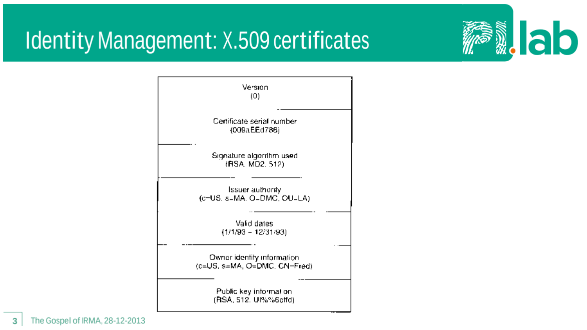
PI.lab
Privacy & Identity Lab

Jaap-Henk Hoepman

Radboud University Nijmegen

The Gospel of IRMA



Identity Management: X.509 certificates

Version
(0)

Certificate serial number
(009aEEd786)

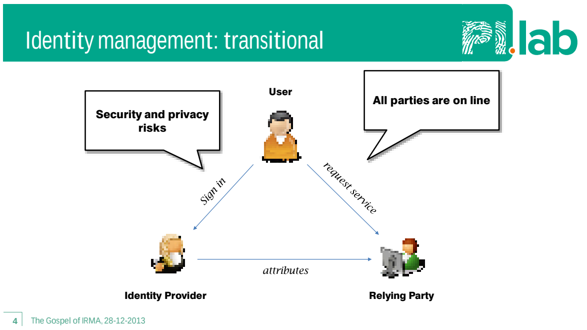
Signature algorithm used
(RSA. MD2. 51?)

Issuer authority
(c−US. s−MA. O−DMC, OU−LA)

Valid dates
(1/1/93 − 12/31/93)

Owner identity information
(c=US. s=MA, O=DMC. CN−Fred)

Public key informat on
(RSA, 512. UI%%6cffd)



Identity management: transitional

Security and privacy risks

User

All parties are on line

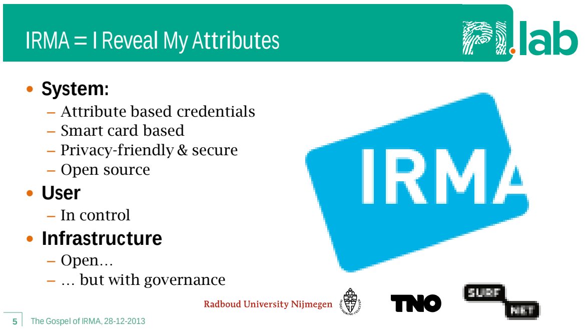
Sign in

request service

attributes

Identity Provider

Relying Party



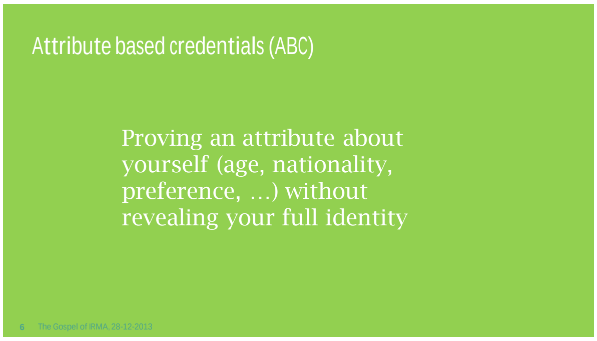
IRMA = I Reveal My Attributes

- **System:**
  - Attribute based credentials
  - Smart card based
  - Privacy-friendly & secure
  - Open source
- **User**
  - In control
- **Infrastructure**
  - Open…
  - … but with governance

Radboud University Nijmegen

TNO

SURF NET

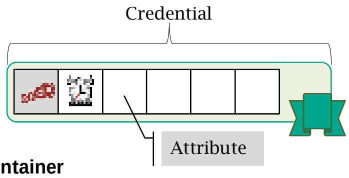


Attribute based credentials (ABC)

Proving an attribute about yourself (age, nationality, preference, …) without revealing your full identity

Credential

PI.lab



- **Secure container**
- **Issued and signed by *credential issuer***
- **Contains attributes, *selectively disclosable***

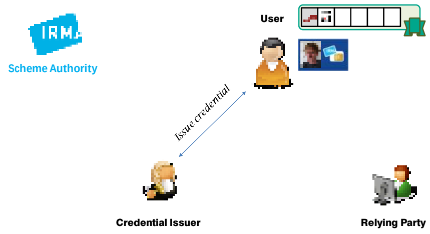
Using such credentials

PI.lab

- **Anonymous**
  - Concert tickets (>16,>18,event,seq. no)
  - Age verification (>16, >18 or <60, <65)
  - Public transport year/track pass (type, period,class)
- **Pseudonymous**
  - Loyalty card (card number)
  - Online newspaper member (membership type, number)
  - Role based access control (military rank, clearances)
- **Identifying**
  - Passport-like (name, BSN, address)
  - Student card (student number, institute)
  - Emergency health info (name, blood group, allergies)

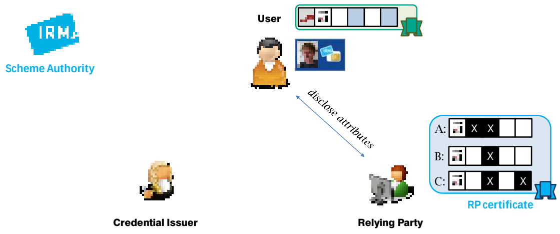
IRMA: issuing a credential

PI.lab



IRMA: disclosing some attributes

PI.lab



ABC Properties

PI.lab

- **Unforgeable**
- **Unlinkable**
  - Issuing with disclosing, and
  - Between two disclosures
- **Revocable**
- **Non transferable**
- **(Inspectable)**

The IRMA card (outside)

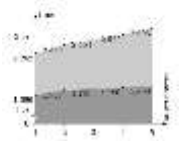
PI.lab

- **Outside**

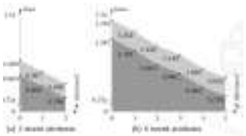
- **Contactless**
  - NFC phones/tablets as terminals
- **Inside**
  - Multos
  - SmartMX (NXP) is option
- **Credentials**
  - Idemix (by IBM)
  - 1024 bit

IRMA card Performance

- **Issuance**



- **Showing**



▨ Computation □ Overhead

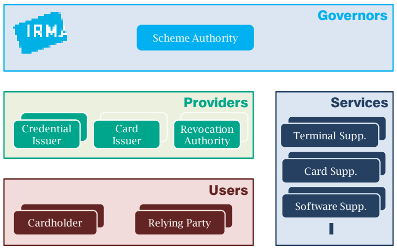
FULL on card implementation

The IRMA terminals

IRMA Applications

- **Verifiers**
  - Running on tablets
  - And even a PoS terminal
- **Card proxy**
  - Using NFC phone as card reader
  - To sign in to websites using attributes
- **Card management app**
  - View and delete credentials
  - Manage PIN codes
  - View logs

IRMA roles



Current limitations

- **1024 bit RSA**
  - Really to low
- **Only equality proofs**
- **No parallel proofs**
  - Due to limited RAM
    - *But we have some ideas how to fix this*
- **Revocation**
  - Being implemented
- **Weak binding of card to cardholder**

William Hogarth: Satan, Sin and Death (A Scene from Milton's 'Paradise Lost'), c.1735-40 , © Tate, London [2013]

Function Creep

- Once you can show *some* attributes to *some* services…
- Sooner or later you will have to reveal *all* your attributes to *all* services

(Overly) strict enforcement

- Real name policies
- No more lying about your address
  - Shopping abroad…
- Or your age
  - Even if you think your children are old enough to be on Facebook

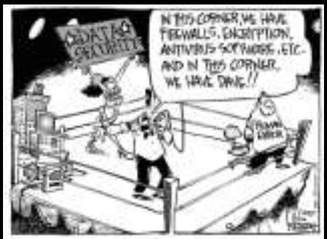
Tracking

DELETE COOKIES?!

Scheme authority

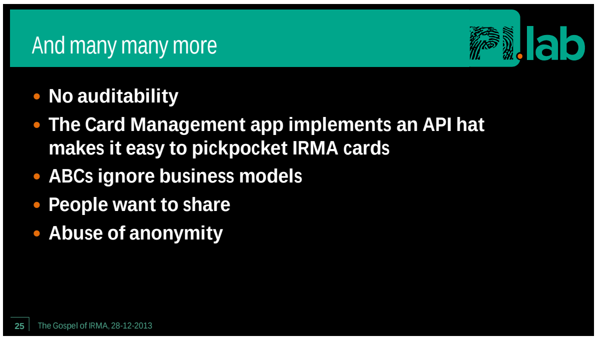
- Not independent
- Not trusted

User in control: user made responsible


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR

Pickpocketing

- The Card Management app implements an API hat makes it easy to pickpocket IRMA cards



And many many more

- No auditability
- The Card Management app implements an API hat makes it easy to pickpocket IRMA cards
- ABCs ignore business models
- People want to share
- Abuse of anonymity

25 The Gospel of IRMA, 28-12-2013

eID everywhere

27 The Gospel of IRMA, 28-12-2013

Technology alone is helpless

28 The Gospel of IRMA, 28-12-2013

Thank you.

www.irmacard.org

@xotoxot jhh@cs.ru.nl http://www.cs.ru.nl/~jhh