The Gospel of IRMA

Identity Management: X.509 certificates

Security and privacy risks

Identity management: transitional

Attribute based credentials (ABC)

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

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, ISIN, address)
  - Student card (student number, institute)
  - Emergency health info (name, blood group, allergies)

IRMA: issuing a credential

IRMA: disclosing some attributes

ABC Properties

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

The IRMA card (outside)

- **Outside**
  - NFC phones/tablets as terminals

- **Inside**
  - Multos
  - SmartMX (NXP) is option

- **Credentials**
  - Idemix (by IBM)
  - 1024 bit
IRMA card Performance

- Issuance
- Showing

The Gospel of IRMA, 28-12-2013

The IRMA terminals

The Gospel of IRMA, 28-12-2013

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

The Gospel of IRMA, 28-12-2013

IRMA roles

Governors

Scheme Authority

Providers

Card Issuer

Revocation Authority

Services

Terminal Supp.

Software Supp.

Card Supp.

Relying Party

Users

Cardholder

Relying Party


The Gospel of IRMA, 28-12-2013

Current limitations

- 1024 bit RSA
  - Really too 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

The Gospel of IRMA, 28-12-2013
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

Pickpocketing

- The Card Management app implements an API that makes it easy to pickpocket IRMA cards
And many many more

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

Technology alone is helpless

Technology alone is helpless