IRMA: The future of identities

dcypher Symposium 2019

Fabian van den Broek

fabian.vandenbroek@ou.nl

Open University of the Netherlands

3 December 2019

#dSymp

The OYOI project

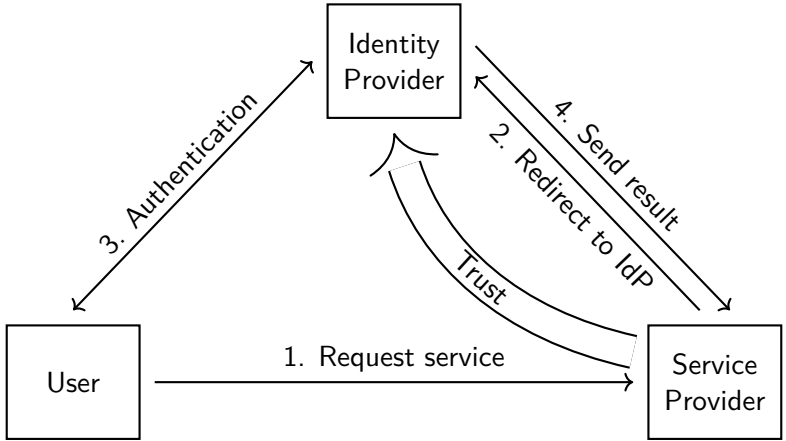
The OYOI project

- Own Your Own Identity
- NWO Long Term Cybersecurity research 2014
  - Radboud University Nijmegen
  - KPN
  - SURFnet
- Valorisation of the IRMA project
- Implementations of "IRMA" on other carriers

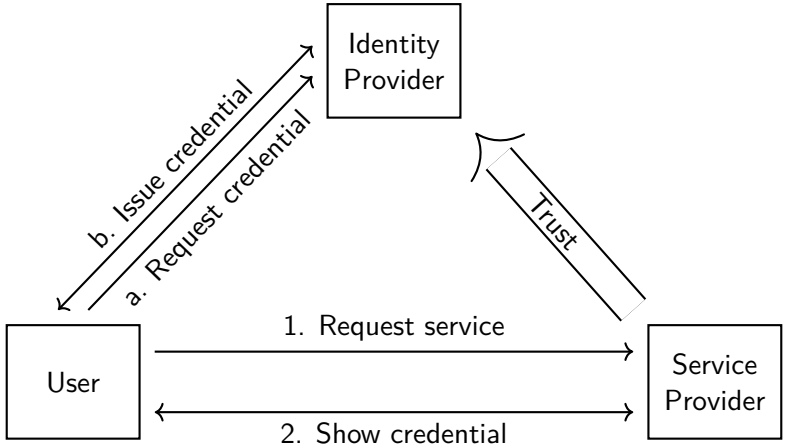
IRMA

- I Reveal My Attributes
- Attribute-based credentials
- Specifically for authentications

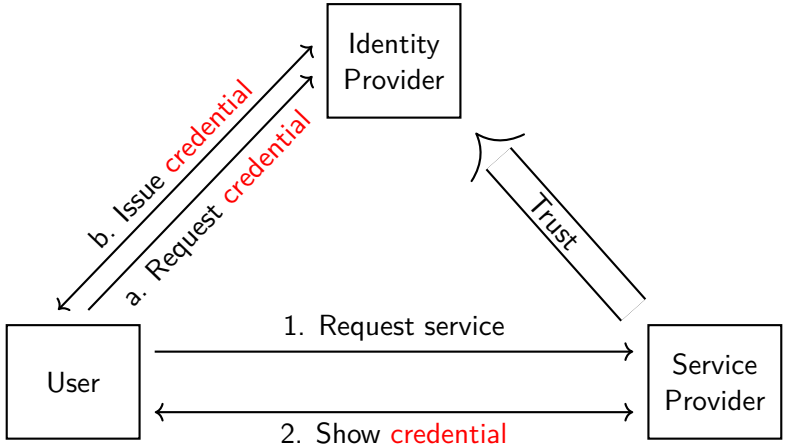
A standard authentication solution



The IRMA solution



The IRMA solution



So, what is this credential?

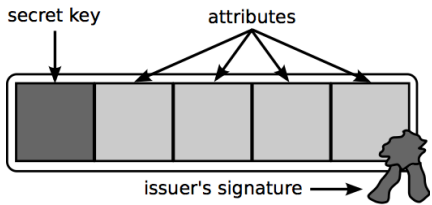
- IRMA is an implementation of Attribute-Based Credentials (ABC)

So, what is this credential?

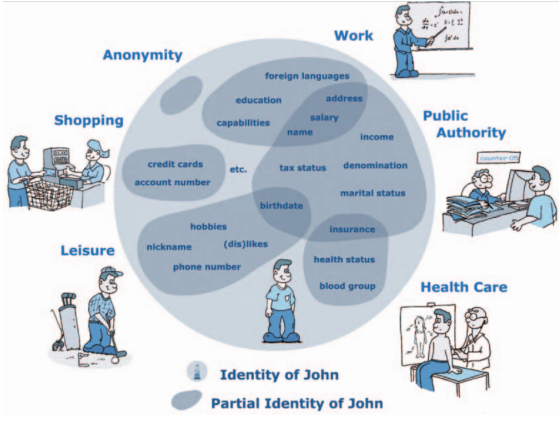
- IRMA is an implementation of Attribute-Based Credentials (ABC)
- Specifically IBM's Identity mixer (Idemix)

So, what is this credential?

- IRMA is an implementation of Attribute-Based Credentials (ABC)
- Specifically IBM's Identity mixer (Idemix)
- A credential is a cryptographic container



Identities versus attributes

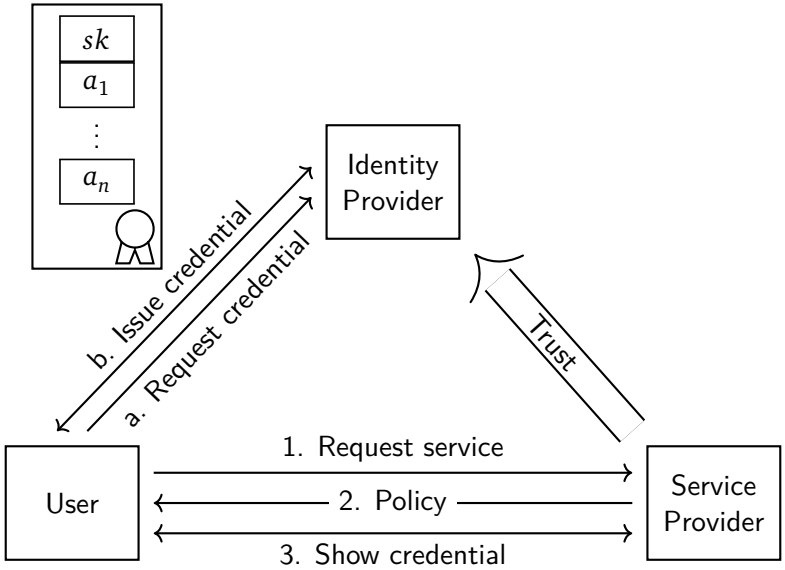


[FIDIS] project

Attributes in Idm

- Flexible
- Identifying (name, address, etc.)
- Or Non-identifying (>18, resident of Amsterdam, etc.)
- Extends role-based authentication

IRMA system


sk
a_1
a_n
Identity Provider
b. Issue credential
a. Request credential
Trust
User
1. Request service
2. Policy
3. Show credential
Service Provider

IRMA features

IRMA features

- Independence between issuing and showing: time and protocol
- Decentralised
- Privacy & Authentication

IRMA features

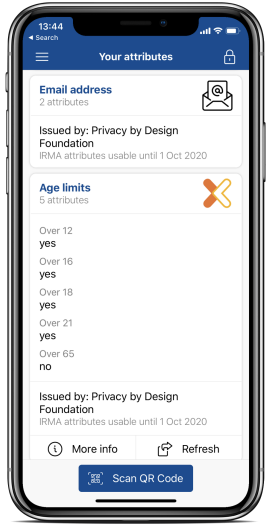
- Independence between issuing and showing: time and protocol
- Decentralised
- Privacy & Authentication
- Credential: security for the system
  - Authenticity
  - Integrity
  - Non-transferability

IRMA features

- Independence between issuing and showing: time and protocol
- Decentralised
- Privacy & Authentication
- Credential: security for the system
  - Authenticity
  - Integrity
  - Non-transferability
- Credential: privacy for the user
  - Selective disclosure (randomisation)
  - Issuer unlinkability (blind signature, randomisation)
  - Multi-show unlinkability (randomisation, zero-knowledge proofs)

At the start of the OYOI project...

And now


13:44
Search
Your attributes
Email address
2 attributes
Issued by: Privacy by Design Foundation
IRMA attributes usable until 1 Oct 2020
Age limits
5 attributes
Over 12
yes
Over 16
yes
Over 18
yes
Over 21
yes
Over 65
no
Issued by: Privacy by Design Foundation
IRMA attributes usable until 1 Oct 2020
More info
Refresh
Scan QR Code

IRMA carrier comparison

A smart card offers:

- Secure key storage
- Strong(er) offline user binding

- A horrible user experience
- Poor computational power
- No Internet connectivity

A smartphone offers:

- Weak key storage
- Weak offline user binding

- Nicer user experience
- Stronger keys, faster performance, unlimited attributes, etc.
- Online issuance & verification, updatability, etc.

Could we have the best of both worlds?

What about smart cards in the mobile phones?

- SIM card

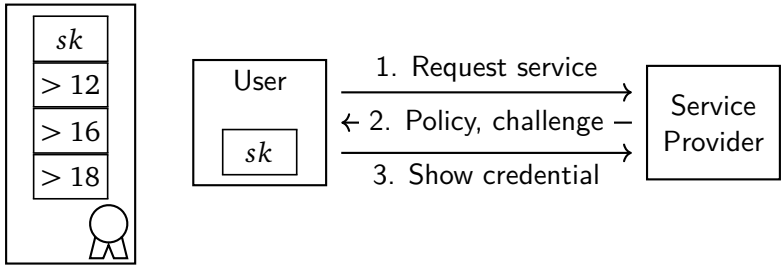
- Trusted Execution Environment

Could we have the best of both worlds?

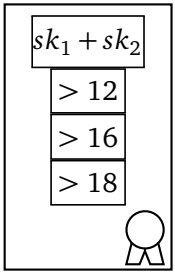
What about smart cards in the mobile phones?

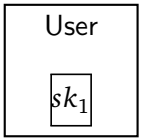
- SIM card
  - JavaCard do not have standard support for the crypto we need
  - it is hard to get generic SIM $\longleftrightarrow$ app communication
- Trusted Execution Environment
  - hard to do anonymous
  - TEE's can differ wildly between phone models
  - we could not get access

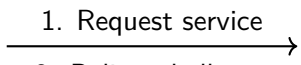
Securing the private key

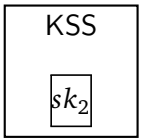


Securing the private key

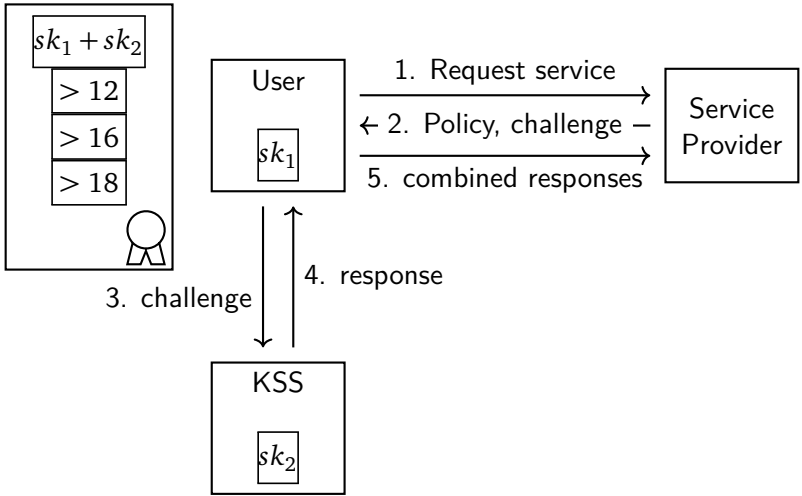








Securing the private key



The Key Share Server

- Secures the key
- Strong revocation (blocking)
- Rate limiting
- Can verify Issuer key validity
- Limited logging
- Limited monitoring

Enrolment

Using a phone also gives innovative ways of enrolment

- Enrolment is an expensive process
- Face-to-face checks needed for high assurance
- Requires a custom approach per country
- NFC-capable phones can read identity documents

Enrolment process

1. User scans her ID card (possibly via another phone
2. Sends the signed data to an *Enroller*
3. The enroller verifies the data and checks that the ID document is not revoked
4. Possible additional checks...
5. An *Issuer* can then issue attributes

Binding ID document to user

- PIN
- Biometrics
- Data consistency checks

Binding ID document to user

- PIN
- Biometrics
- Data consistency checks
  - check with outside data
  - mobile subscription contract
  - other attributes

Binding ID document to user

- PIN
- Biometrics
- Data consistency checks
  - check with outside data
  - mobile subscription contract
  - other attributes
- The mobile subscription contract might also provide binding to the actual phone
- Cross checking with other attributes can lead to higher assurance

Conclusions

- The OYOI project delivered some nice contributions
  - 1 thesis and several scientific publications
  - Self-enrolment scenario's
  - ...
  - And bringing IRMA from academia to society

Conclusions

- The OYOI project delivered some nice contributions
  - 1 thesis and several scientific publications
  - Self-enrolment scenario's
  - ...
  - And bringing IRMA from academia to society
- IRMA now under the Privacy by Design Foundation
- SIDN runs the core infrastructure
- Several proof of concepts running in the field

For more information see:
https://privacybydesign.foundation/irma/
http://credentials.github.io/

Or mail me:
fabian.vandenbroek@ou.nl
f.vandenbroek@privacybydesign.foundation

For more information see:
https://privacybydesign.foundation/irma/
http://credentials.github.io/

Or mail me:
fabian.vandenbroek@ou.nl
f.vandenbroek@privacybydesign.foundation

Thank you!

For more information see:
https://privacybydesign.foundation/irma/
http://credentials.github.io/

Or mail me:
fabian.vandenbroek@ou.nl
f.vandenbroek@privacybydesign.foundation

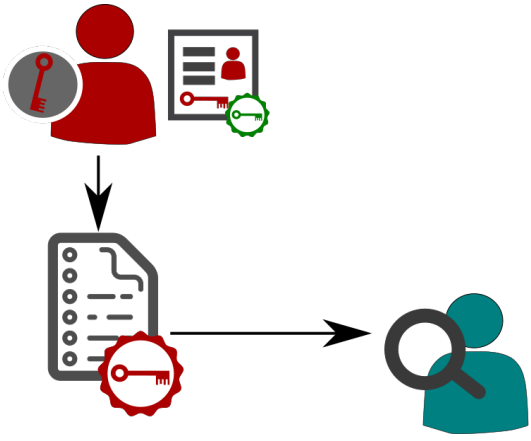
Thank you!

Questions?

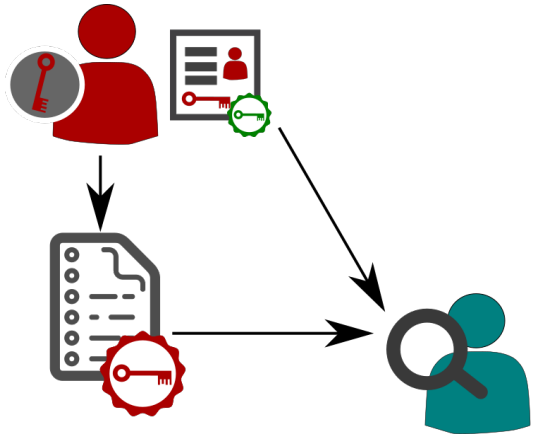
Traditional digital signatures

Traditional digital signatures

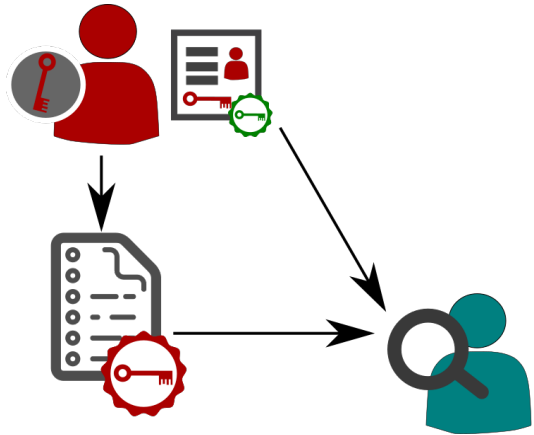
Traditional digital signatures



Traditional digital signatures

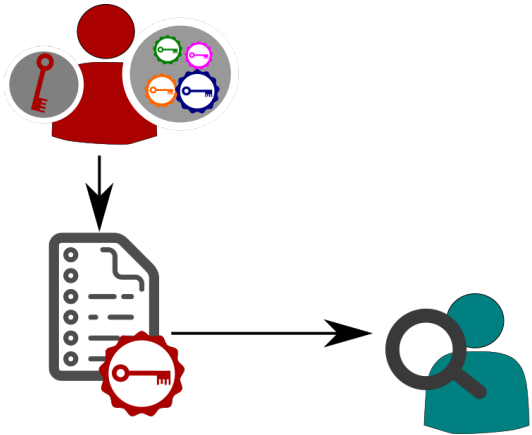


Traditional digital signatures

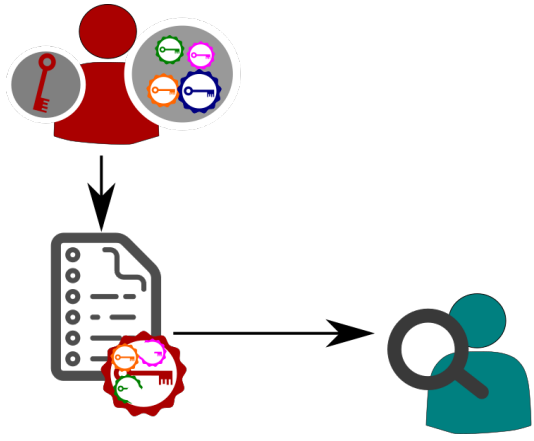


Attribute-based signatures

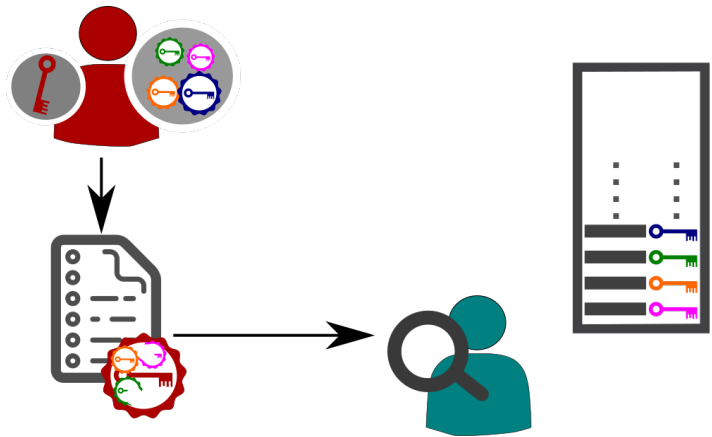
Attribute-based signatures



Attribute-based signatures



Attribute-based signatures



Comparison

Standard digital signatures:

- Are very rigid
- Always identifying and linkable
- Provide non-repudiation & integrity

Attribute-based signatures:

- Are flexible
- Can be anonymous and always unlinkable
- Provide non-repudiation & integrity

Comparison

Standard digital signatures:

- Are very rigid
- Always identifying and linkable
- Provide non-repudiation & integrity

Attribute-based signatures:

- Are flexible
- Can be anonymous and always unlinkable
- Provide non-repudiation & integrity
- ... and authentic attribute data

Comparison

Standard digital signatures:

- Are very rigid
- Always identifying and linkable
- Provide non-repudiation & integrity

Attribute-based signatures:

- Are flexible
- Can be anonymous and always unlinkable
- Provide non-repudiation & integrity
- ... and authentic attribute data
- Realised by serialising standard authentication proof
- where the challenge is the document hash.