Digital Certificate Operation in a Complex Environment

Presentation as part of the
Digital Projects in Oxford series

4 February 2004

Digital Certificate Operation in a Complex Environment

- What a mouthful.
  [dəˈkʌtʃi] …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?

- A few findings from our consultation
- Questionnaire results
- A few soft findings
- A bit of psychology
- Our challenges

- (And see our glossary)

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)

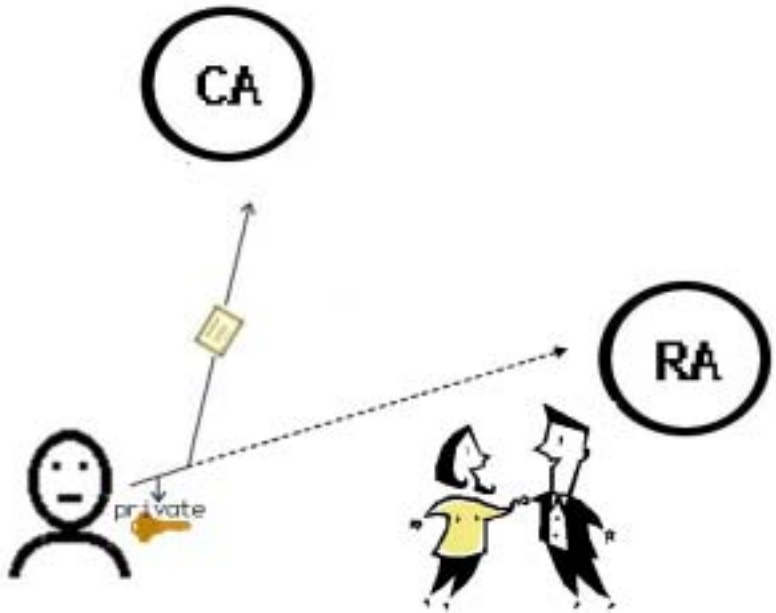
The aims (in short…)

- 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?

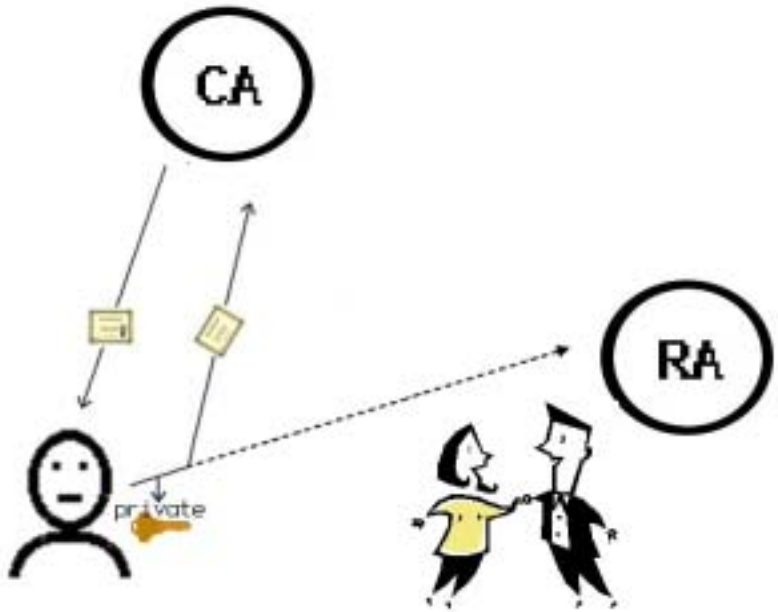
What ARE digital certificates?

- 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

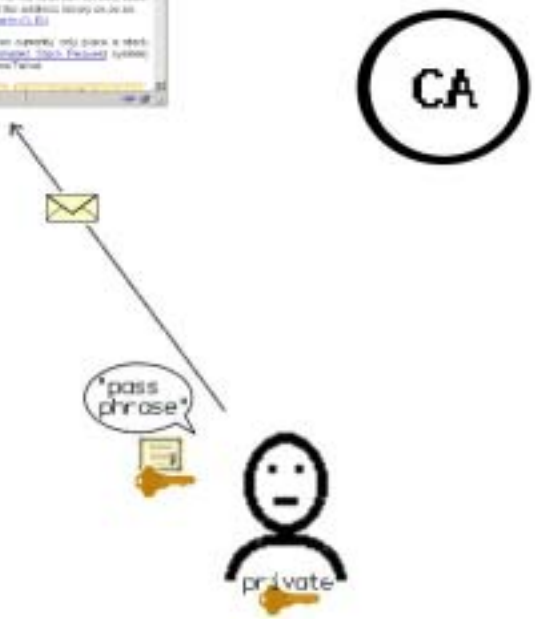
Summary of PKI



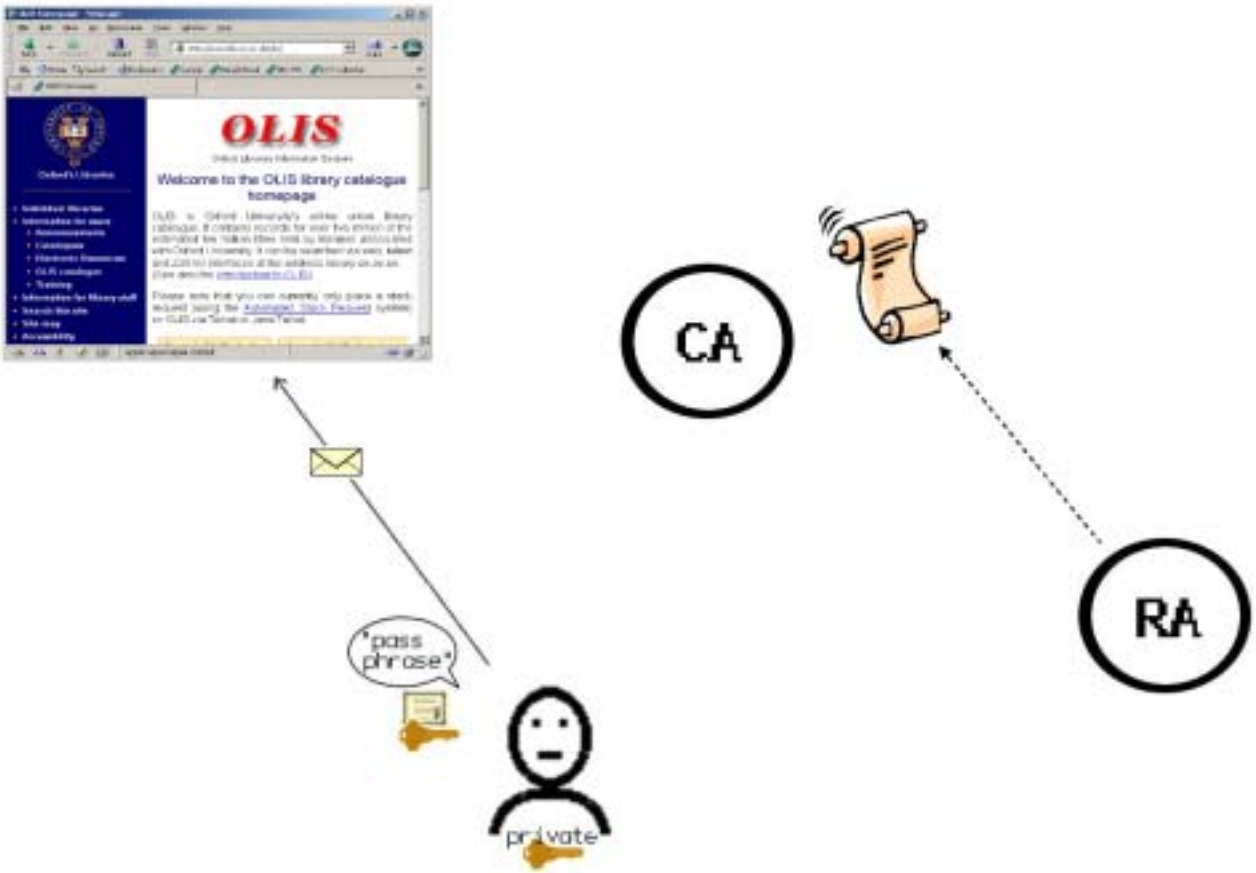
Summary of PKI



Summary of PKI



Summary of PKI



What have we done so far?

- Stakeholders and consultees
- Found out about other PKIs
- Designed a few bits of ‘architecture’ to stimulate discussion
- Held a consultation meeting
  - Where we presented those ‘bits’
  - Analysed the feedback
- Used the feedback to design the architecture
  - And begin coding

A few findings from our consultation

- What we did on the day:
  - PKI preamble (primer talk)
  - About the project
  - Talk from Athens
  - Describe our ‘ideas’
  - Discuss the ideas
  - Talk (contextualise) our questionnaires
  - Complete questionnaires
  - Further discussion

Our ideas (briefly…)

- 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’?

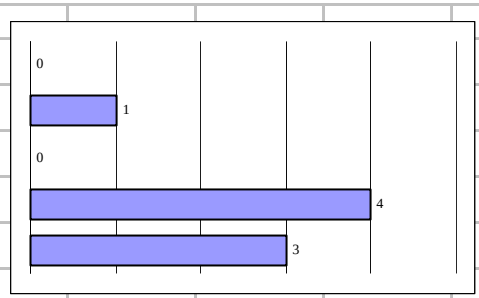
Some results from the questionnaires

- 2 questionnaires
  - Service/security people
  - Users/user reps
  - About 10 of each
- A lot of ‘noise’!

A few findings (preliminary)

- From the users/support staff

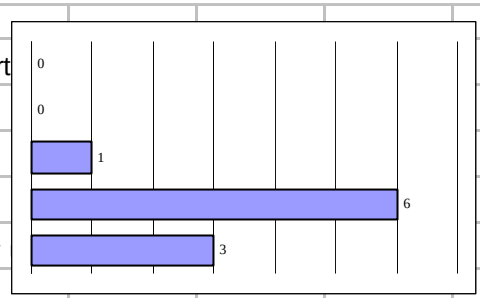
2	**Any new system of this type must not be *difficult* for users and, especially, they should not be forced to understand digital certificates and PKI.**	
	1	strongly disagree (users must fully understand PKI/certificates)
	2	disagree (users must understand a little)
	3	not sure
	4	agree (users should be minimally aware of the PKI)
	5	strongly agree (a PKI should be completely unseen by users)



A few findings (preliminary)

- From the service/security staff

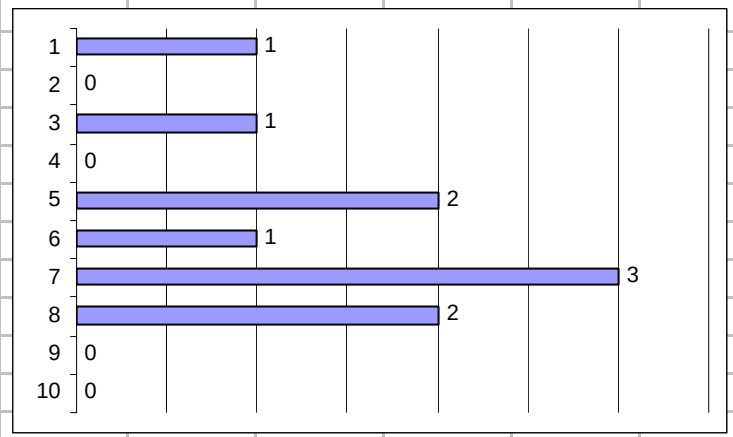
5	**Any new system of this type must not be difficult for users and, especially, they should not be forced to understand digital certificates and PKI.**	
1	strongly disagree (users must fully understand PKI/cert	0
2	disagree (users must understand a little)	0
3	not sure	1
4	agree (users should be minimally aware of the PKI)	6
5	strongly agree (a PKI should be completely unseen by	3



A few findings (preliminary)

- From the service/security staff

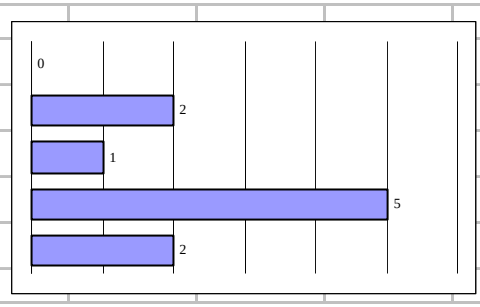
1	For an Oxford University authentication system based on digital certificates, **what strength or *level* of security** do you think it is appropriate with which **to access the *majority* of services** (services like OXLIP and the ITSS web pages, for example)?		
	Please give your answer on a scale from 1 to 10, using our 'benchmark' strengths for guidance (tick a box alongside):		
	1	Authentication via passwords sent 'in the clear'	
	2		
	3		
	4		
	5	via challenge/response methods	
	6		
	7		
	8	PKI similar to UK e-Science grid	
	9		
	10	Military strength PKI	



A few findings (preliminary)

- From the service/security staff

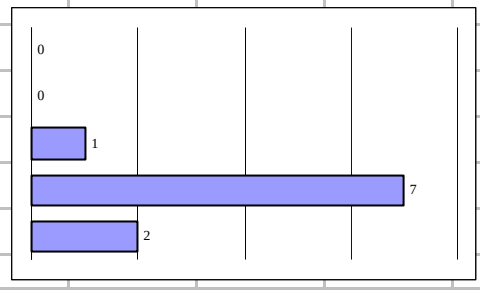
Question		
10	At Oxford University, **it would be acceptable** for a new authentication system (based on PKI) **to provide the same level of security as the current systems**. There is no pressing need to increase the level of security with respect to authentication (but PKI may be a more reliable system that can be **'tightened up' more easily in future**). Do you agree with these statements?	
	1	strongly disagree
	2	disagree
	3	not sure
	4	agree
	5	strongly agree



A few findings (preliminary)

- From the service/security staff

Question		
18	**It is possible to implement a PKI system that is very insecure** (technically or due to 'social engineering'). **This can lead to 'false trust', due to the 'good name' of PKI. This is a potential problem for some PKI rollouts.** Do you agree with this statement?	
	1	strongly disagree
	2	disagree
	3	not sure
	4	agree
	5	strongly agree



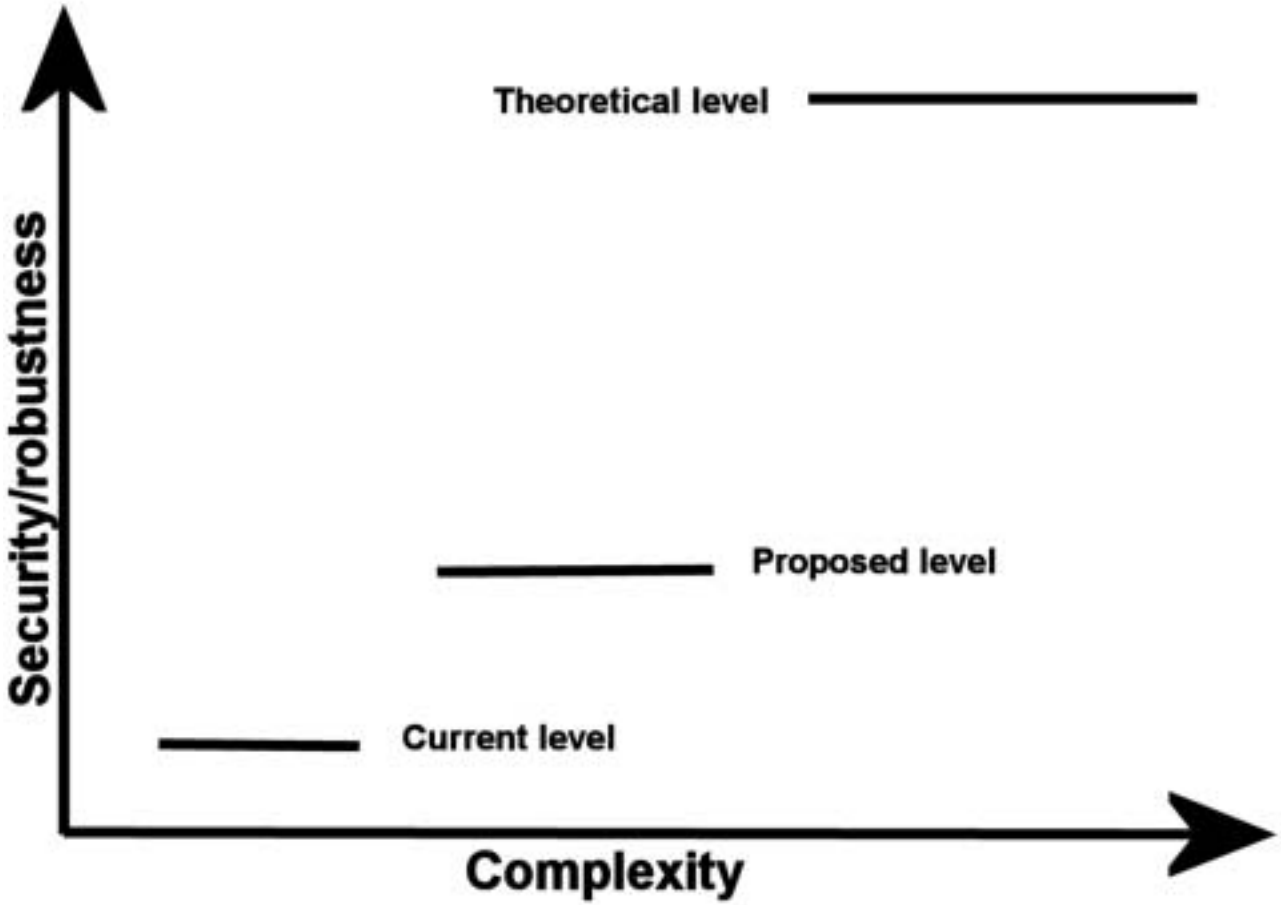
A few soft findings

- Should try to use a devolved system of RAs (i.e. Colleges)
- Security ‘experts’ sceptical of man in the middle
  - Very suspicious of the flaws in the PKI
- Although questionnaire responses said that the PKI should be transparent/unseen/easy
  - Everyone heaped extra requirements
- No relationship between the answer of level of security and their expectations of the PKI

A bit of psychology

- We don't need high *levels* of security
- However, when people hear PKI, they then want it

That psychology…



Our biggest challenge

- Persuading people that PKI is a good idea
- Why do it – people don't want extra security?
  - (But service providers need it)

Follow our progress (or otherwise) at

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