Why X.509 and Identity Management Don’t Mix

Ben Laurie
The Bunker Secure Hosting
and
The Apache Software Foundation
Requirements for IM

- Statements must be:
  - Verifiable
  - Minimal
  - Unlinkable
X.509 and IM

- X.509 certificates are:
  - Verifiable
  - Minimal
  - Unlinkable
Single-use X.509?

- Verifiable
- Minimal
- Unlinkable
Self-signed X.509?

- Self-signed X.509 certs are:
  - **Verifiable**
  - Minimal
  - Unlinkable
And Don’t Forget...

 Unless the underlying network provides anonymity everything is linkable anyway