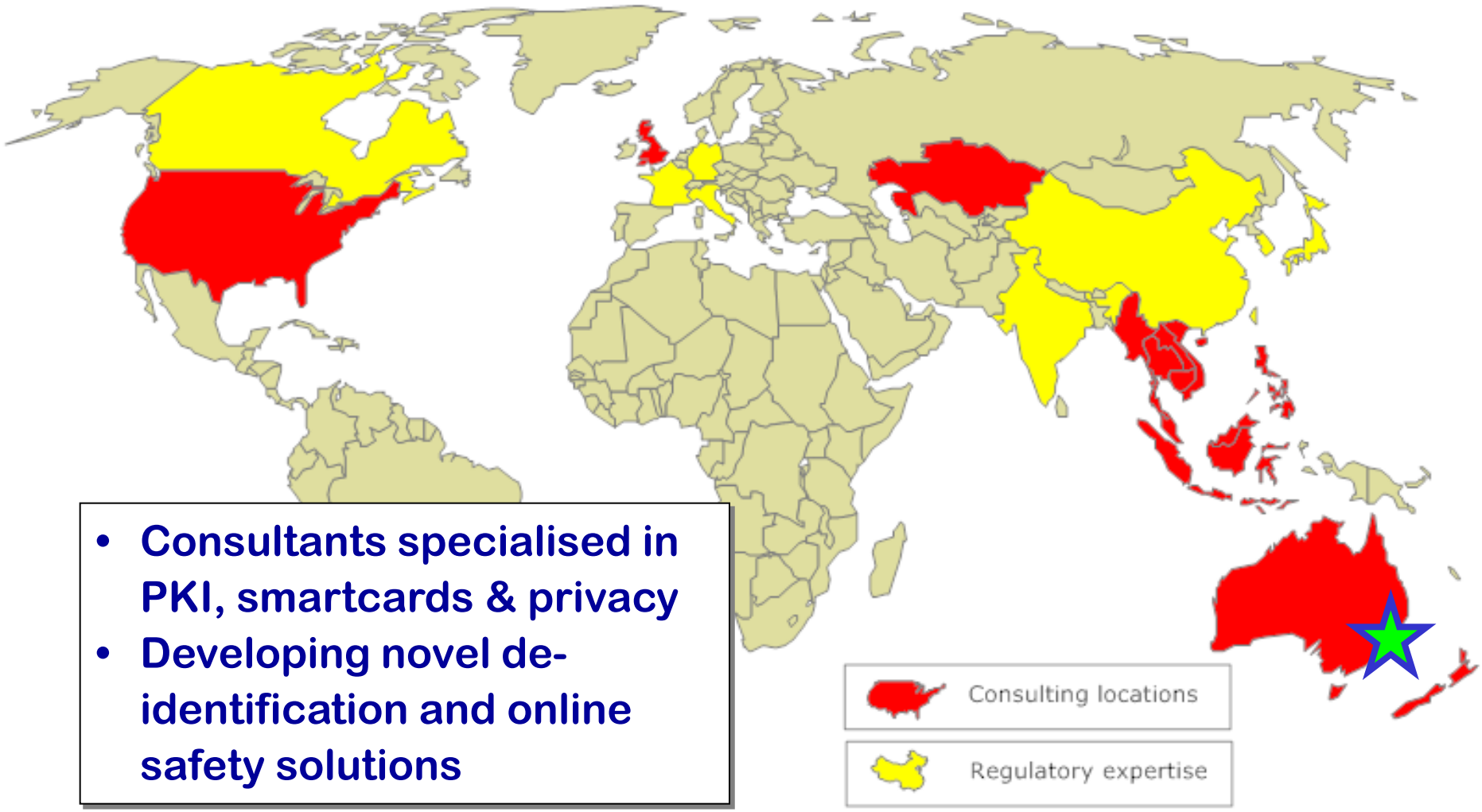
Public Key Superstructure

It's PKI Jim, but not as we know it!

7th Annual "IDtrust" Symposium
5 March 2008, Gaithersburg MD, USA

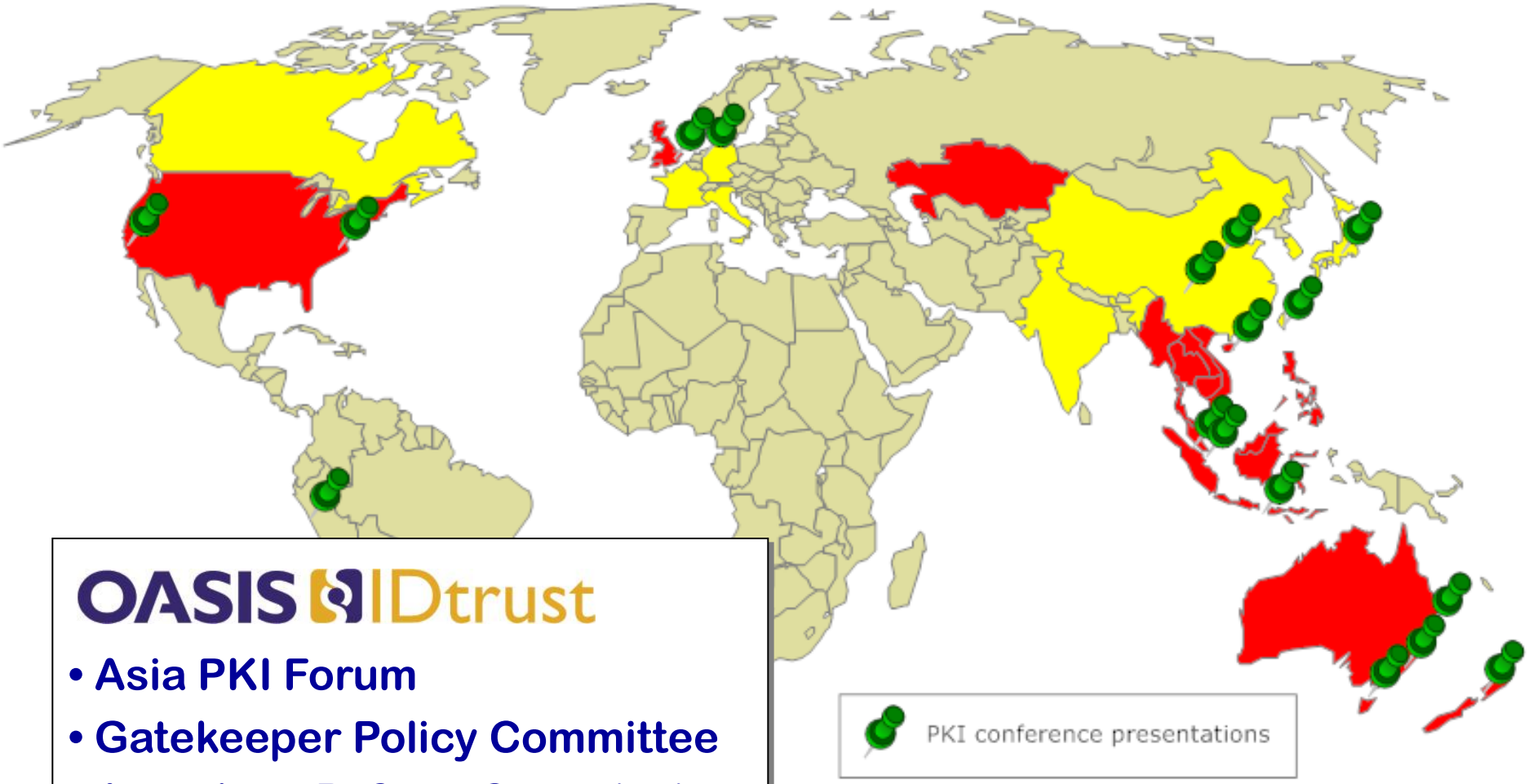
Stephen Wilson
Lockstep Consulting Pty Ltd

About Lockstep



- Consultants specialised in PKI, smartcards & privacy
- Developing novel de-identification and online safety solutions

About Lockstep



OASIS IDtrust

- Asia PKI Forum
- Gatekeeper Policy Committee
- Aust. Law Reform Commission

Historical PKI experience

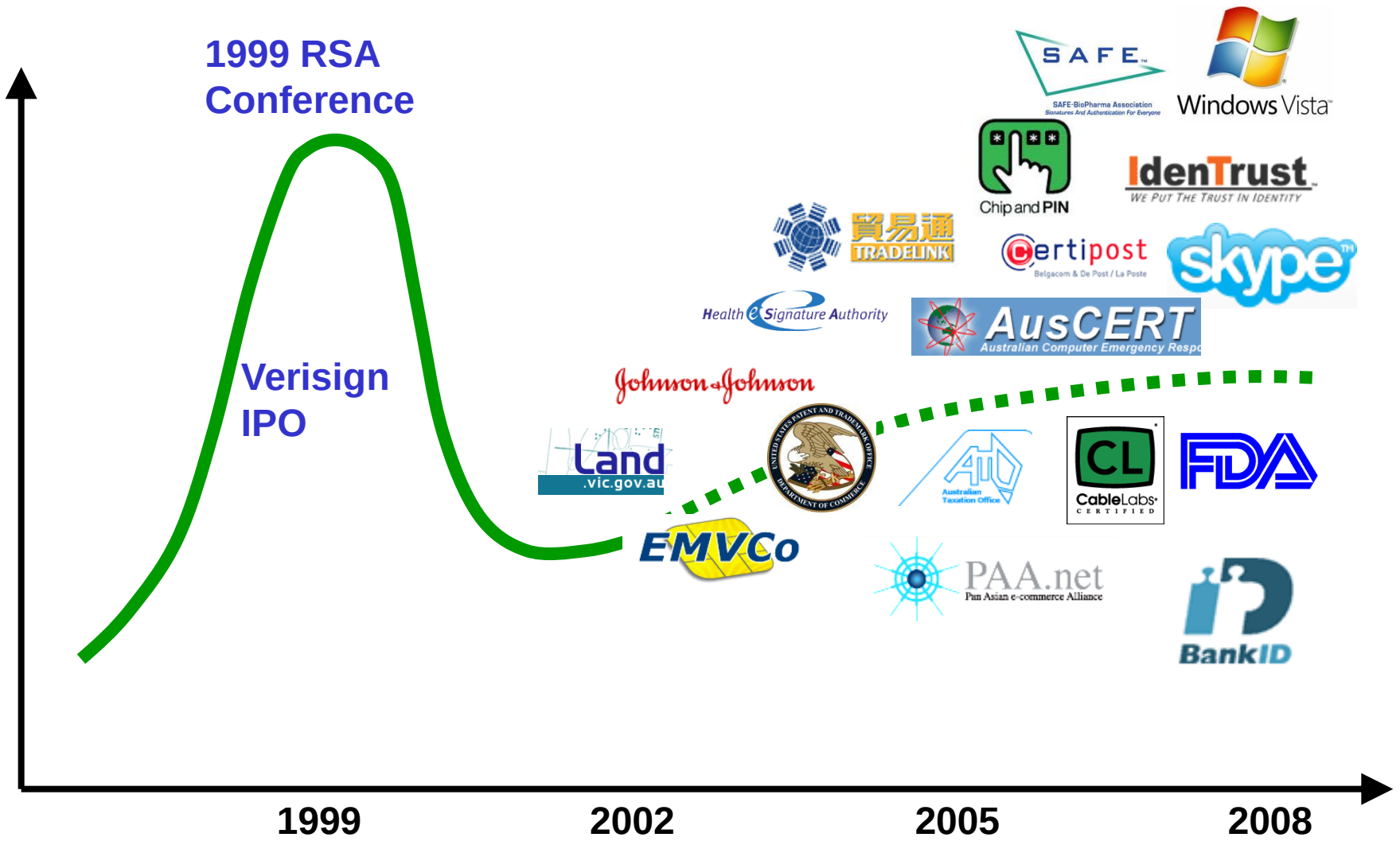
The passport metaphor

- Non-descript applications
  - impossible for CAs to manage risk
- Stranger-to-stranger e-business
  - “It’s good to trust but it’s better not to”
- Novel TTP business models
  - Imposed incredible CPSs upon users
- Notion of a single identity
  - “Interoperability” = cross certification

“Cross-certification and policy mapping has been a rat hole that has sucked up vast amounts of energy better spent elsewhere”

Anonymous, Feb 2008

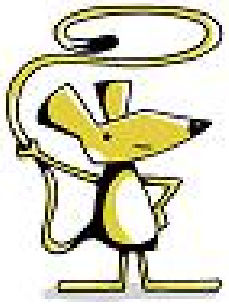
PKI thickets

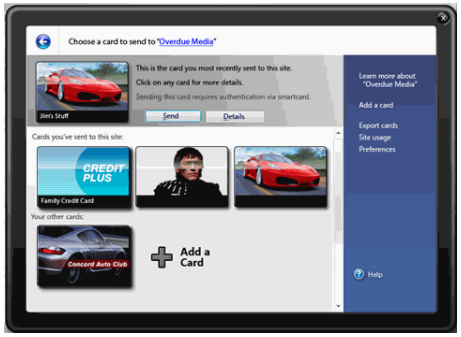


PKI in practice

- Works best in closed communities
  - Automates transactions *in context*
  - This is a Good Thing
- Embedded keys & certificates
- Fits with *identity plurality*

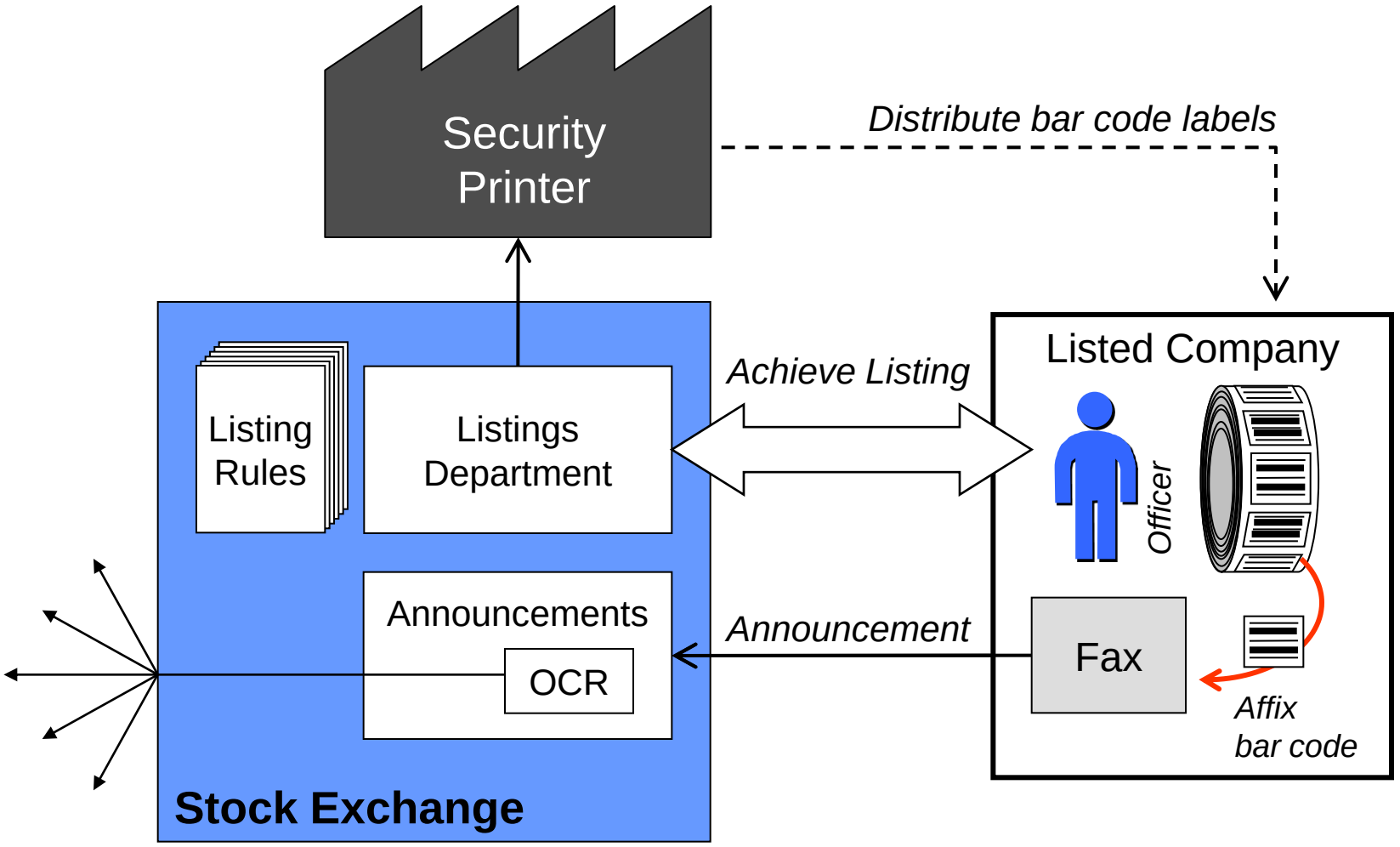
OpenID



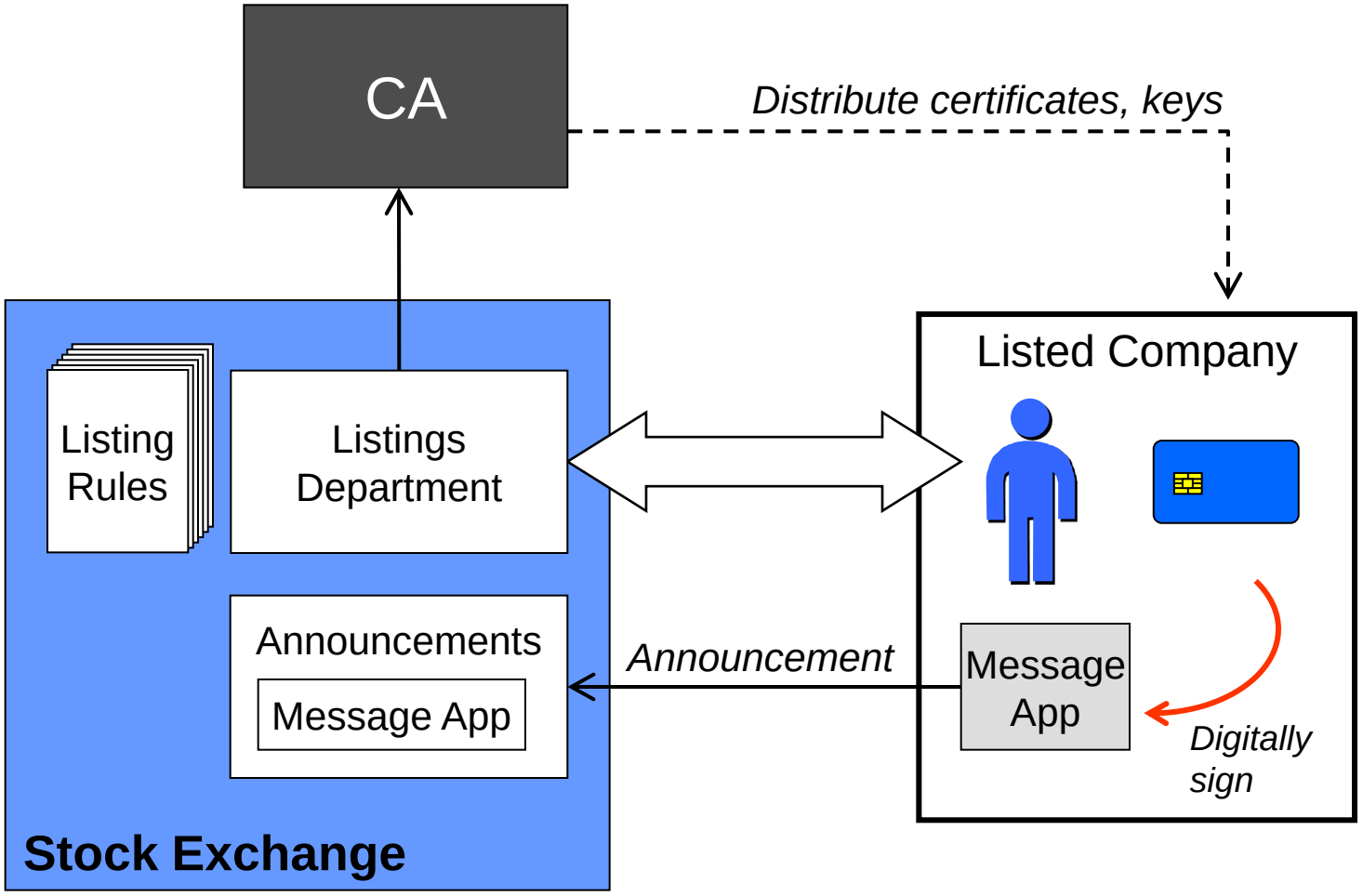


PK Superstructure

CA as *Security Printer*



CA as *Security Printer*

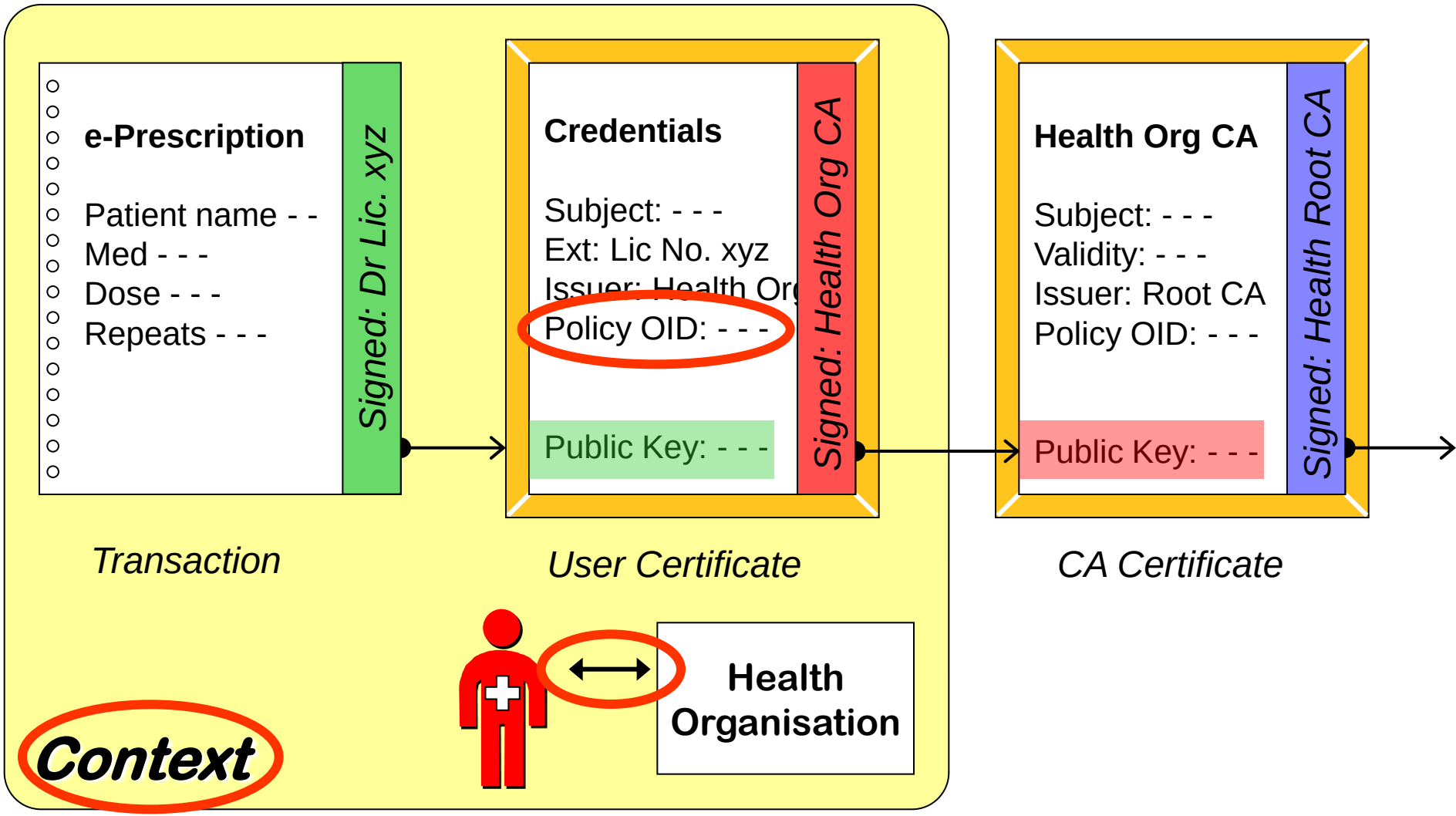


Security printer implications

- Decouples registration from production
- Manages risks associated with registration & production separately

- No contract between Subscriber & CA
- No exposure of CPS to Subscriber
- Easier to novate CA service providers
- Accreditation not affected by new Policies

“Relationship Certificates”



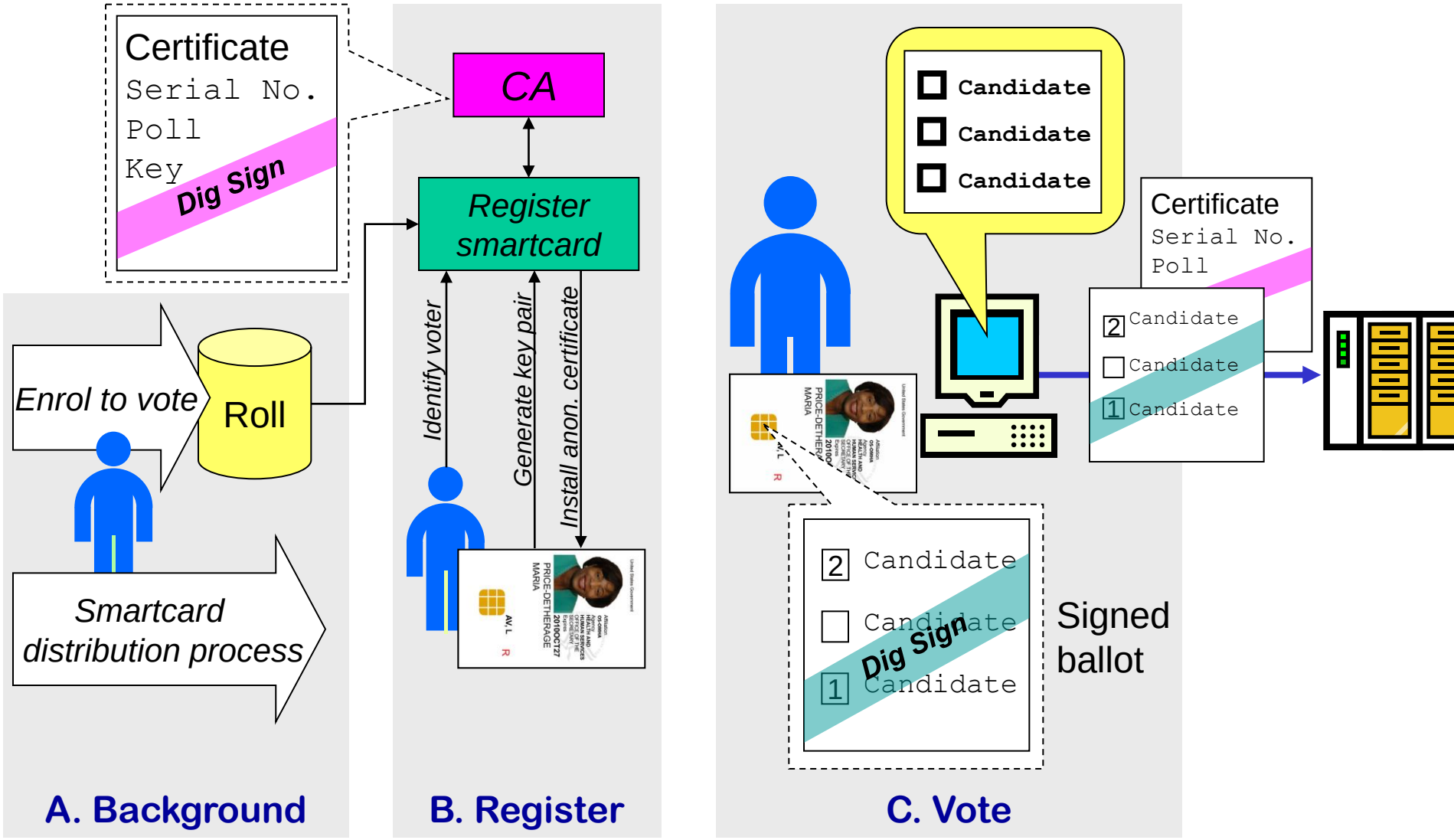
“Relationship Certificates”

- Form of “Authorization PKI”
- Kill the holy cow of authentication being primary over authorization

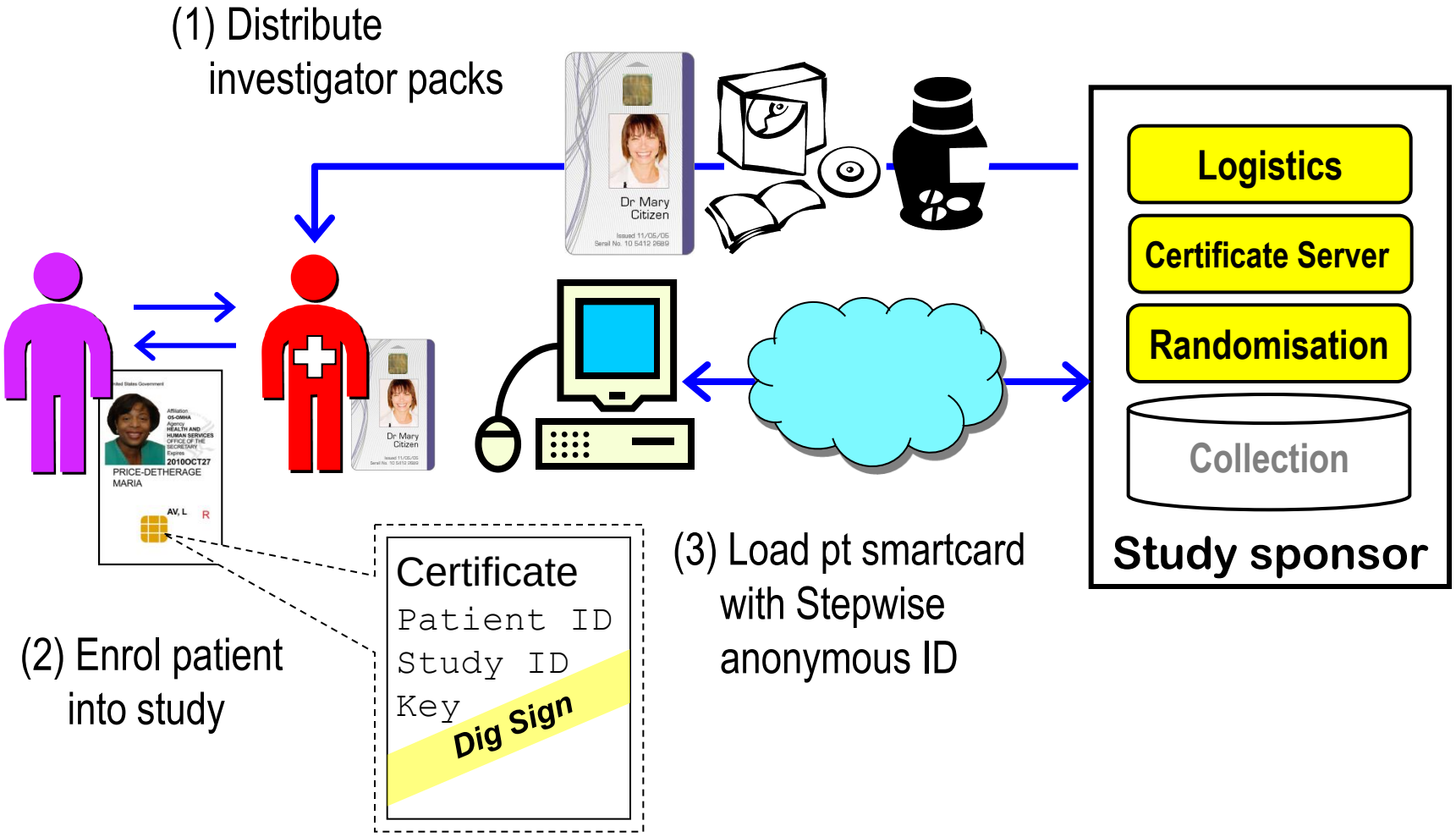
- Preserves X.509 formats, software

- *Not SPKI*: no ‘primary’ ID certificate
- *Not Attribute Certs*: we can *sign* with cert

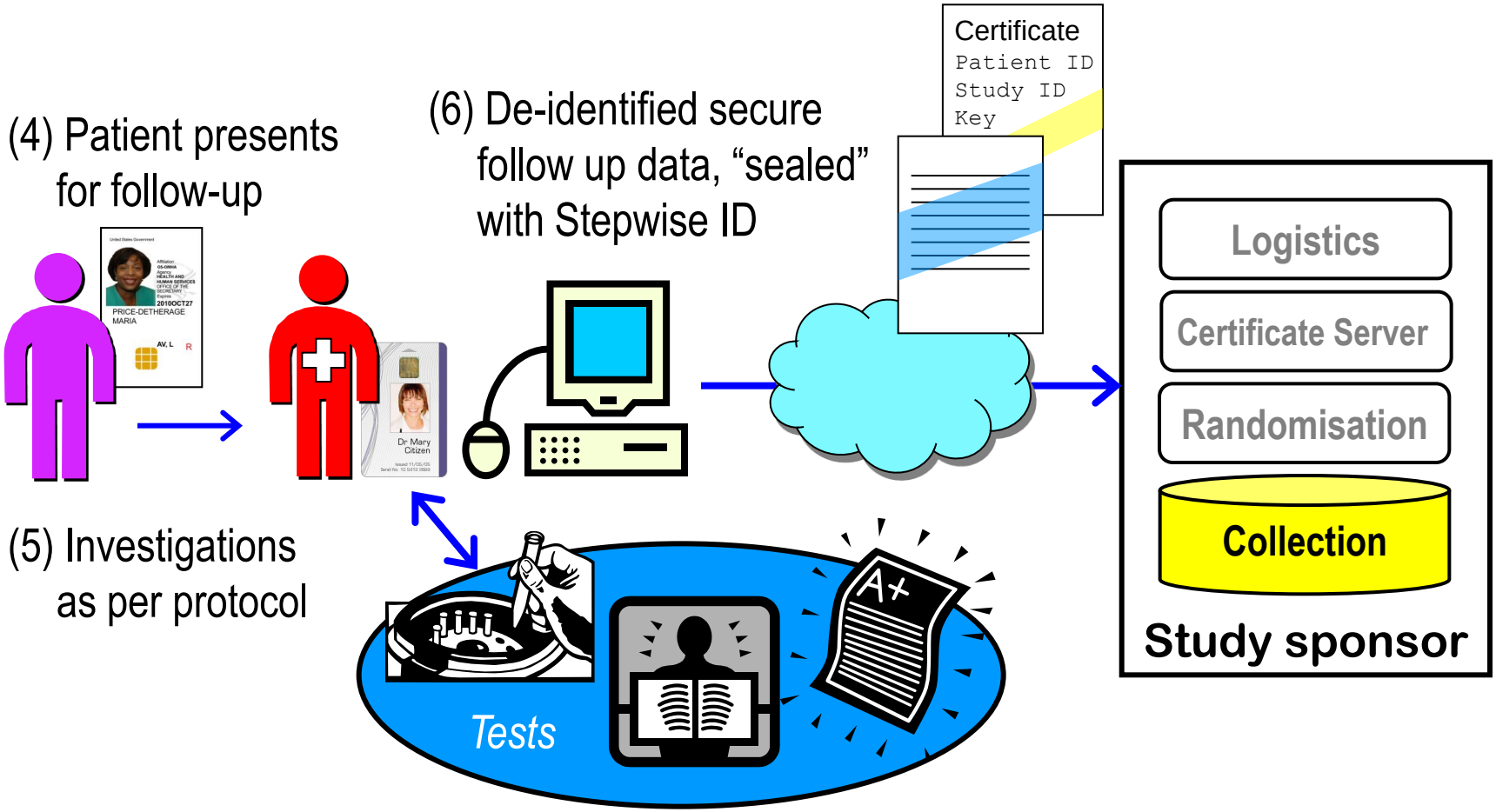
Lockstep anonymous e-voting



Lockstep clinical study privacy



Lockstep clinical study privacy



Discussion

See also www.lockstep.com.au/technologies

OASIS IDtrust

swilson@lockstep.com.au