Jaap-Henk Hoepman
The Gospel of IRMA
### Identity Management: X.509 certificates

<table>
<thead>
<tr>
<th>Field</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>(0)</td>
</tr>
<tr>
<td>Certificate serial number</td>
<td>(009aEEed786)</td>
</tr>
<tr>
<td>Signature algorithm used</td>
<td>(RSA, MD2, 512)</td>
</tr>
<tr>
<td>Issuer authority</td>
<td>(c=US, s=MA, O=DMC, OU=LA)</td>
</tr>
<tr>
<td>Valid dates</td>
<td>(1/1/93 – 12/31/93)</td>
</tr>
<tr>
<td>Owner identity information</td>
<td>(c=US, s=MA, O=DMC, CN=Fred)</td>
</tr>
<tr>
<td>Public key information</td>
<td>(RSA, 512, UI%=6etfd)</td>
</tr>
</tbody>
</table>
Identity management: transitional

Security and privacy risks

All parties are on line

User

Identity Provider

Relying Party

attributes

Sign in

request service
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
Attribute based credentials (ABC)

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

Credential Issuer → Issue credential → User → Relying Party
IRMA: disclosing some attributes
ABC 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

![Graphs showing time vs. attributes for Issuance and Showing, with shaded areas labeled Computation and Overhead, and a note indicating 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
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 dark side of IRMA

Satan, hel, de verleiding

The Gospel of IRMA, 28-12-2013

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
Scheme authority

- Not independent
- Not trusted
User in control: user made responsible

In this corner, we have firewalls, encryption, antivirus software, etc. And in this corner, we have Dave!!
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
elD everywhere
Technology alone is helpless
Thank you.

www.irmacard.org