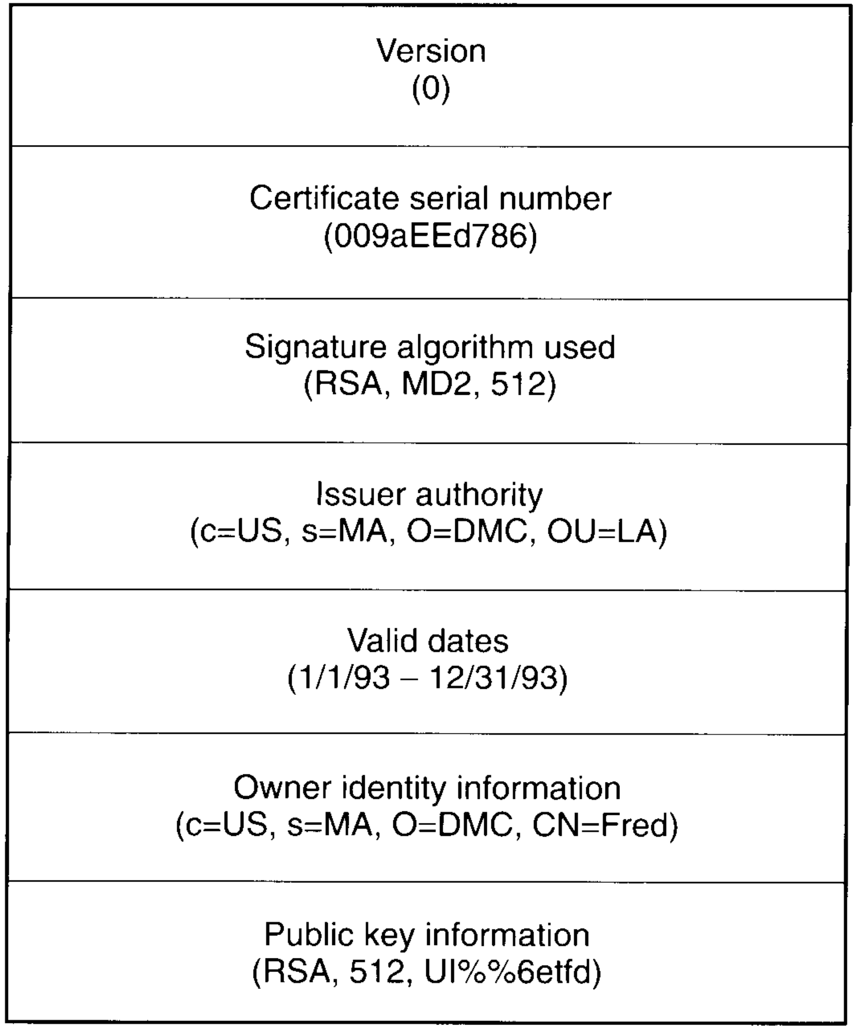
Privacy & Identity Lab

Jaap-Henk Hoepman

The Gospel of IRMA

Identity Management: X.509 certificates



Version
(0)

Certificate serial number
(009aEEd786)

Signature algorithm used
(RSA, MD2, 512)

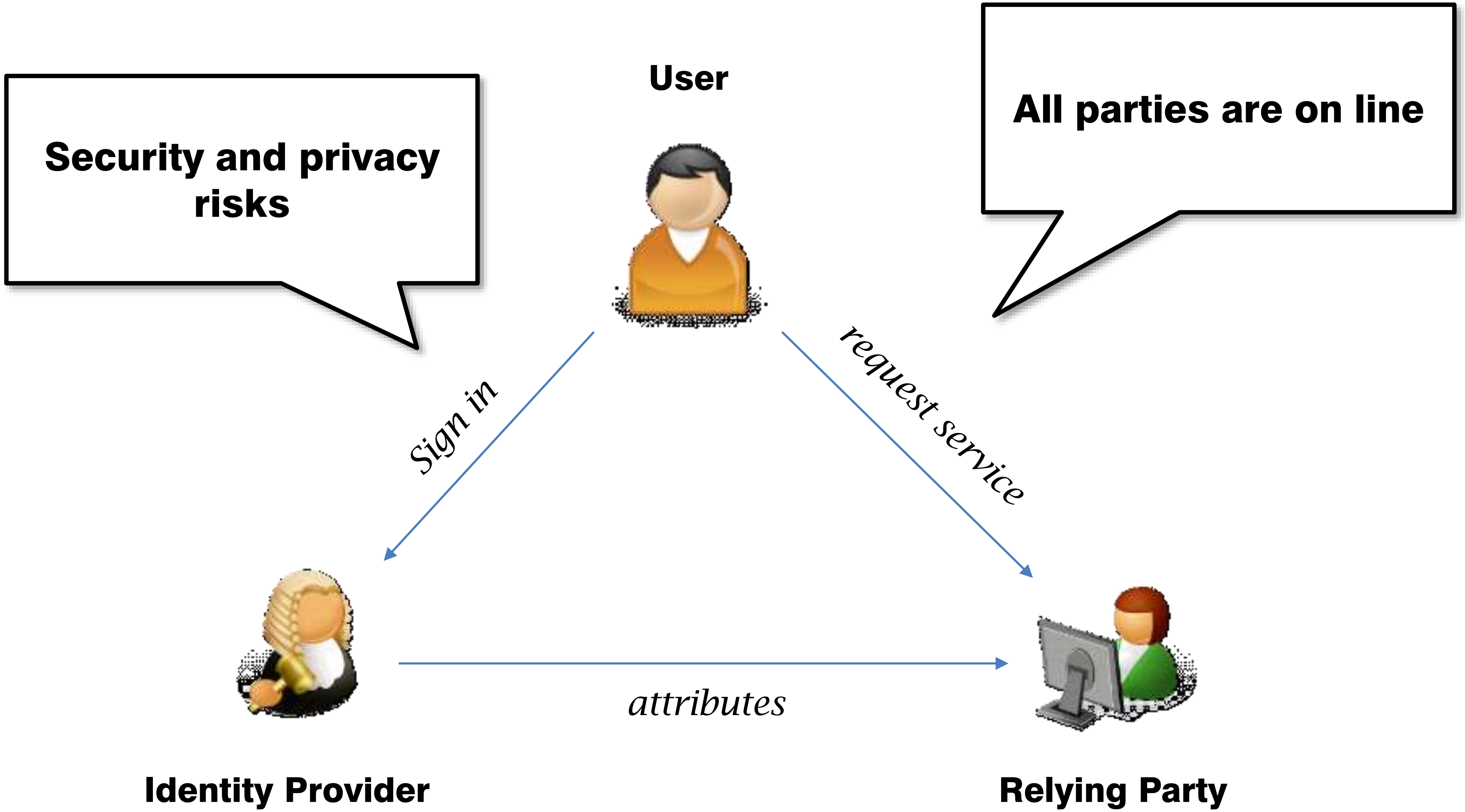
Issuer authority
(c=US, s=MA, O=DMC, OU=LA)

Valid dates
(1/1/93 – 12/31/93)

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

Public key information
(RSA, 512, UI%%6etfd)

Identity management: transitional



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

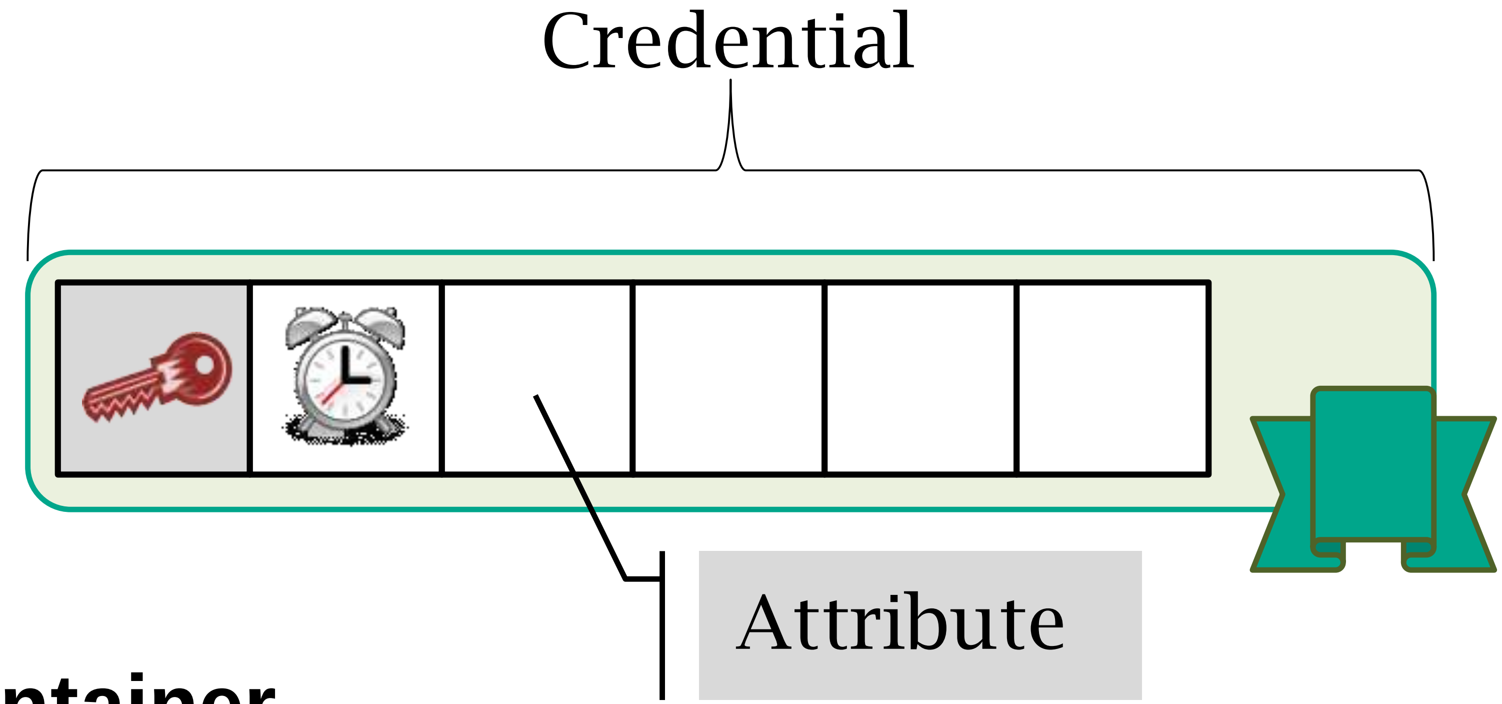
TNO

SURF NET

Attribute based credentials (ABC)

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

Credential

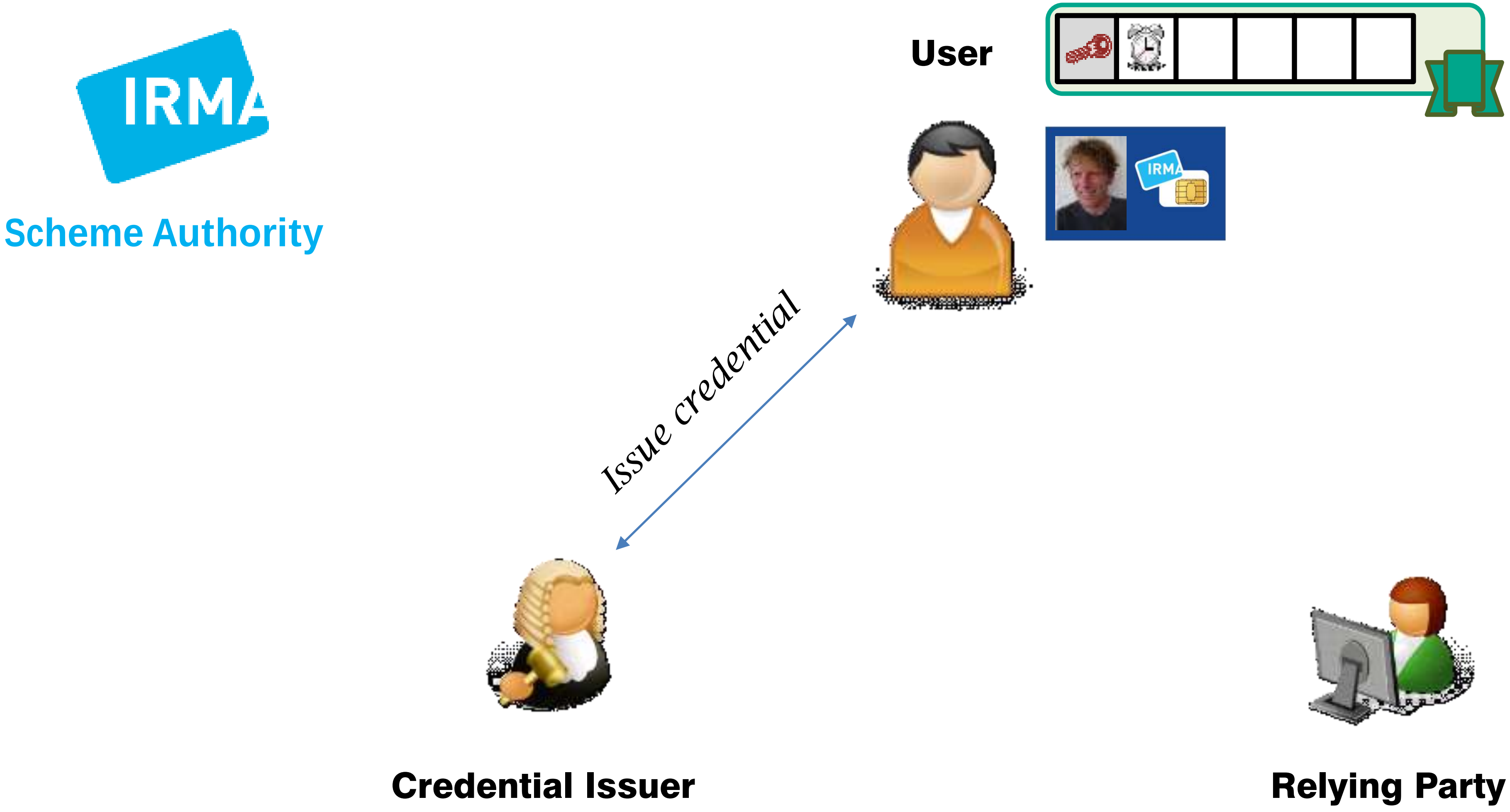


- **Secure container**
- **Issued and signed by *credential issuer***
- **Contains attributes, *selectively disclosable***

Using such credentials

- **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



Scheme Authority

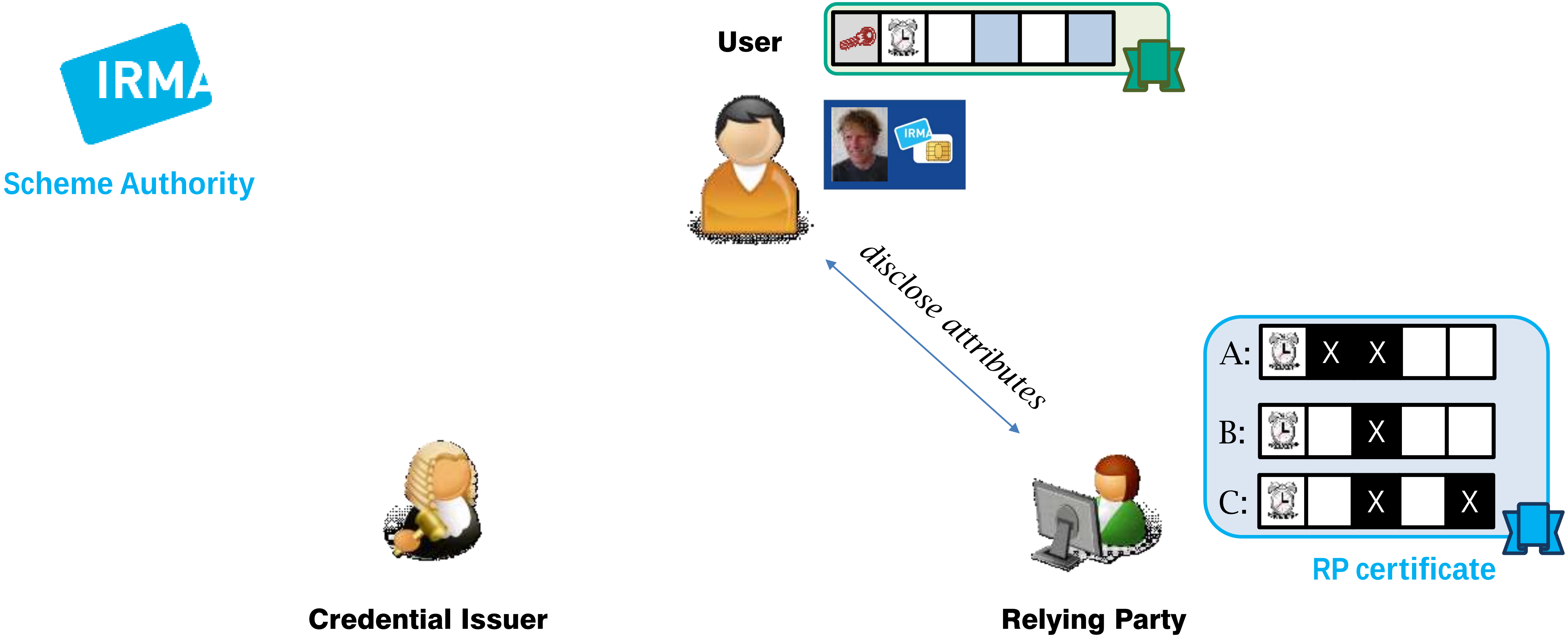
User

Issue credential

Credential Issuer

Relying Party

IRMA: disclosing some attributes



Scheme Authority

User

disclose attributes

A:	🕓	X	X		
B:	🕓		X		
C:	🕓		X		X

RP certificate

Credential Issuer

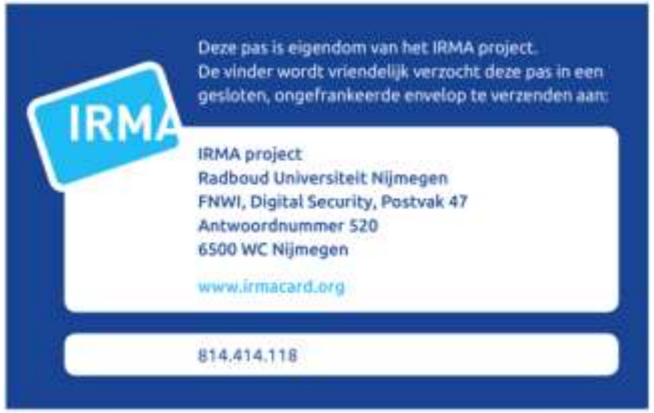
Relying Party

ABC Properties

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

The IRMA card (outside)

- **Outside**



Deze pas is eigendom van het IRMA project.
De vinder wordt vriendelijk verzocht deze pas in een gesloten, ongefrankeerde envelop te verzenden aan:

IRMA project
Radboud Universiteit Nijmegen
FNWI, Digital Security, Postvak 47
Antwoordnummer 520
6500 WC Nijmegen

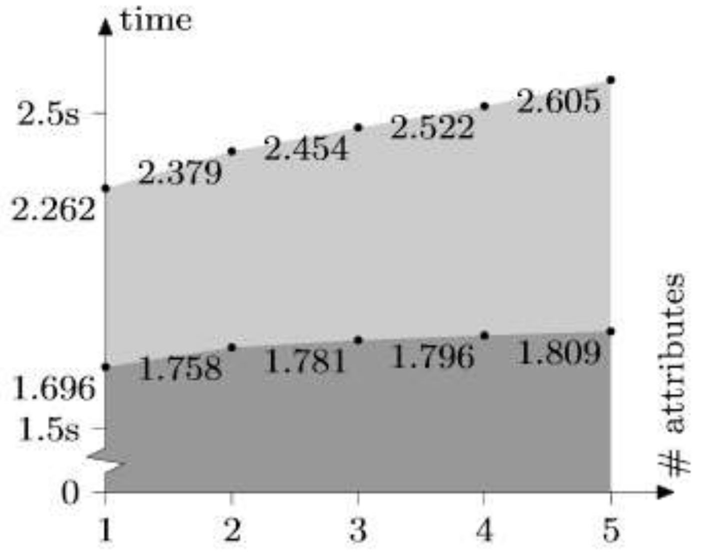
www.irmacard.org

814.414.118

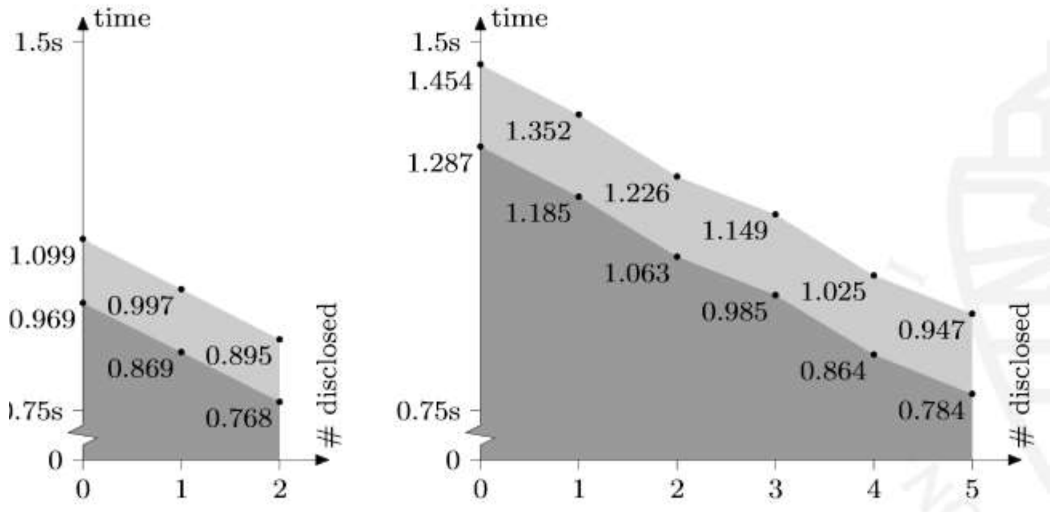
- **Contactless**
  - NFC phones/tablets as terminals
- **Inside**
  - Multos
  - SmartMX (NXP) is option
- **Credentials**
  - Idemix (by IBM)
  - 1024 bit

IRMA card Performance

- **Issuance**



- **Showing**



(a) 2 stored attributes

(b) 5 stored attributes

■ Computation ▒ Overhead

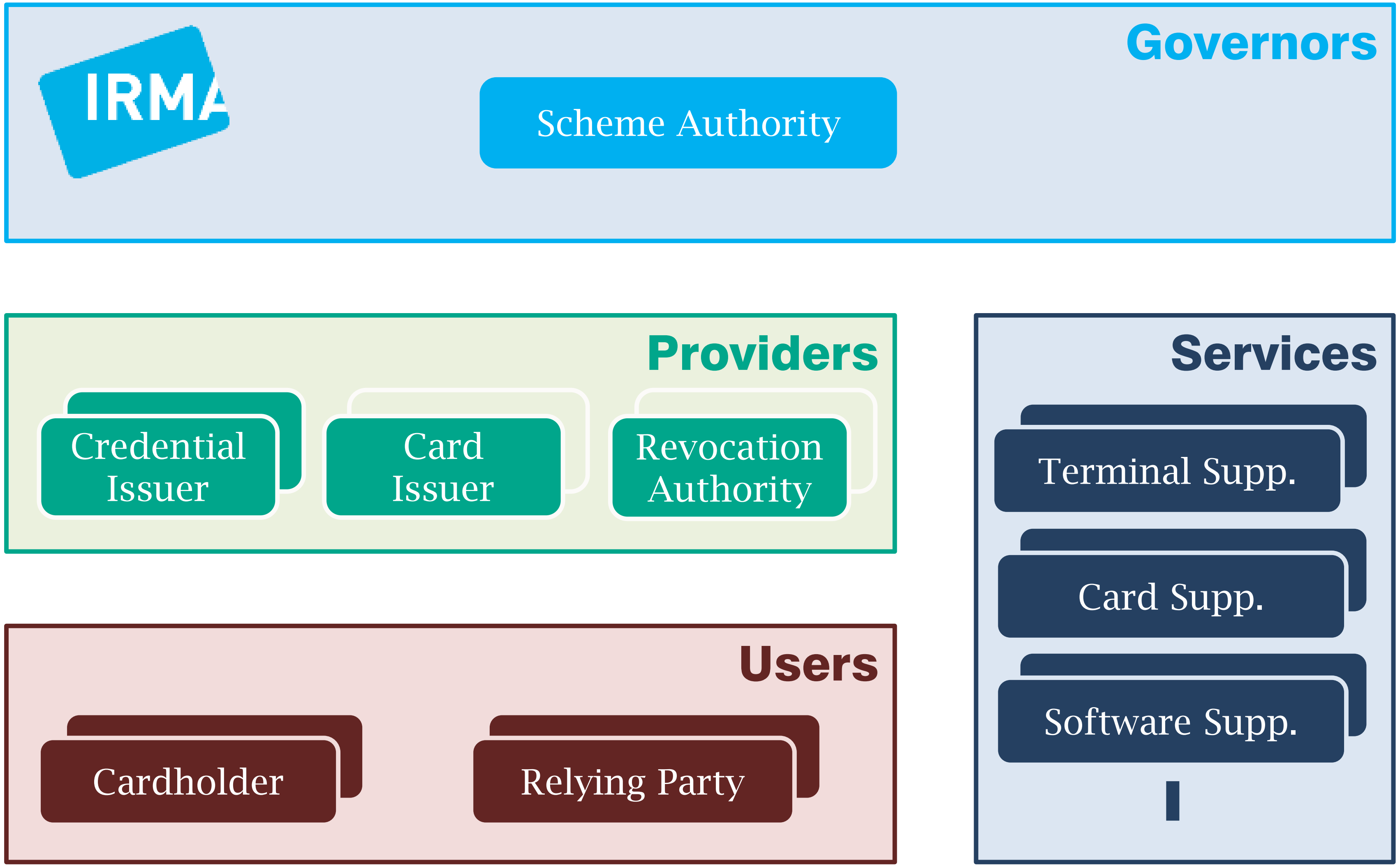
FULL on card implementation

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



Governors

Scheme Authority

Providers

Credential Issuer

Card Issuer

Revocation Authority

Services

Terminal Supp.

Card Supp.

Software Supp.

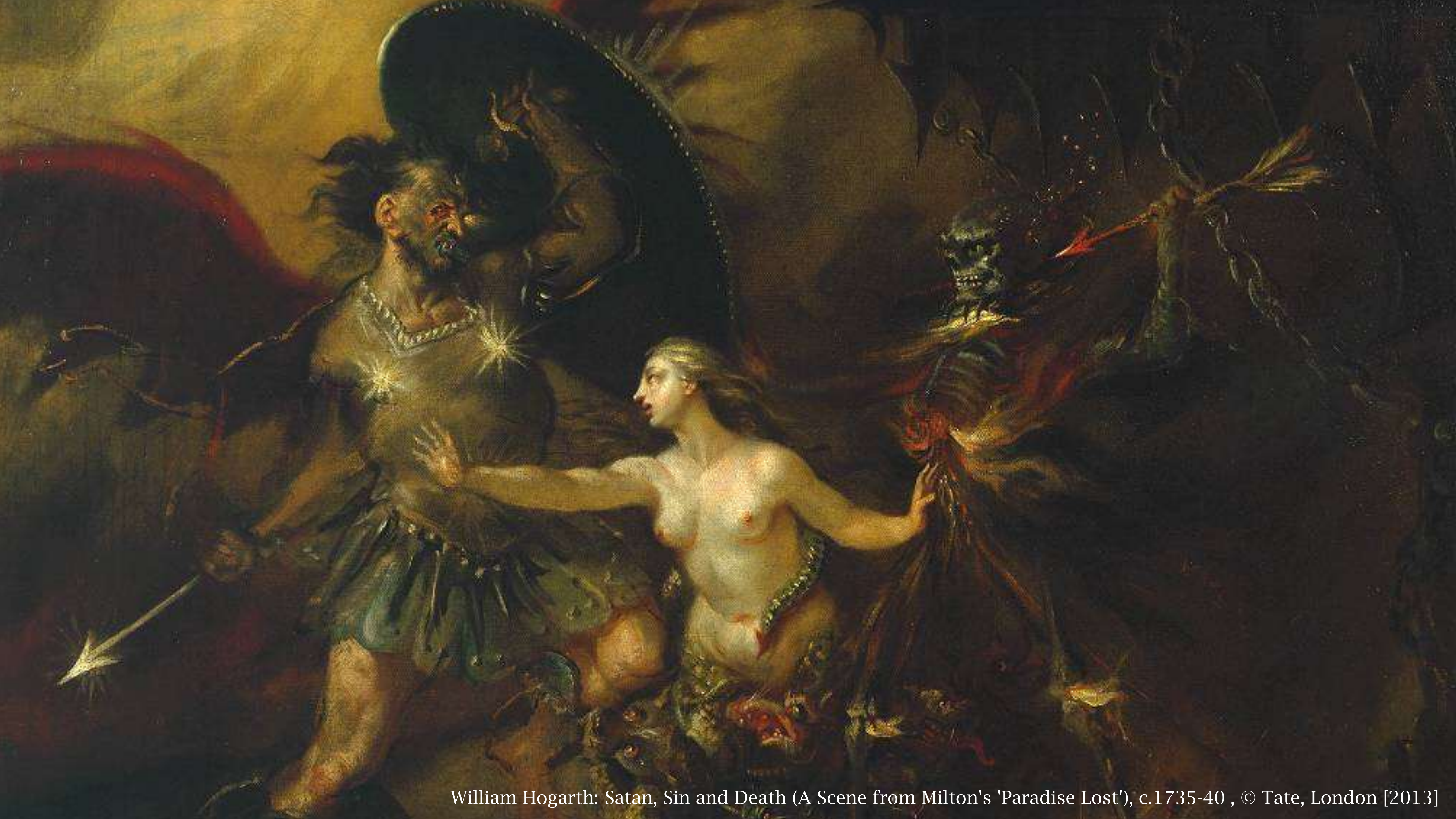
Users

Cardholder

Relying Party

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

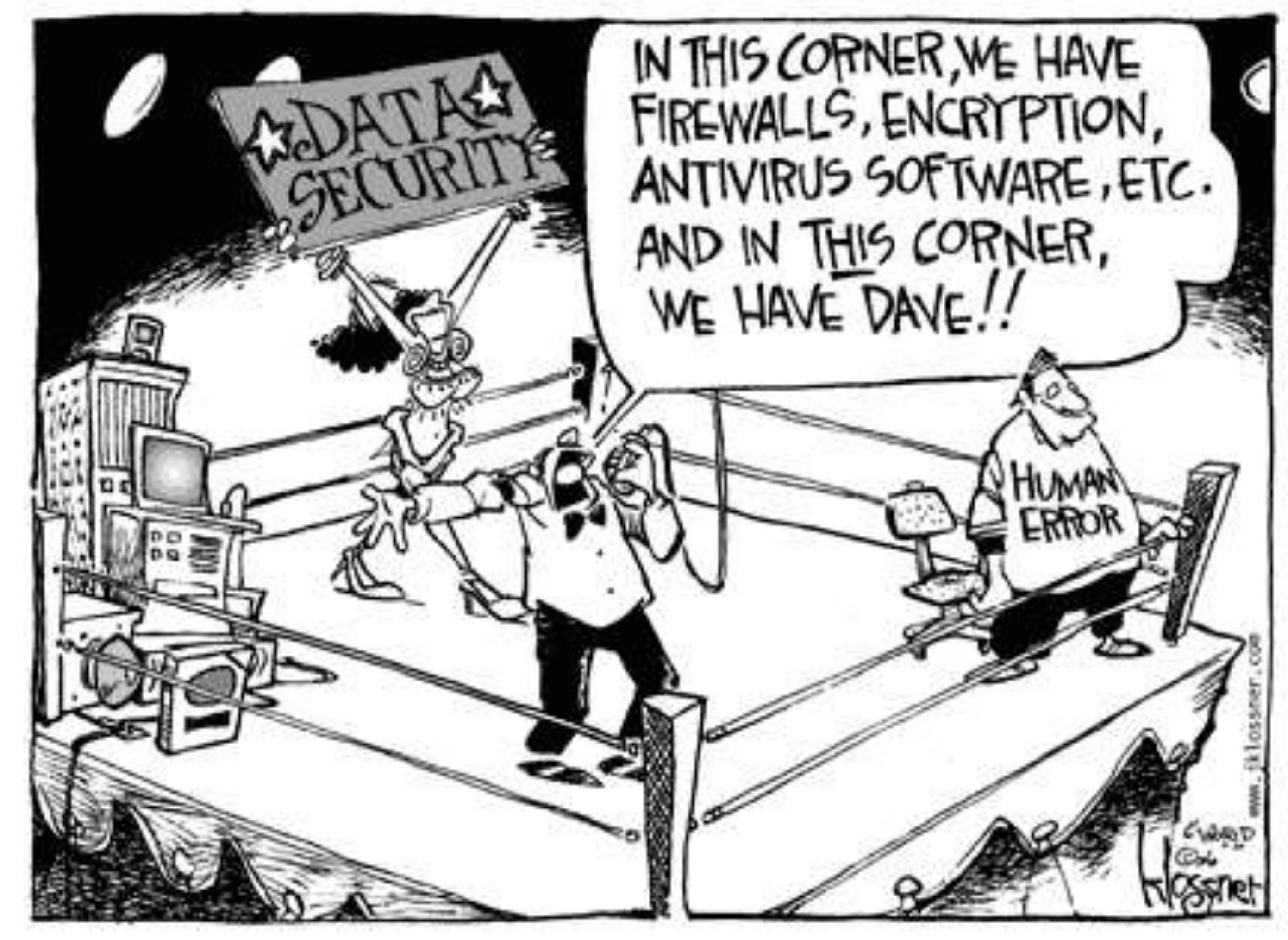
- **Real name policies**
- **No more lying about your address**
  - Shopping abroad…
- **Or your age**
  - Even if you think your children are old enough to be on Facebook

Tracking

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
www.jklossner.com
©06
Klossner

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

eID everywhere

BELGIQUE BELGIË BELGIEN BELGIUM

CARTE D'IDENTITE IDENTITEITSKAART PERSONALAUSWEIS IDENTITY CARD

SPECIMEN

Nom / *Name* **Le Meunier**

Prénoms / *Given names* **Jennifer Anne**

Lieu et date de naissance / *Place and date of birth* **Han-sur-Lesse 01 JAN 1985**

Sexe / *Sex* **F**

Nationalité
Nationality **Belge**

N° carte / *Card No*
000-5902781-01

Valide du - au / *Valid from - until*
01.01.2004 - 01.01.2009

Signature du titulaire / *Holder's signature*

0101002

EESTI VABARIIK
REPUBLIC OF ESTONIA

PEREKONNANIMI/SURNAME
MÄNNIK

EESNIMED/GIVEN NAMES
MARI-LIIS

SUGU/SEX **N/F**

KODAKONDSUS/CITIZENSHIP **EST**

SÜNNIAEG/DATE OF BIRTH **20.02.1973**

ISIKUKOOD/PERSONAL CODE **47302200234**

DOKUMENDI NUMBER/DOCUMENT NUMBER
A3051479

KEHTIV KUNI/DATE OF EXPIRY
04.10.2011

OMANIKU ALLKIRI/HOLDER'S SIGNATURE

BUNDESREPUBLIK DEUTSCHLAND
FEDERAL REPUBLIC OF GERMANY / REPUBLIQUE FEDERALE D'ALLEMAGNE

T22000129

PERSONALAUSWEIS
IDENTITY CARD / CARTE D'IDENTITE

Name/Surname/Nom
MUSTERMANN
GEB. GABLER

Vornamen/Given names/Prénoms
ERIKA

Geburtstag/Date of birth/Date de naissance 12.08.1964

Staatsangehörigkeit/Nationality/Nationalité DEUTSCH

Geburtsort/Place of birth/Lieu de naissance
BERLIN

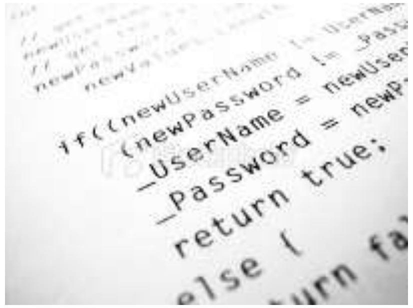
Gültig bis/Date of expiry/Date d'expiration
31.10.2020

938568

Unterschrift der Inhaberin/des Inhabers - Signature of bearer - Signature de la titulaire/du titulaire

Mustermann

Technology alone is helpless



```
if((newUserName != UserNa
   (newPassword != _Pass
   _UserName = newUser
   _Password = newP
   return true;
else {
   return fa
```

Thank you.

www.irmacard.org

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