The Gospel of IRMA

Jaap-Henk Hoepman

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

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
IRMA: disclosing some attributes

ABD Properties

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

The IRMA card (outside)

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

IRMA card Performance

- **Issuance**
- **Showing**

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**
- **Providers**
  - Cardholder
  - Revocation Authority
- **Users**
  - Cardholder
  - Relying Party

**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

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

Current limitations

- 1024 bit RSA
  - Really too low
- Only equality proofs
- Revocation
  - Being implemented
- Weak binding of card to cardholder
- Lack of pilots
Thank you.

IRMA

www.irmacard.org

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