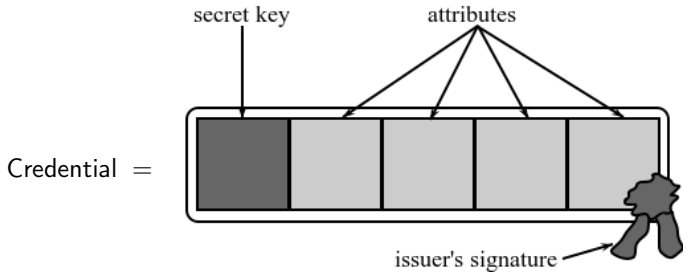
IRMA in action

Conclusions

iCIS | Digital Security
Radboud University

Credentials and attributes in IRMA context

An IRMA app contains multiple credentials, each with multiple attributes:



- The issuer's signature guarantees authenticity and integrity
- Any subset of the attributes can be shown in transactions. This is called selective disclosure.

Example credential: address

Address
Country
City
Street + Number
Postal code

} Separately usable attributes

Issued eg. by: public authorities, or by banks

- Name is not included here; can be stored elsewhere
- Expiry info is omitted, but exists per credential, not per attribute
- Same attribute (eg. name) can be in different credentials, from different issuers, with different trust levels (eg. Facebook or banks)

Attribute representation I

System parameters:

- $n = pq$, for large "safe" primes: p, q, where $p = 2p' + 1, q = 2q' + 1$, with also p', q' prime

  The pair (p, q) is the secret key of the credential issuer
- quadratic residues: $R_0, R_1, R_2, R_3, R_4, S, Z \in QR_n \subseteq \mathbb{Z}_n^*$
  (5 R's, for say 4 attributes per credential, plus the user's secret key)

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

$$R_1^{a_1} \cdot R_2^{a_2} \cdot R_3^{a_3} \cdot R_4^{a_4} \in \mathbb{Z}_n$$

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

Attribute representation II

- Let k be the secret key. A credential is a triple:

$$v,\ e,\ C \quad = \quad \left(\frac{Z}{S^v R_0^k R_1^{a_1} R_2^{a_2} R_3^{a_3} R_4^{a_4}} \right)^{1/e}$$

  where v, e are random, with $e \cdot 1/e \equiv 1 \mod \phi(n) = (p-1)(q-1)$.
- The crucial signature verification equation is:

$$Z \quad \equiv \quad C^e \cdot S^v \cdot R_0^k \cdot R_1^{a_1} \cdot R_2^{a_2} \cdot R_3^{a_3} \cdot R_4^{a_4} \mod n$$

Blinding of the signature/credential

- the equation still holds for $v' := v + e \cdot r$, $C' := C \cdot S^{-r}$
- the RSA-exponent e remains the same; it is not disclosed itself to the verifier, but only via a zero-knowledge proof

Selective disclosure essentials

- Assume I wish to disclose attributes a_1, a_3, but not a_2, a_4.
  - The blinding of the credential e, v, C is skipped here
- I reveal attribute values a_1, a_3 and credential (parts) v, C
- Via a zero-knowledge proof I show that I know exponents $\varepsilon, \kappa, \alpha_2, \alpha_4$ with:

$$\frac{Z}{R_1^{a_1} \cdot R_3^{a_3}} \quad \equiv \quad C^\varepsilon \cdot S^v \cdot R_0^\kappa \cdot R_2^{\alpha_2} \cdot R_4^{\alpha_4} \mod n$$

Signing in IRMA, via Schnorr ZKP (with memory refresh)

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

$\mathbf{P} \longrightarrow \mathbf{V}$:	$a \stackrel{\text{def}}{=} g^w \in G$	with $w \in \mathbb{Z}_q^*$ random
$\mathbf{V} \longrightarrow \mathbf{P}$:	$c \in \mathbb{Z}_q$	a random challenge
$\mathbf{P} \longrightarrow \mathbf{V}$:	$r \stackrel{\text{def}}{=} c \cdot x + w$	
	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 is also a signature scheme: take hash of message as challenge: $c = \mathcal{H}(m)$.
- Idemix is used this way in IRMA, with domain separation & extended with a time-stamp server — using quantum secure signature!

Split-key solution for key protection

- Idemix/IRMA requires a private user key, which is embedded in each credential — but never disclosed
- The key has to be used on the phone, but storing it there is a bad/dangerous idea
- Therefor a split key solution has been developed:
  (1) a threshold protocol, with part of the user's key stored on a central server
    - app's PIN activates this central part of the key
    - user-initiated revocation by disabling central part
    - (alternative login via optionally registered email address)
  (2) . . . together with Pallier homomorphic encryption
    - the central server can not see which attributes you reveal to which verifier

Scheme and scheme manager

- The Privacy by Design foundation maintains a public scheme with all available IRMA credentials/attributes
  - esp. for meta-info: attribute names, public key of issuer, validity
  - verifiers look up this information when needed
- Issuers need to go through the foundation for:
  - registering new credential in this scheme
  - getting a certificate to issue to apps
- Thus: IRMA is open source, but cryptographically closed
  - this gives the foundation control over who issues. Needed?
  - and also a source of income ☺
- However, anyone can set-up own scheme manager
  - might be useful for "closed" communities, like military
  - mutual use of credentials is possible, but requires users to adapt their app settings — a fuss
  - foundation aims to maintain one public realm

Where we are, so far

IRMA overview

Cryptographic essentials

IRMA in action

Conclusions

A long road

It's a long, long road from academic research to deployed systems

- esp. when there are established (commercial) interests
- and when government is vison/clue-less
  - eg. NL has open source preference policy
  - in practice it does not work: "you participate in the bidding"
- it takes a lot of explaining, discussion and convincing
- useability, and design, are really important
  - we now have such people on board
- in the end what counts are functionality, useability, and "wow factor"
  - value-aspects don't convince, in the end
  - attribute-based signatures make a real difference
- down this long road, academic publishing becomes increasingly difficult

People and funding

- Dedicated group of developers and useability/legal experts
  - Fabian van den Broek, Joost van Dijk, Katerina Demetzou, Maarten Evers, Brinda Hampiholi, Tomas Harreveld, Koen van Ingen, Ayke van Laethem, Wouter Luecks, Sietse Ringers, Hanna Schraffenberger, David Venhoek, Pim Vullers, Tim Walree, Bas Westerbaan
  - volunteers; funded by foundation; funded by research projects
  - upcoming group: external developers, eg. from corporation or government — they like to join our Slack channel
  - this is basically a community project
- Funding needed for basic activities — even for non-profit
  - initial 100K€ from energy company Alliander
  - additional 200K€ from projects
  - "support" initiative starting only now — see webpage

Chicken and egg problem for new identity platform

(1) users will not install it unless many webshops offer/require it
(2) webshops will not offer/require it unless many users have installed it

The foundation decided to focus on the "chicken" problem first

- this means setting up the infrastructure and issuing attributes
- initially, mostly issued by the foundation as proxy
  - user logs into bank/university/social-media/...
  - attributes are made available to the foundation
  - foundation signs and issues itself — and deletes attributes
  - seen as temporary, sub-ideal but workable solution

Internationally available IRMA attributes

(1) **Email**
  - via one-time code sent to address

(2) **Social media** (Facebook, Twitter, Linkedin)
  - low assurance, self-supplied attributes
  - potential to make Facebook Connect "blind"

(3) **EduGain**
  - attributes from academic institutes
  - "R&S" version; attributes differ
  - limited experience so far — please try it too and tell us!

Nationally available IRMA attributes (in NL)

(1) **iDIN**: authentication via standard internet banking means
  - provides names, date-of-birth, address
  - (initially free, but costs will be passed on to user soon)

(2) **SURFconext**: national version of EduGain
  - name, institution, institution email, student/employee, institution personal identifier

(3) **mobile phone number**
  - checked via one-time SMS-code; could be expanded to EU

(4) **Medical professional registration**
  - obtained after look-up in public register "BIG"

(5) **Citizen administration**
  - issued by municipalities, from their official citizen administration
  - recent spectacular step forwards

(6) in preparation: **IBAN** and school/university **diplomas**

Current issuers

(1) **Privacy by Design** foundation
- for attributes that the foundation checks itself: email, phone nrs
- for attrubes from others, as proxy, for: bank, universities, health (preferably these parties start doing the issuing themselves)

(2) **SURFnet**, the net-provider for academia in NL
- issues special attributes after strong authentication

(3) **Cities of Nijmegen, Haarlem**
- experimentally issuing 20-25 attributes from citizen administration
- in principle usable by all Dutch citizens

(4) • • •

Issuing issues

- IRMA app is like a local cache for authentication data
  - how long should data remain there? — expiry question
  - short expiry period can be used for senstive attributes — but verifier can also require fresh attributes
- Now there is only user-initiatied revocation
  - what about issuer-initiated revocation
  - technically possible, cumbersome in practice
  - not yet implemented in IRMA — but often requested
- What about back-up and/or restore of credentials
  - mostly an organisational problem
  - e.g. you want a private key to work only on one device
  - who do you trust? How do you authenticate to back-up?

Attribute-based signatures

What is this about?
- selective inclusion of attributes of signer in a signature
- verifier learns: doc was signed by someone with these attributes
- e.g. signed by medical doctor, lawyer, possibly with registration nr.
- or teacher's signature on student marks
- but also: signature with bank account nr. as attribute, as cheque
- or signed with BSN, as citizen's request to government

These signatures could be the real killer application
- however, integration in existing work flows requires much work
- also, much support software is still needed, like various plugins
- foundation is developing generic "signature requestor app"

IRMA applications in preparation (june'18)

- in **healthcare**
  - patient portals — for authentication & consent signing
  - medical staff portal — for authentication and signing, esp. of medicine prescriptions/renewals
- in **education**
  - for strong staff authentication and signing of student marks
- in **(local) government**
  - for (alternative, proportional) authentication
  - for form-filling
  - for call me back requests via the web, signed with mobile phone number and citizen identification number — so that personal dossier info can be discussed over the phone

International usage of IRMA

- The decentralised set-up makes IRMA ideal for international usage
  - only public keys needed for verification — and open source software
  - attributes can reflect existing national authentication cultures
- However, international "expansion" will probably go step-by-step
  - national trust anchors are needed, per country, as reliable sources of attributes

Inspired? Wanna join? — contact me

- IRMA is very much a community effort
- You can contribute in your own country by eg.
  - talking about it and demonstrating the technology, esp. to decision makers in government and corporations
  - doing (student) projects with IRMA
  - translating the foundation's website (and app) into your own language (markdown code is on github, now for EN and NL)
  - join the development effort — esp. for integrating IRMA in email clients, text processors, etc.
- Of course, we like to have a reasonable level of stability in such cooperations — with longer term commitment
- If you have a corporate background: ask your company to support us!

Developer gadgets

- Docker image for IRMA "API server"
  - software for verifying and issuing attributes
  - get it running in 2 commands!
- Tutorial video for integrating IRMA authentication in your website
  - See https://youtu.be/5aYQ2N7KR3c
- Online index of available IRMA attributes
  - see https://privacybydesign.foundation/attribute-index/en
- Join our Slack channel!

What's next on the agenda?

- Consolidate the foundation itself, both financially and professionally
  - partnership talks are ongoing with a bigger like-minded foundation
- Consolidate the server infrastructure
  - professional hosting is being discussed, with the same party
  - replication of key-sharing servers is possible, but requires some redesign
- Expand the app's functionality, with eg.
  - possibility to change your PIN
  - back-up & restore of credentials
  - make refreshment of credentials easier
  - add issuer-initiated revocation
- Improve user experience
  - usability tests are being set up
- Work on the "egg problem": encourage wider usage!

Where we are, so far

IRMA overview

Cryptographic essentials

IRMA in action

Conclusions

Main points

- Information flows and authentication requirements determine power relations in modern societies
- 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?
- Maybe Idemix peaked too early, when the time was not ripe yet
- IRMA is a decentralised, open source, non-profit, flexible identity platform that is up and running, and being tested by various parties
  - it integrates attribute-based authentication and signing
  - it provides privacy-friendly empowerment of users
  - it's well on the way on a long road
  - now organised and run by non-profit foundation

Interested? Join, or follow on `twitter.com/IRMA_privacy`

iCIS | Digital Security
Radboud University