Will client digital certificates ever fly?

Presentation to the UK Unix Users Group
Birmingham
25 February 2005

The Digital Certificate Operation in a Complex Environment Project

- What a mouthful.
  [dəˈkʌtʃi] …bless you!
- What were we trying to do?
  - "To provide a detailed implementation and evaluation report of 'real world' digital certificate services at the University of Oxford"
    - Attempt to learn from the experience of others
    - Development/implementation of, a public key infrastructure…
    - Evaluations
    - Dissemination

This talk

- The staff
- The aims
- What ARE digital certificates?
- (Summary of PKI)
- The DCOCE architecture
- Requirements and challenges
- Findings and conclusions (for PKI and more generally)

Staff

- Project team:
  - Project Manager: Mark Norman
  - Evaluators: Alun Edwards (OUCS), Johanneke Sytsema (SERS), James Wilson (OUCS)
  - Systems Developer: Christian Fernau
- Project Board:
  - Mike Fraser/Paul Jeffreys (Co-Project Directors)
  - Frances Boyle (SERS)

The aims (in short…)

- Use digital certificates for authentication at Oxford (and elsewhere)
  - Involved ‘building’ a PKI and
  - making some services ‘certificate aware’
- Look at usability and issuing mechanisms
  - Registration, renewal, revocation etc.
- Have an open mind about the success
  - Maybe balance the high security (potential) with ease of use/implementation… …pragmatism?

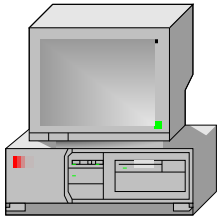
What ARE digital certificates?

- Lots of jargon:
  - X.509
  - Public key infrastructure
  - Signing, encryption, hashes
- Where have you seen them before?
  - Secure Sockets Layer (SSL)
  - (DCOCE is about personal or *client certificates*)
- But *what are* they?
  - Little bits of digital information that are *signed* by a trusted authority

DCOCE was interested in…

- Authentication
- (Unfortunately, not signing or encryption)

Web server

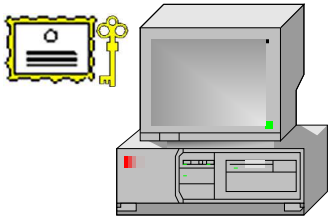


End user

DCOCE was interested in…

- Authentication
- (Unfortunately, not signing or encryption)

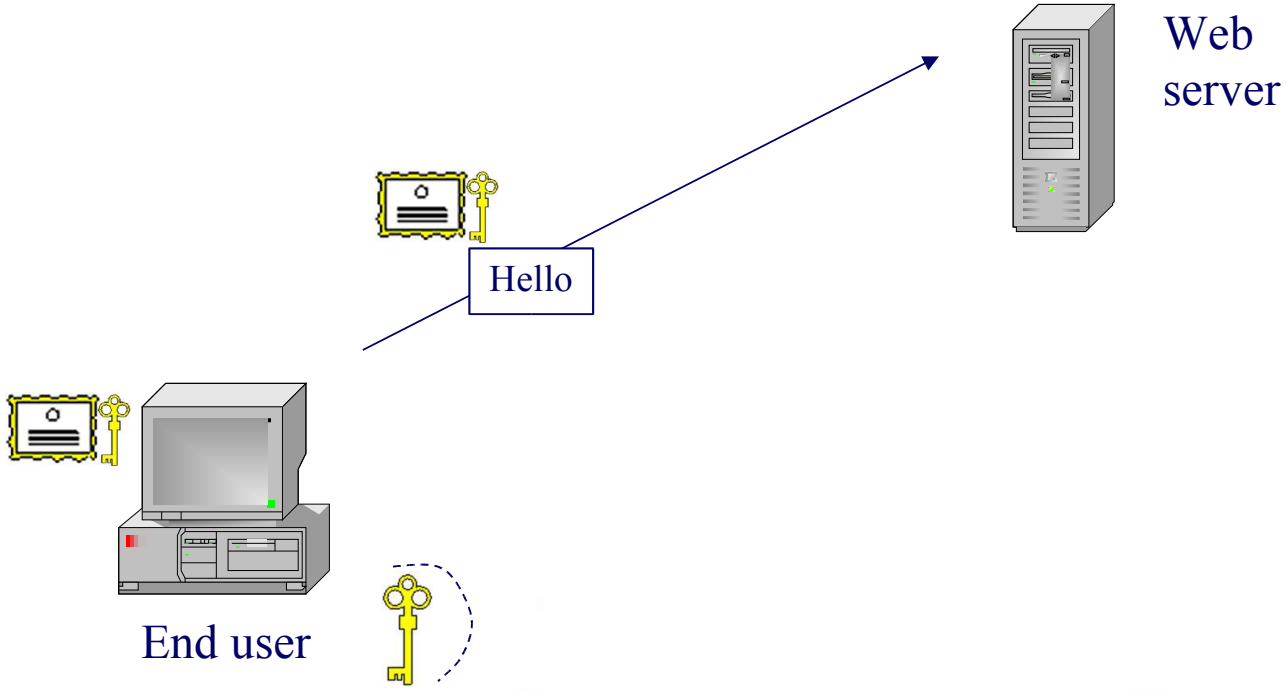
Web server



End user

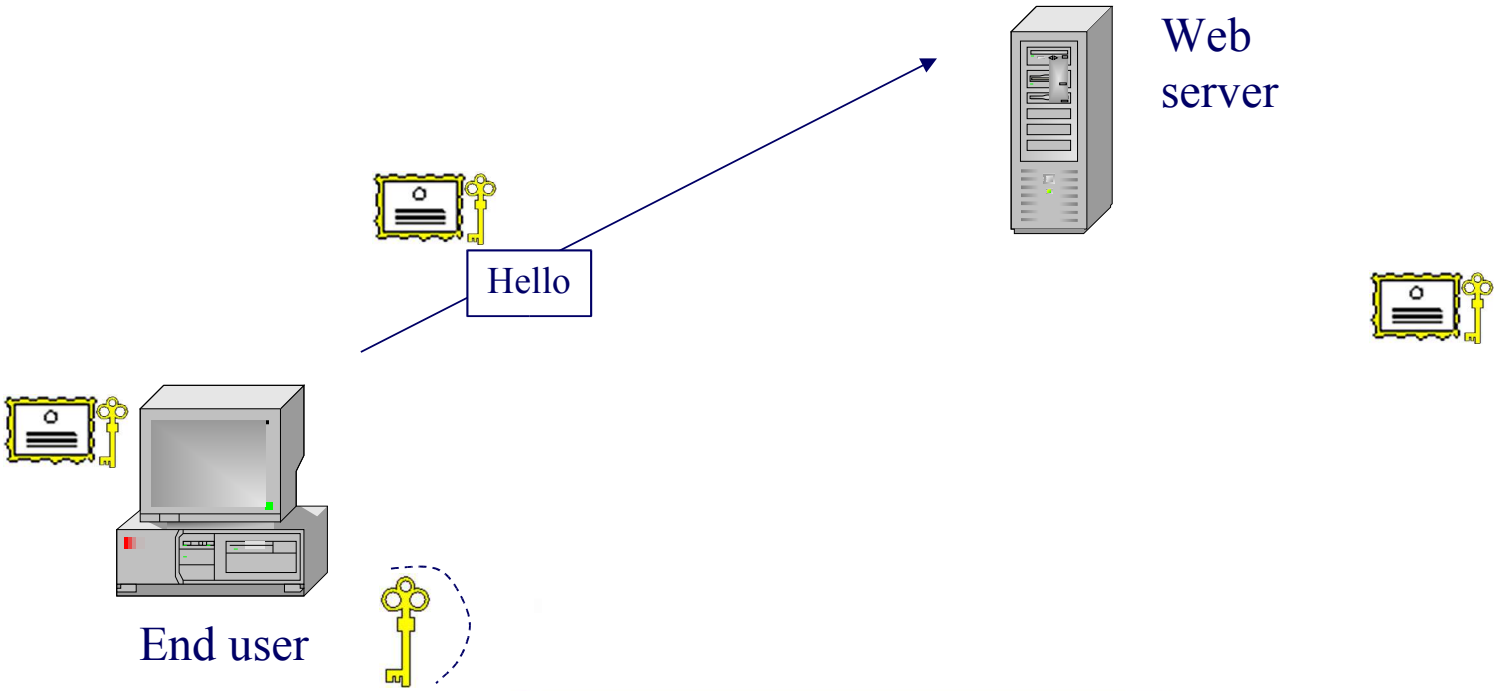
DCOCE was interested in…

- Authentication
- (Unfortunately, not signing or encryption)



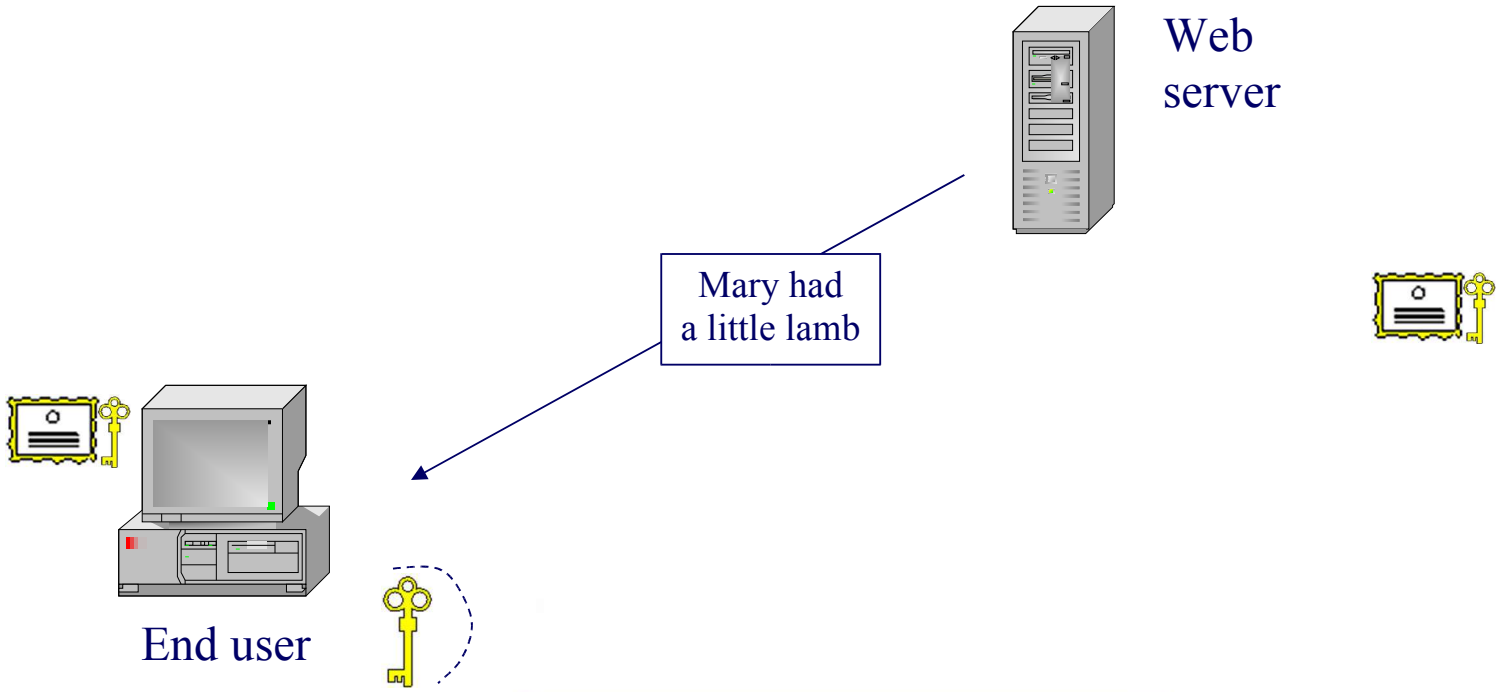
DCOCE was interested in…

- Authentication
- (Unfortunately, not signing or encryption)



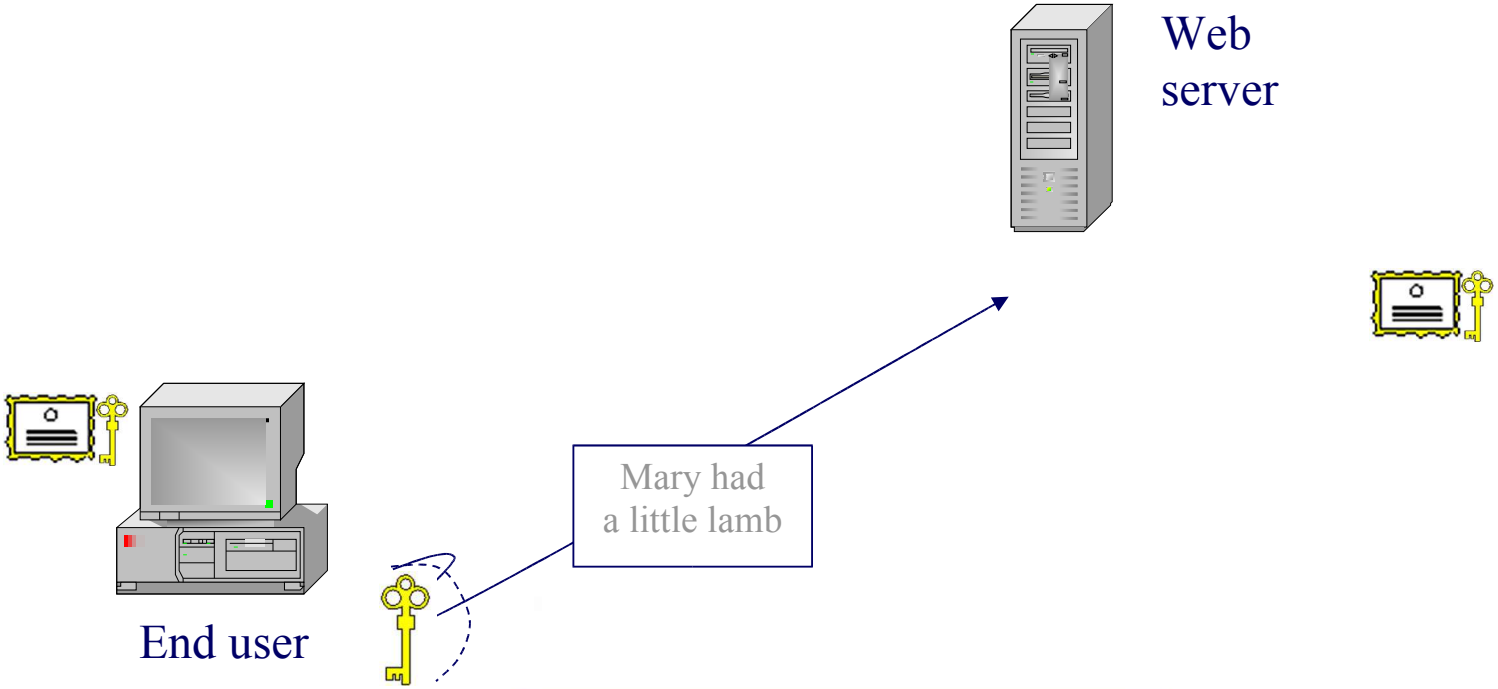
DCOCE was interested in…

- Authentication
- (Unfortunately, not signing or encryption)



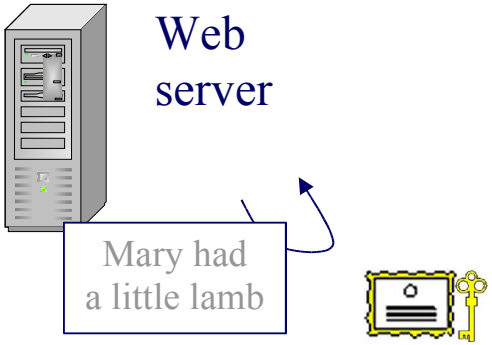
DCOCE was interested in…

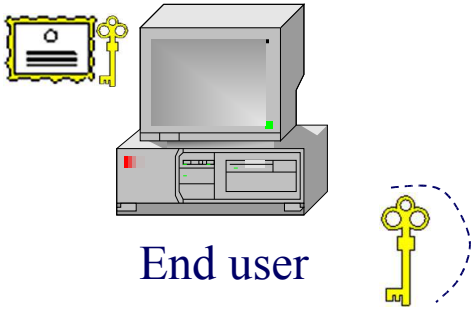
- Authentication
- (Unfortunately, not signing or encryption)



DCOCE was interested in…

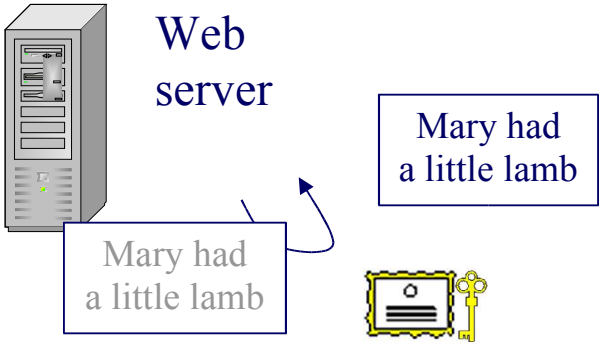
- Authentication
- (Unfortunately, not signing or encryption)

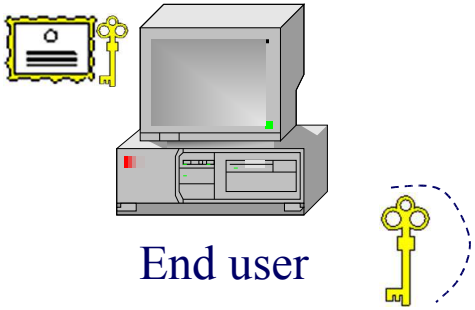




DCOCE was interested in…

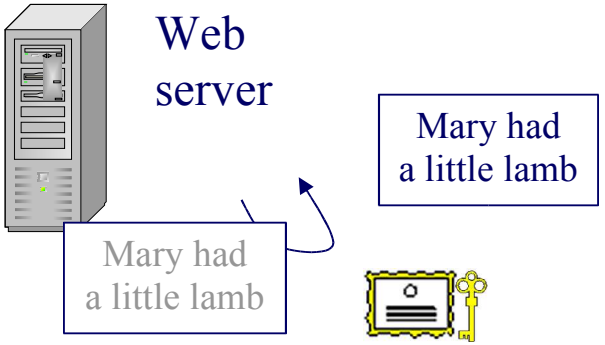
- Authentication
- (Unfortunately, not signing or encryption)

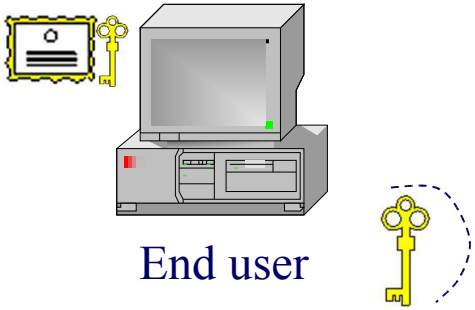




DCOCE was interested in…

- Authentication
- (Unfortunately, not signing or encryption)

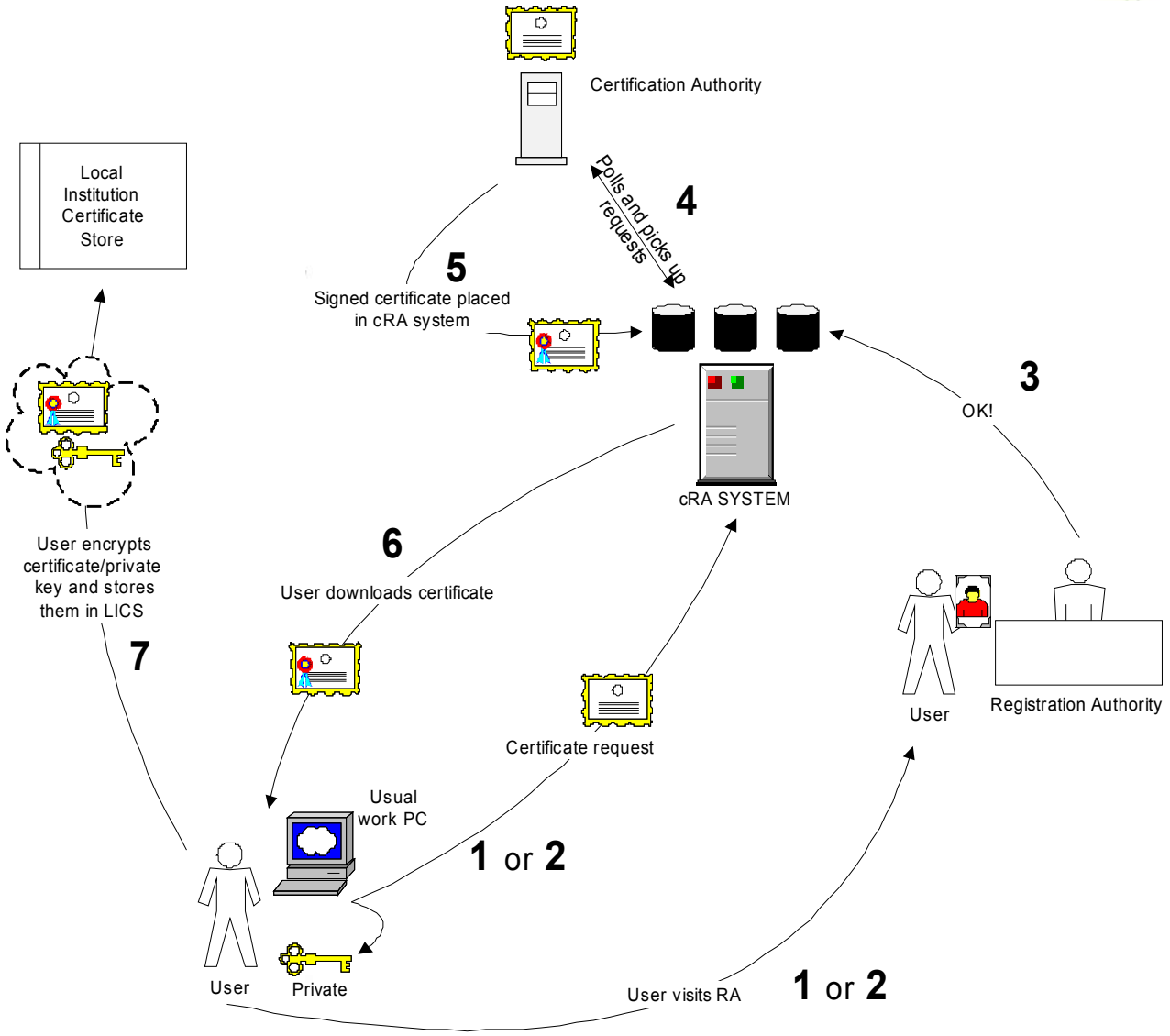




OK. The server is happy that the end user is a holder of a genuine Oxford certificate!

Oxford University Computing Services

Architecture summary


Certification Authority
Local Institution Certificate Store
Polls and picks up requests
4
5
Signed certificate placed in cRA system
3
OK!
cRA SYSTEM
6
User downloads certificate
User encrypts certificate/private key and stores them in LICS
7
Certificate request
Usual work PC
1 or 2
User
Private
User
Registration Authority
User visits RA
1 or 2

What are the real challenges?

- Usability, usability, usability
  - Concepts (currently) are too complex for most end users
  - Need to help them guard their private key
  - Disincentives against doing silly things
    - e.g. our Local Institution Certificate Store (LICS)
- Browser support isn't brilliant
- Moving from machine to machine
    - So why not keep your certificate and private key on a central server, protected by a password!?!?!

Usability vs Security

A quick indication of the ‘requirements’

- Basic level assurance
  - For most University users
  - Medium level for the Grid and others
- How to scale the registration
  - Trusting the registration servers
  - Generating keys locally
  - Being secure
- Mobility problems
  - Save cert.s and private keys on a central server?
  - Or use ‘devices’?

PKI makes some security experts focus on the wrong things

The privacy thing

- Anonymity/pseudonymity
  - Have we exaggerated this as a requirement?

"On the Internet, nobody knows you're a dog."

Findings and conclusions (1)
Relevant to PKI

- The use of PKI and client certificates in UK H&FE *is* feasible and scalable
  - Technically feasible
  - Usability (the supposed bottleneck)
    - Many minor problems (but no 'showstoppers')
    - Little need to fully 'educate' users
    - Once certificates installed, usability reports overwhelmingly positive
    - Usable for RAs too!
  - Scalable – need lots of RAs!

Findings and conclusions (2)
Relevant to PKI

- Crypto devices are *very* useful!
  - Usability: the 'something you have' is obvious to users
  - Scalability: can pre-load the devices (and it is secure)
  - Feasibility: too expensive at present
  - May solve the 'public computer problem'

Findings and conclusions (3)
Relevant to PKI

- Without a crypto device, you need a central backup
  - We called this the LICS
    - It was in our requirements
  - We wanted it to be very secure (even from our own sysadmin)
    - It isn't (because of the improved time-memory trade-off)
    - But it is as (or more) secure than other password based systems

Findings and conclusions (4)
Relevant to PKI

- Client digital certificates can make some common authorisation problems trivial to overcome
  - Implicit authorisation

```
SSLRequire %{SSL_CLIENT_I_DN_CN} == "GlobalSign PersonalSign
                                    Class 1 CA" \
and   %{SSL_CLIENT_S_DN_O} == "Oxford University" \
and   %{SSL_CLIENT_S_DN_OU} == "oucs"
```

- Nevertheless authorisation and authentication should otherwise be separated completely!

Findings and conclusions (5)
Relevant to PKI

- It makes better sense to store authentication digital certificates (and private keys) in the operating system, rather than in software
  - Windows may do this better

Findings and conclusions (6)
Of general relevance

- The concept of Registration Authorities in each unit is good
  - It's scalable
  - It's secure
- Sysadmins (or central registration staff) can police the RAs

Will client digital certificates ever fly?

- Depends largely on the single sign on and Shibboleth initiatives
- Client digital certificates can be used as SSO front end authentication tokens
- They can plug gaps that appear between local SSO and global Shibboleth resources

More information at

http://www.dcoce.ox.ac.uk