Digital Certificate Operation in a Complex Environment

Presentation to the IT Support Staff Conference

24 June 2004

Research Technologies Service

Information & Support Group

Digital Certificate Operation in a Complex Environment

- What a mouthful.
  [də'kʌtʃi] …bless you!
- What are 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
- What have we done so far?
- Requirements and challenges
- The architecture
- Demonstration of our certificate request/issuing system
- Appeal for help!

Staff

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

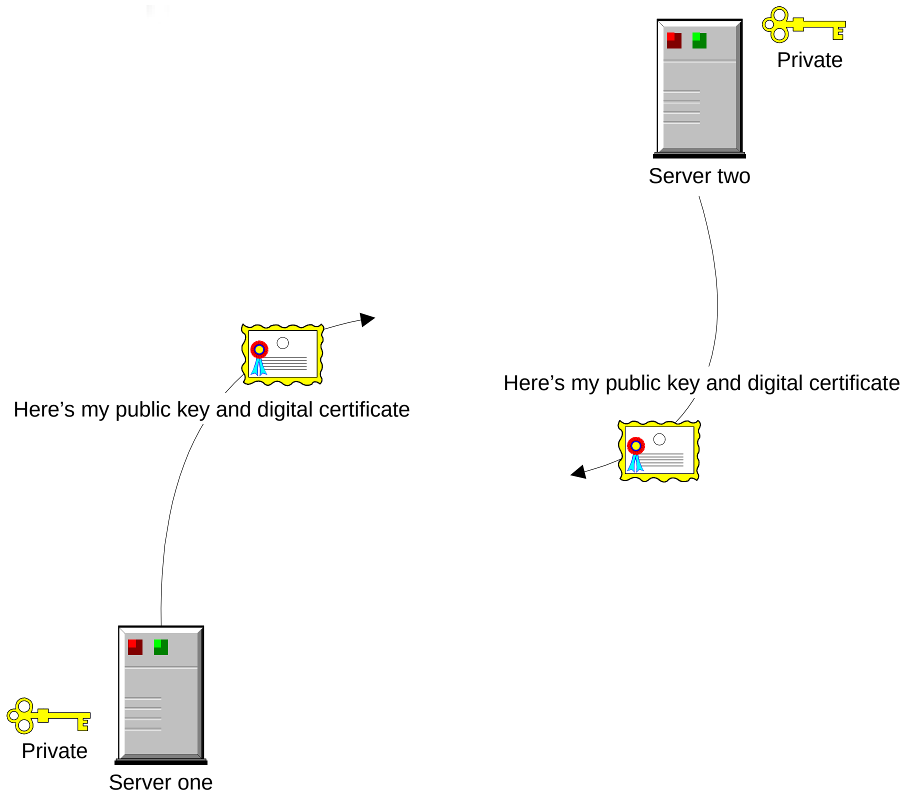
The aims (in short…)

- Use digital certificates for authentication at Oxford (and elsewhere)
  - Involves '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?

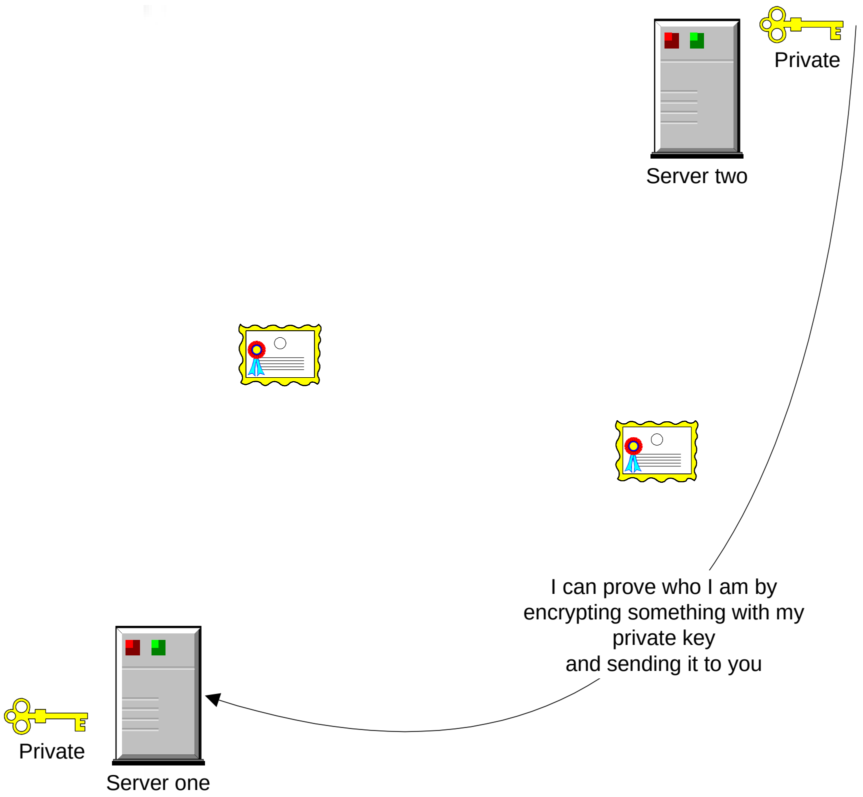
What ARE digital certificates?

- 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 certificates*)
- But *what are* they?
  - Little bits of digital information that are *signed* by a trusted authority

And how do they work?

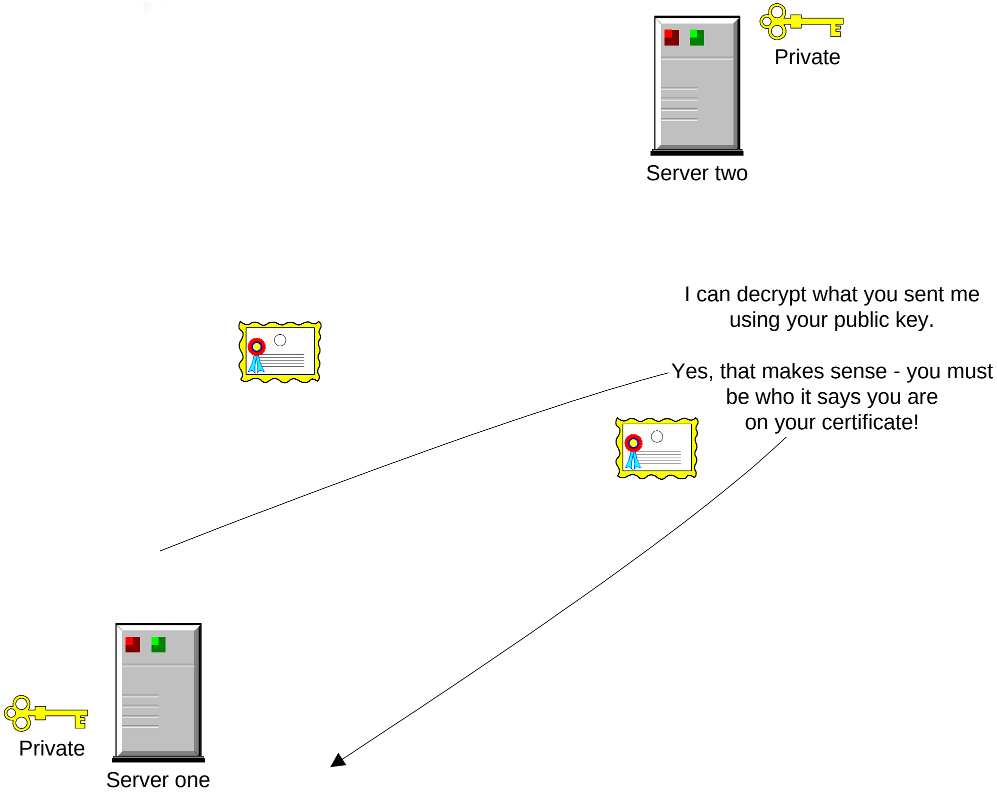

Private
Server two
Here’s my public key and digital certificate
Here’s my public key and digital certificate
Private
Server one

And how do they work?



I can prove who I am by
encrypting something with my
private key
and sending it to you

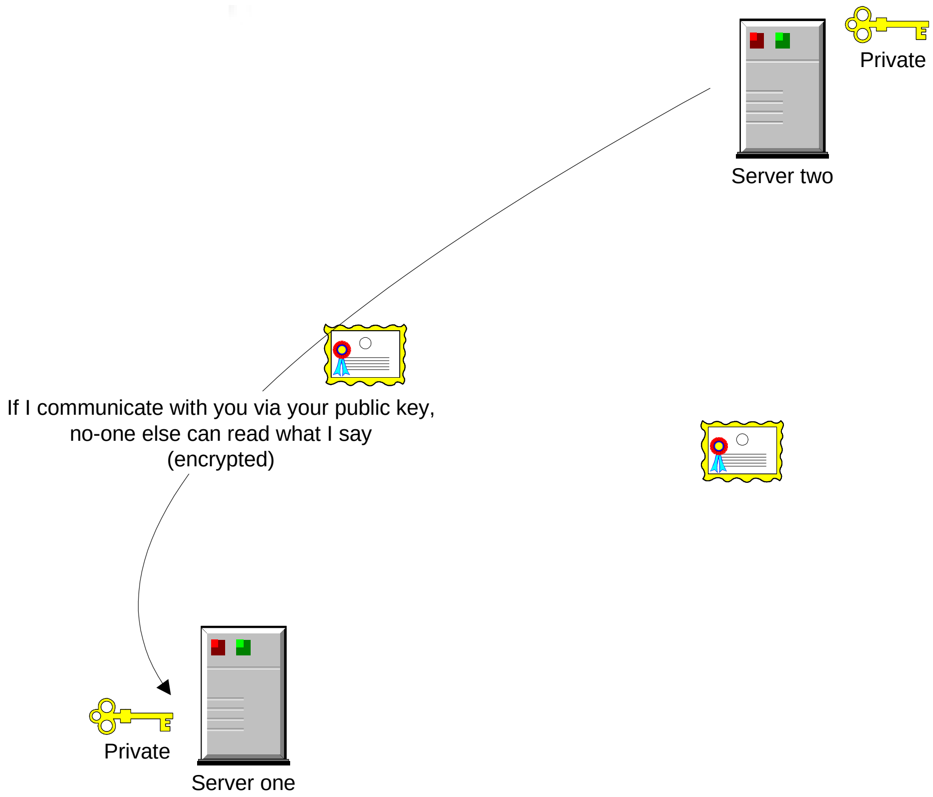
And how do they work?



I can decrypt what you sent me
using your public key.

Yes, that makes sense - you must
be who it says you are
on your certificate!

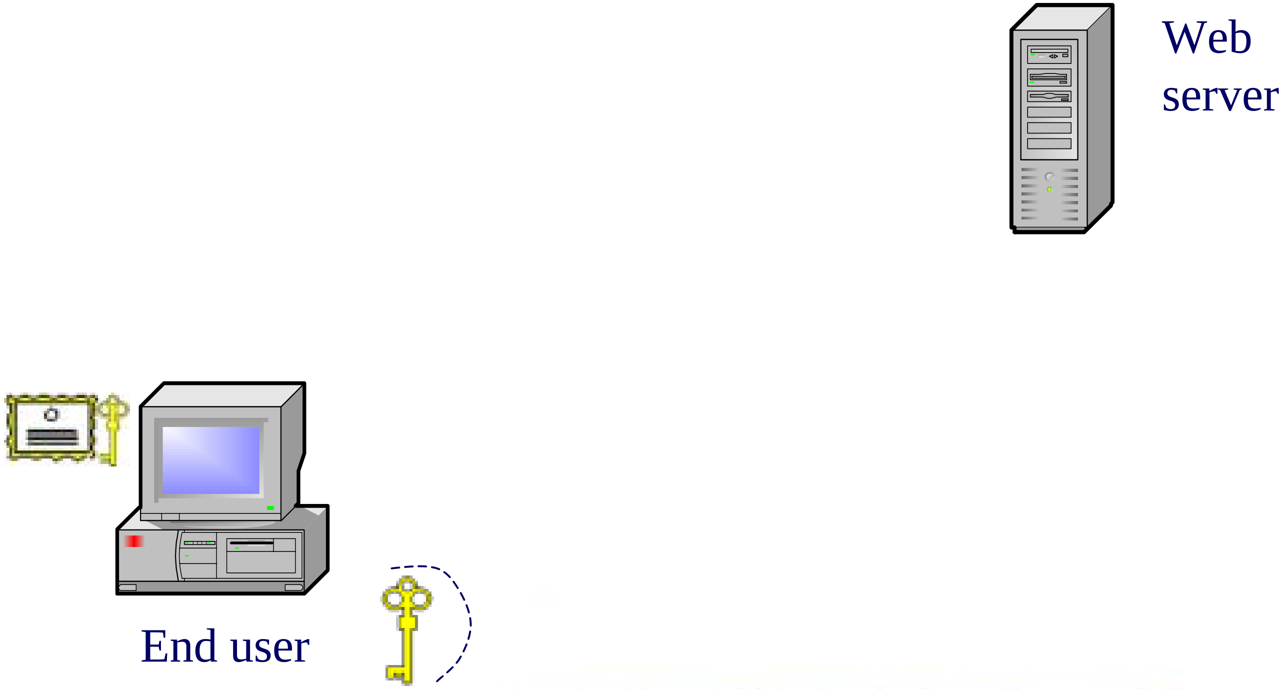
And how do they work?



If I communicate with you via your public key, no-one else can read what I say (encrypted)

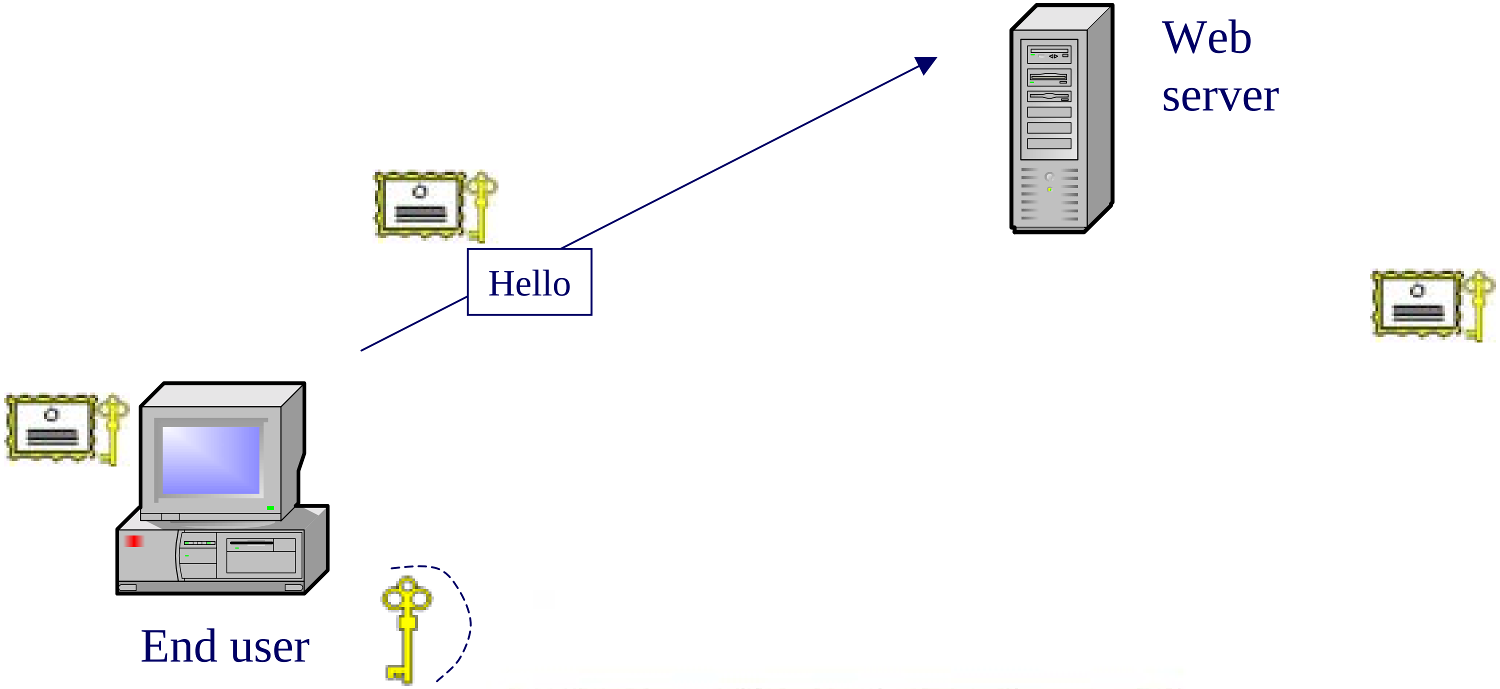
But what is DCOCE interested in?

- Authentication
- (Unfortunately, not signing or encryption)



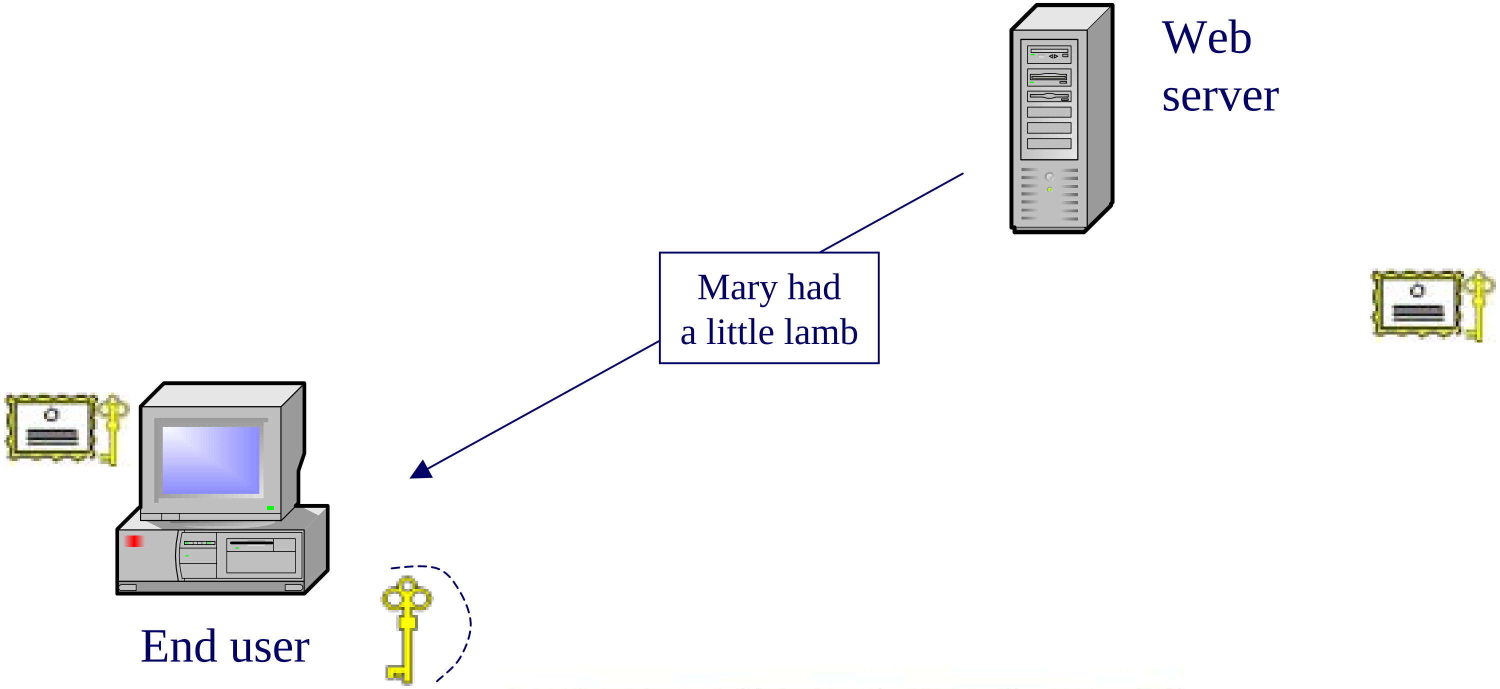
But what is DCOCE interested in?

- Authentication
- (Unfortunately, not signing or encryption)



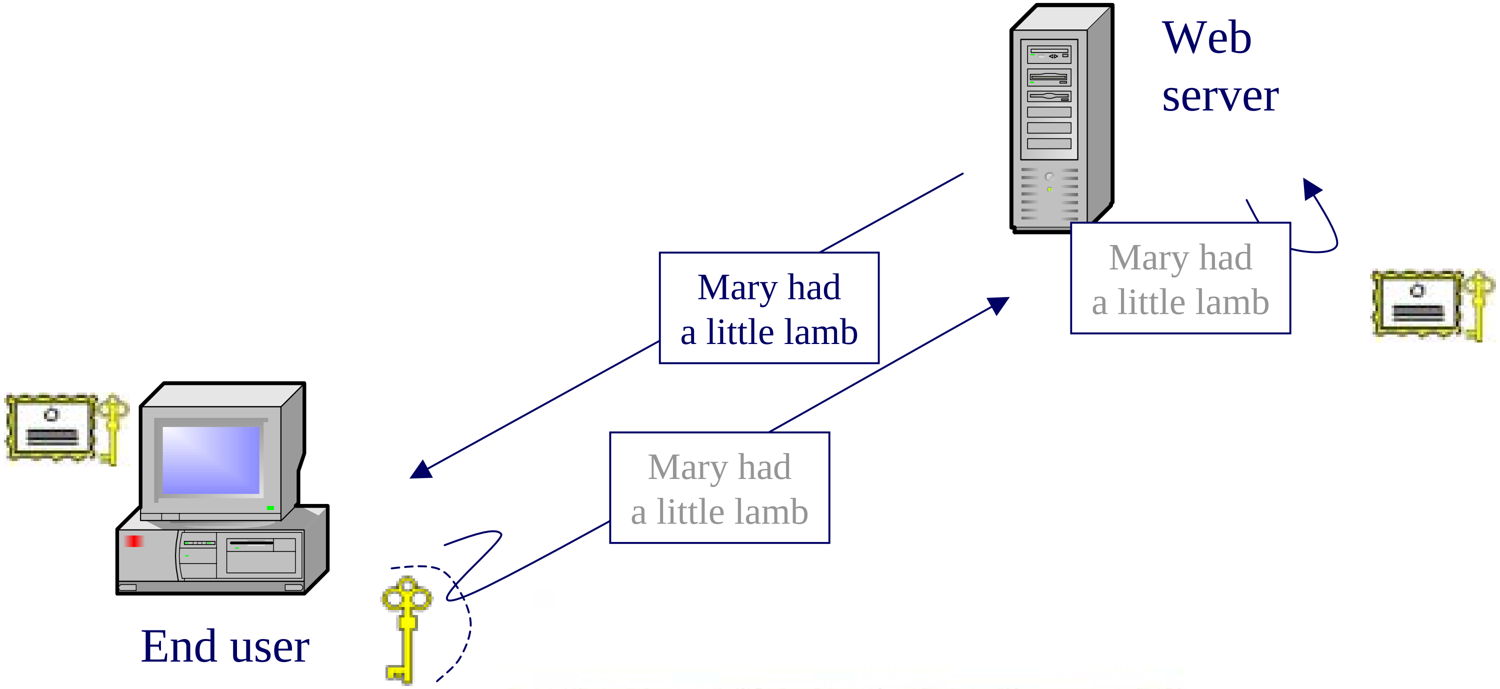
But what is DCOCE interested in?

- Authentication
- (Unfortunately, not signing or encryption)



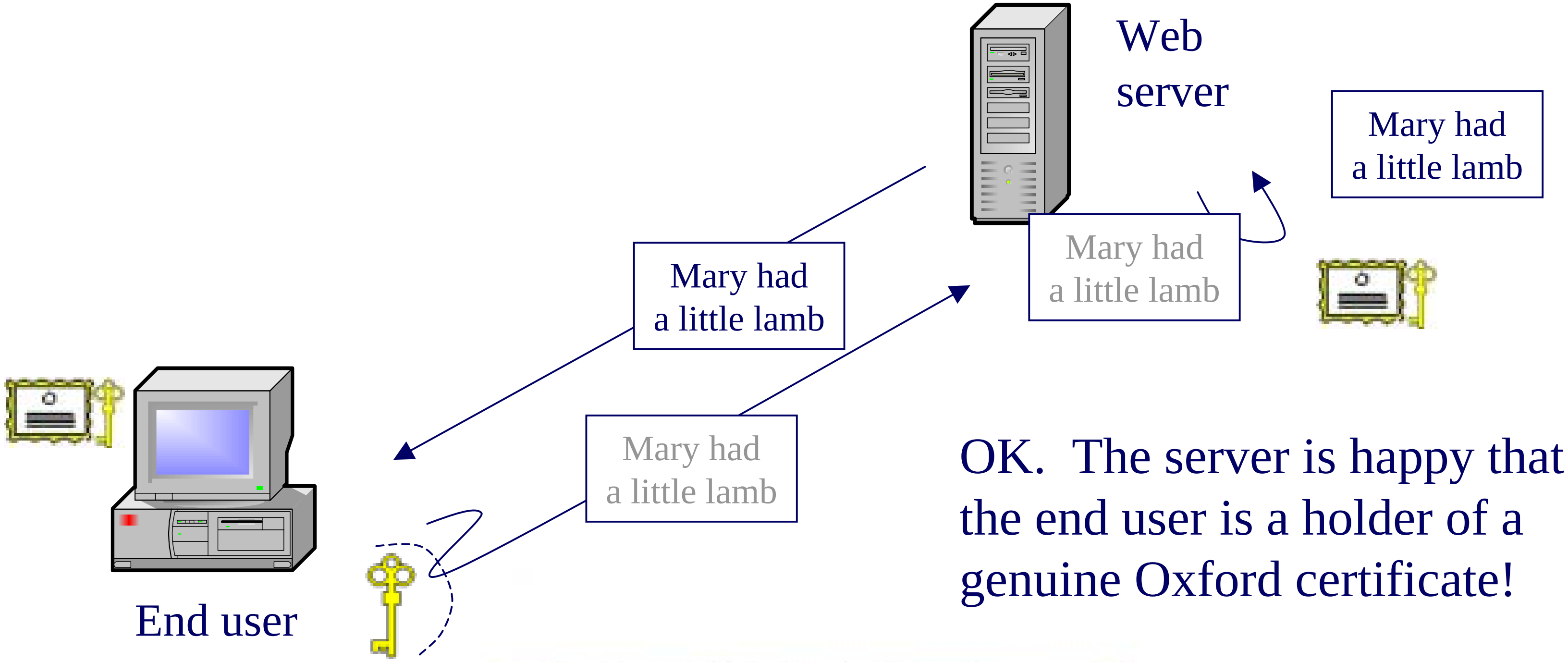
But what is DCOCE interested in?

- Authentication
- (Unfortunately, not signing or encryption)



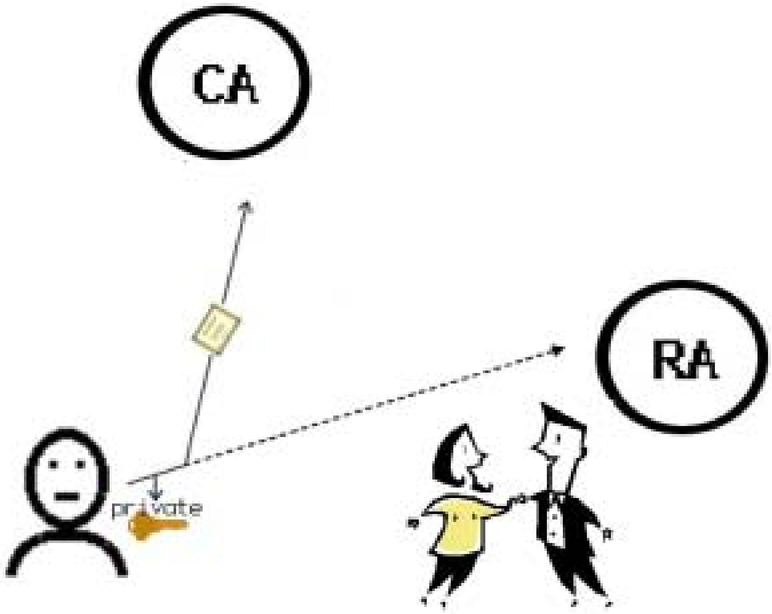
But what is DCOCE interested in?

- Authentication
- (Unfortunately, not signing or encryption)

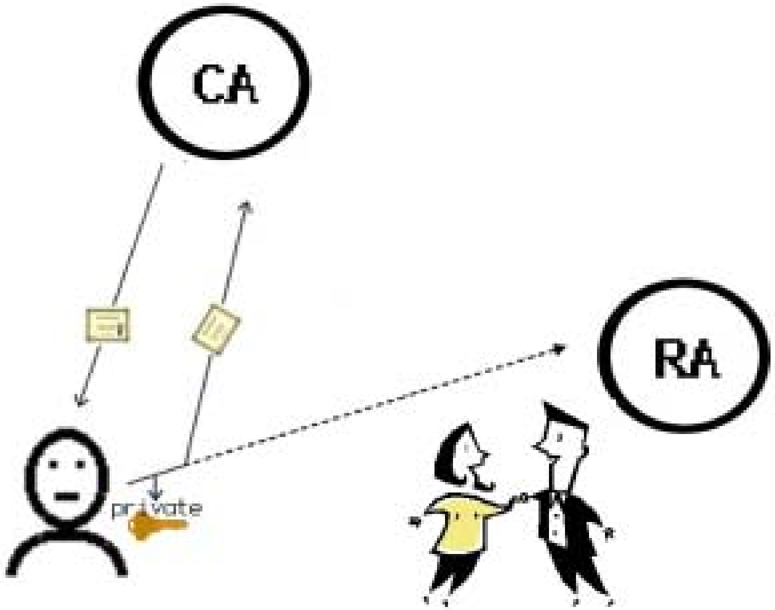


OK. The server is happy that the end user is a holder of a genuine Oxford certificate!

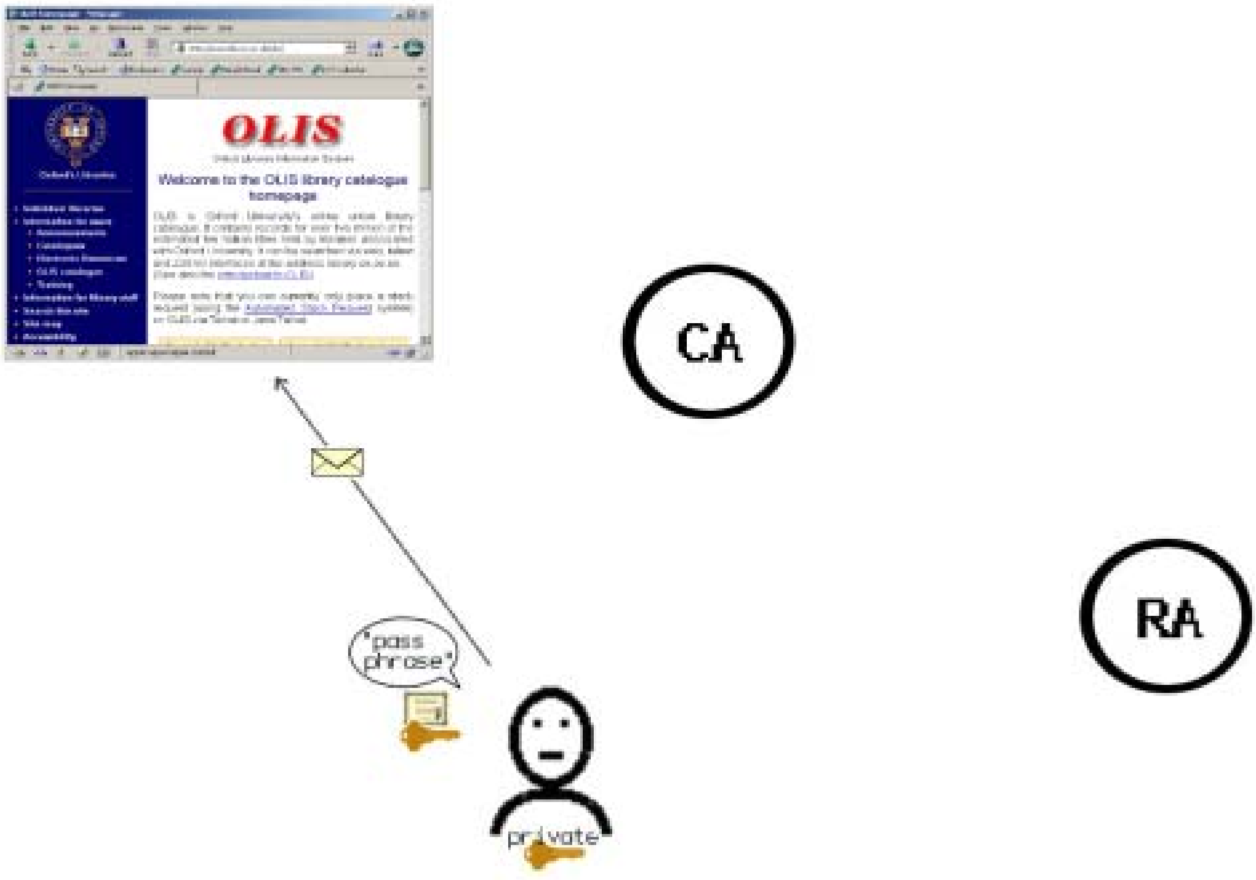
PKI – certificate issuing and use



PKI – certificate issuing and use



PKI – certificate issuing and use



OLIS

Welcome to the OLIS library catalogue homepage

PKI – certificate issuing and use

Oxford's Libraries

- Individual libraries
- Information for users
  - Announcements
  - Catalogues
  - Electronic Resources
  - OLIS catalogue
  - Training
- Information for library staff
- Search this site
- Site map
- Accessibility

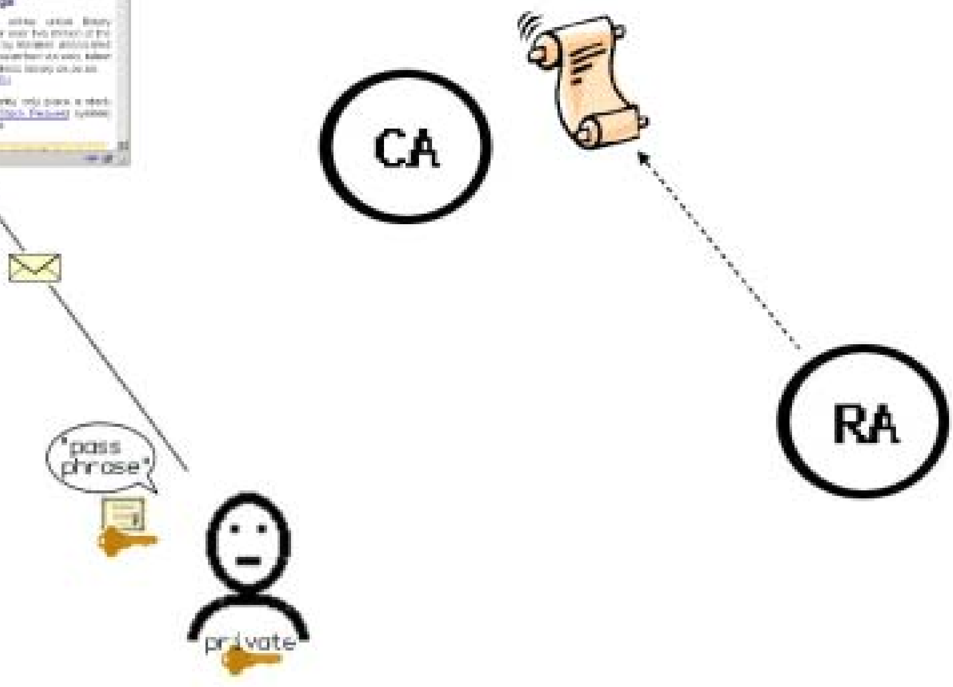
OLIS

Oxford Libraries Information System

Welcome to the OLIS library catalogue homepage

OLIS is Oxford University's online union library catalogue. It contains records for over two million of the [illegible] titles held by libraries associated with Oxford University. [illegible] and Z39.50 interfaces [illegible]

Please note that you can currently only place a stack request using the Automated Stack Request system on OLIS via Telnet / Java Telnet.



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!?!?!

What have we done?

- Consultation – to refine our requirements
- Looked at registration information flow
  - And how we expect it could work in the future
- Architecture design – as per requirements
- Very nearly finished most parts of development

What have we done *wrong*?

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

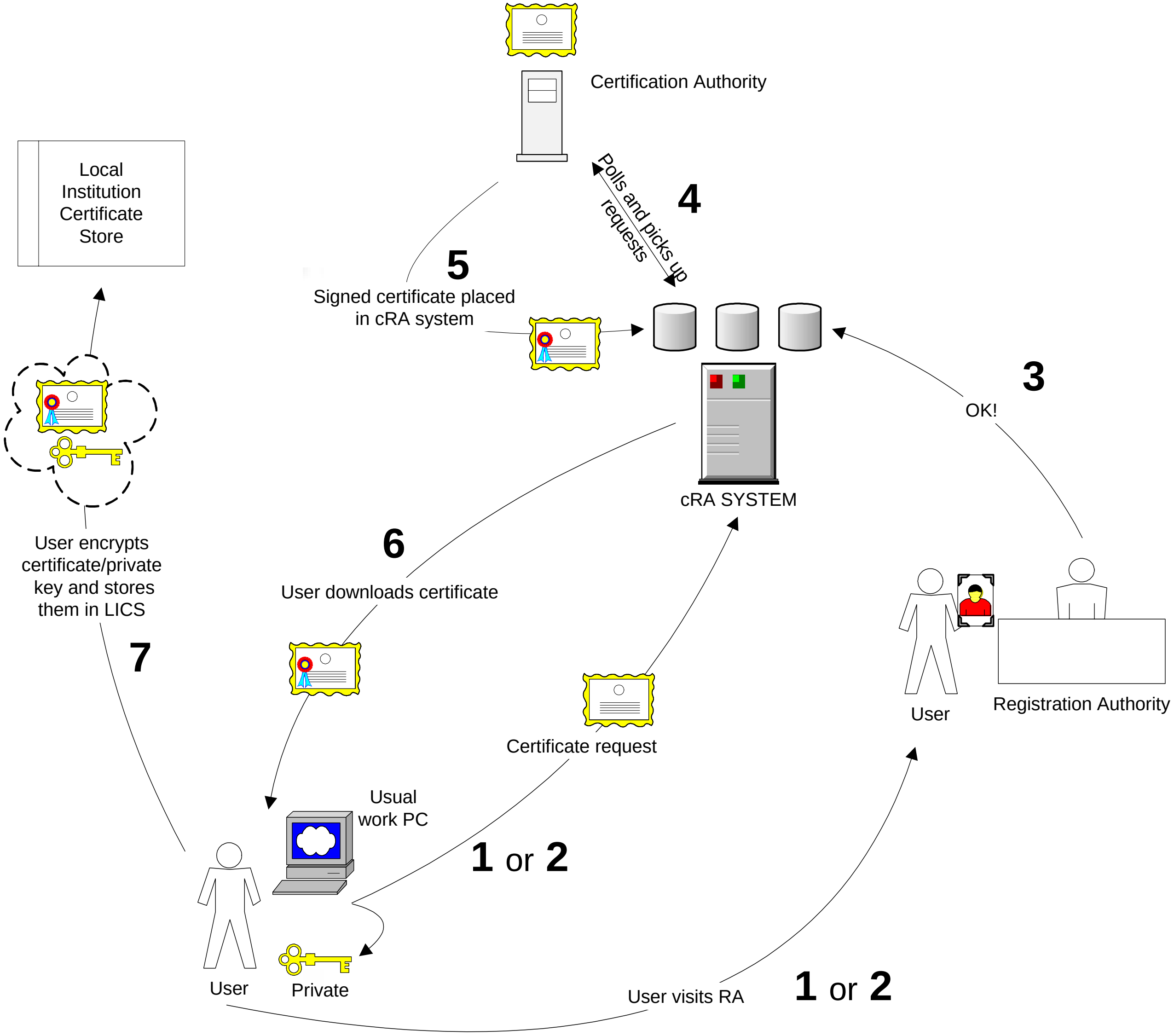
A quick indication of the ‘requirements’

- 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 certs and private keys on a central server?
  - Or use ‘devices’?

And the *real* challenges are

- Oxford pilot/feasibility vs. production (a ‘system for HE/FE generally’)
- Getting users, and giving them something to play with
  - i.e. letting them use their certificate to authenticate to something useful
- Having to ‘ignore’ signing and encryption possibilities
  - (revocation problems with these)

Architecture summary


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

A quick demonstration of our prototype

We need help!

- ITSS can really help us! We need:
  - Volunteers to be certificate users this summer*
  - Volunteers for ‘local’ RAs
  - Applications/web servers that need authentication

- * planned going live date for ITSS staff is 20th July 2004
- (we hope to involve more ‘end users’ in Sept and Oct)

More information at

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