Digital Certificate Operation in a Complex Environment

Report from Consultation/Stakeholders Meeting of 3 December 2003

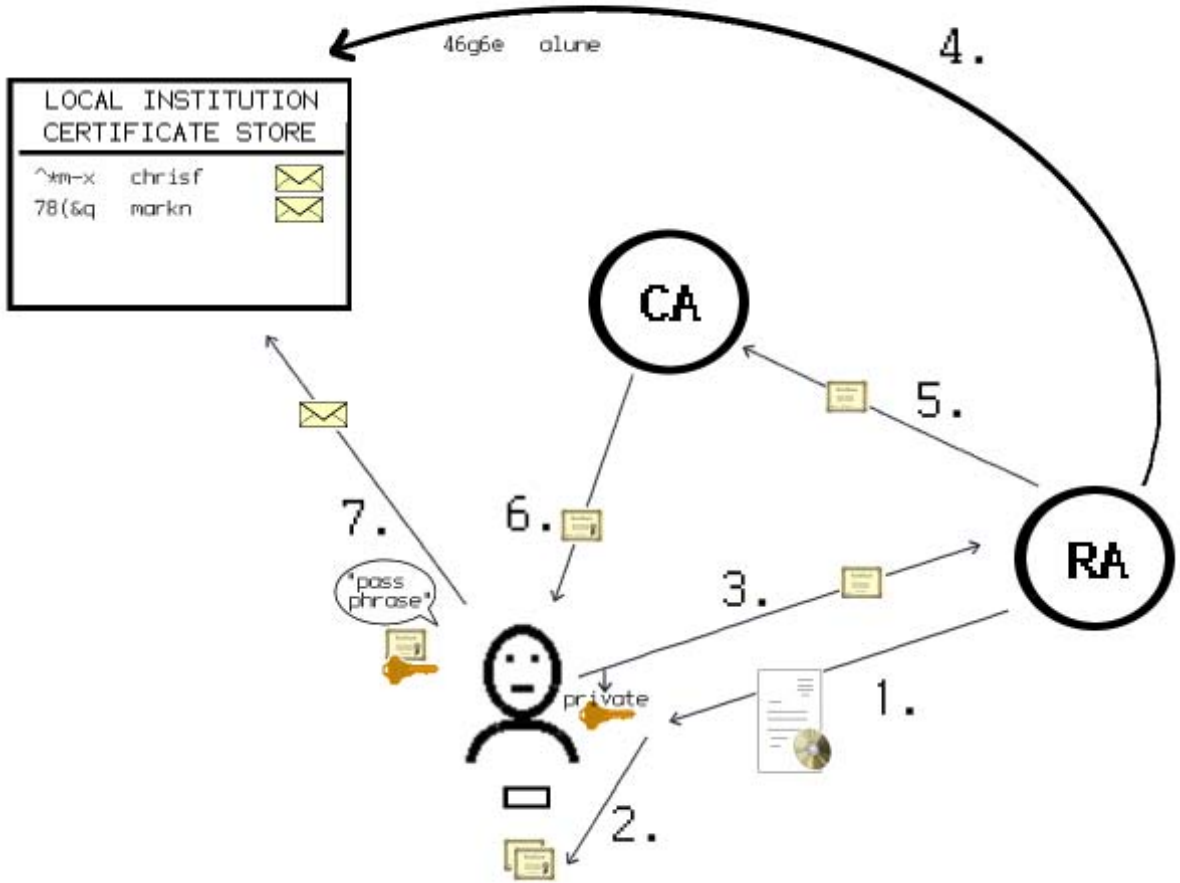
This is what we did

- 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
  - Saving certs and private keys on a central server

Summary


46g6e alune
4.
LOCAL INSTITUTION
CERTIFICATE STORE
^xm-x chrisf
78(&q markn
CA
5.
7.
6.
RA
'pass phrase'
3.
private
1.
2.

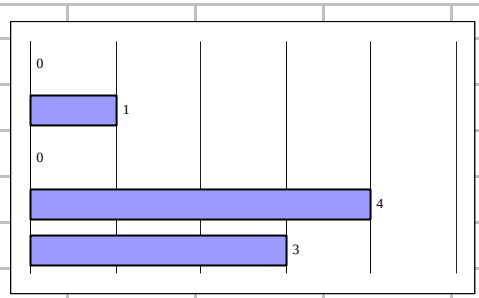
Some results from the questionnaires

- 2 questionnaires
  - Service/security people
  - Users/user reps
  - About 10 of each
- A lot of ‘noise’!
  - Some of these findings will be adjusted

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)

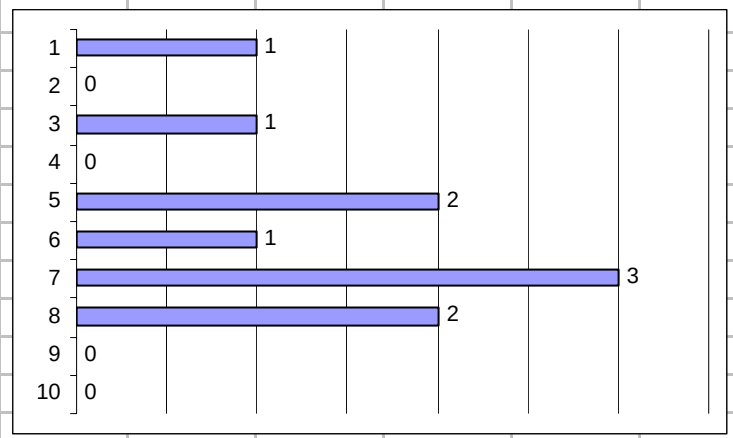
- From the service/security staff

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

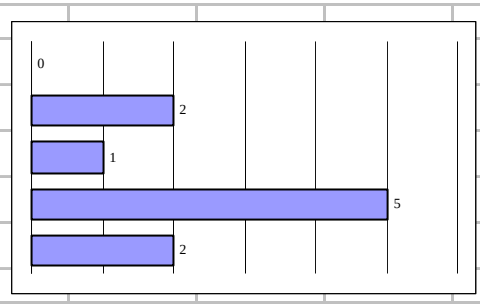
1	For an Oxford University authentication system based on digital certificates, what strength or *level* of security do you think it is appropriate with which to access the *majority* of services (services like OXLIP and the ITSS web pages, for example)?		
	Please give your answer on a scale from 1 to 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

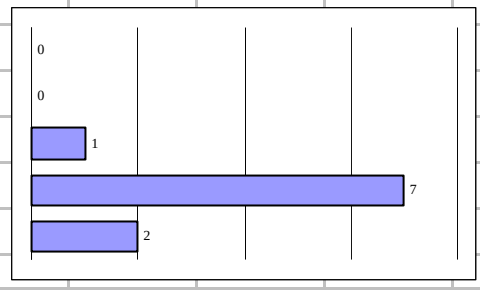
Question		
10	At Oxford University, **it would be acceptable for a new authentication system** (based on PKI) **to provide the same level of security as the current systems. There is no pressing need to increase the level of security with respect to authentication (but PKI m**	
	1	strongly disagree
	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

Our biggest challenge

- Persuading people that PKI is a good idea
- Why do it – people don't want extra security?

- Any ideas?!?