Digital Certificate Operation in a Complex Environment

A project within the Joint Information Systems Committee's Authentication, Authorisation and Accounting middleware programme

PKI ARCHITECTURE QUESTIONNAIRE (Questions only)

Project abbreviation	DCOCE
Project Title	Digital Certificate Operation in a Complex Environment
Workpackage	Workpackages 3 and 4 Modelling of administration architecture, Modelling of system architecture.
Project Manager & contact details	**Name:** Dr Mark Norman **Email:** mark.norman@oucs.ox.ac.uk **Address:** Oxford University Computing Service, University of Oxford, 13 Banbury Road, Oxford OX2 6NN **Tel:** 01865 273287 **Fax:** 01865 273275

Document History

Version	Date	Comments
0.3	29 August 2003	Final draft of questionnaire
0.2	28 August 2003	Second draft of questionnaire
0.1	21 July 2003	First draft of questionnaire

Introduction

This questionnaire is intended to serve as a framework for finding out about public key infrastructure (PKI) implementations with the objective of informing the University of Oxford's own pilot study into digital certificate utility within the complex environment that is Oxford University and beyond. The project is funded by the University and the Joint Information Systems Committee (JISC) as part of the JISC's Authentication, Authorisation and Accounting middleware programme.

Any information that you can give will be most gratefully received and, if requested, will be kept confidential. Alongside each question are boxes that can be ticked to indicate that you would not like this information to be made public. However, please feel free to inform us if you wish *all* of the contents to be kept confidential.

Even if you cannot permit any of this information to be passed to the outside world, please consider assisting with us in completing this questionnaire. We will respect your wishes and will not disclose your replies. However, your experience could benefit our project greatly.

The survey is split into four main areas:

1. General.
2. Assigning certificates and trust issues
3. Using certificates
4. Infrastructure issues

Some questions are repeated due to – for example – different hardware components being covered separately. It is unfortunate that this may cause some unnecessary repetition for you.

The questionnaire is laid out to include the question, any explanatory notes regarding the scope of the question, space for your reply and a final indicator as to whether you would wish your response to this question to be made public. The following is an example:

Question		Notes	Answer	Results not to be made public?
2.4	Do you use a separate Registration Authority (RA) or are its procedures and organisation bound up within the CA? Please describe your arrangements.	You may have a separate body (e.g. student registration) that takes on the role of RA or this may be covered by the same body that handles the CA.		☒

Anywhere that the 'not to be made public' box is checked, we will respect your wishes and not reveal this information to anyone else outside the immediate project team.

Question	Notes

1. General

Your aims

1.1.	What did you wish to achieve by establishing a PKI or digital certificate services?	What were your specific aims? Using certificates for signing or authentication or encryption etc.?

2. Assigning certificates and trust issues

Certification Authority (CA)

2.1.	How many certificates have been issued? How many are active? How many have been revoked?	Have you issued keys to a few select users, to everyone at the institution etc? What about members who never physically visit the institution? What about the general public?
2.2.	Do you run an internal CA or have you devolved this to a CA service provider?	
2.3.	Do you employ (or make use of) more than one CA?	Does your organisation use multiple root CAs or subordinate CAs etc.?

Registration Authority (RA)

2.4.	Do you use a separate Registration Authority (RA) or are its procedures and organisation bound up within the CA? Please describe your arrangements.	You may have a separate body (e.g. student registration) that takes on the role of RA or this may be covered by the same body that handles the CA.
2.5.	Do you have more than one RA? Please describe.	The procedures of using a geographically remote RA may be interesting to us.
2.6.	Please outline the RA process for identifying entities/users and the certification granting process.	Do you physically see the user? Do you use username/password, other details from a web form etc.?

Question		Notes
Main CA root certificate		
2.7.	Is this signed by an external body (Verisign, Globalsign, etc)? Can you give us an indication of the annual cost of this?	
2.8.	Can the external body (if any) revoke the certificate as part of the renewal process? (If the root certificate is not externally signed, do you have a policy of revocation time-scale?)	It can be advantageous for the server certificate to have a limited life span? Is this included in the contract with the external provider?
2.9.	What is the lifetime of your CA root certificate?	What effect does this have (especially in combination with issues involved in question 2.8)?
2.10.	Does the revocation process have a cost?	If external, is there a contractual cost? If internal, is there a human resource cost (i.e. time) of doing this?
2.11.	Are there any other issues regarding the revocation of your CA root keys/certificates?	Who has the authority to do this? How many people have this authority? How do you re-issue these certificates (in the event of a disaster situation)?
2.12.	Who generates the CA key, and what size is the key	e.g. 1024,2048,4096 bytes?
2.13.	Could you outline the process of storing your CA root *private* key(s)?	How are they stored securely and backed-up etc.? Is the backup secure/encrypted etc. – i.e. who can access the backups?
Trust issues		
The answers to some of these questions depend heavily upon whether your (internal) CA root certificate is signed by an external (trusted) certificate.		
2.14.	Regarding your *internal* services: what is the mechanism to ensure that the internal services trust your CA root certificate?	How does your internal service *X* trust your CA root certificate? Have you carried out this procedure 'by hand' for each service, or is there an automated, repeatable mechanism?

Question		Notes
2.15.	Are (were) there any issues in persuading services *external* to the institution to trust the certificate?	How does an external service *Y* trust your CA root certificate?
2.16.	By what mechanism have you persuaded browsers and other client software to trust your CA signed certificate?	Browsers etc. must trust your CA certificate and that their own certificates have been signed by a reputable authority. This is an important issue when certificates are *first distributed*.
2.17.	How/where have you published your CA public certificate/key?	
2.18.	(For any sites that use a PGP or web of trust model): how do you ensure that all users are exchanging keys in the same manner and keys are signed appropriately?	
2.19.	Please could we have a copy of your certificate policy statement?	(If you have one).
2.20.	Please could we have a copy of your certification practices statement?	(If you have one).
Delegation issues		
2.21.	Do you delegate registration and/or CA within the institution?	
2.22.	Are there any trust issues associated with this that may be significant to an external service?	How do you agree on the trust relationship? Are (or were) there any interesting issues here?
2.23.	Do you (or do you plan to) carry out any auditing procedures within the institution regarding the trust mentioned in the previous question?	
User certificate issues		
2.24.	Who generates the public/private key pairs – the user or the CA?	
2.25.	(If user). How are the certificates delivered?	Please describe the delivery mechanism? The medium, security medium, checks before delivery etc.

Question		Notes
2.26.	(If CA). Are users' private keys held centrally? Who has access to these? Who has access to backups?	
2.27.	Is there a central (public/private) key server?	Please give hardware, software and operating system details in (4) below.
2.28.	Is there a central certificate server?	Please give hardware, software and operating system details in (4) below.
2.29.	What happens when the user loses a certificate, or forgets a pass-phrase necessary for its use?	Is there a mechanism for recovery or re-issue? How is this handled administratively?
2.30.	Do you have procedures for key recovery?	Do you require key recovery and how do you do this? (e.g. you may have keys for authentication and other pairs for encryption. Do you handle these differently?)
Client storage issues		
2.31.	How do users move their private key and/or certificate from machine to machine?	How portable is this across different hardware/software platforms?
2.32.	Do you use, or have you evaluated, secure devices for transport of certificates and keys?	e.g. USB tokens, smart cards etc. Do you use these widely? Do all of the commonly used devices have crypto-chips?
Revocation		
2.33.	How does your method of revocation work?	Do you publish a revocation list? Is the list *always* checked at authentication?
2.34.	What is the mechanism if the key has been used for signing or encryption?	Are keys kept for non-repudiation and decryption purposes?

Question	Notes
2.35. Did you have to write custom routines/look-ups for your revocation mechanisms? Please give details.	
2.36. How do (would) external services know that a certificate has been revoked?	Please explain any mechanisms that are in place, planned – or any *thinking* if this has not yet been achieved.

3. Use of certificates

Possibilities for use

3.1.	Are certificates (needed or) used on public access machines?	Please interpret 'public access' as anything from a library PC to any machine that accommodates >1 user (including those machines where remote access is possible).
3.2.	What is the typical lifetime of user certificates? Is this always the same?	
3.3.	Can the user use the certificate for anything else apart from the institution's authentication?	Are the same or multiple keys/certificates used for signing, authentication and encryption? Do you allow, recommend or prevent use of the authentication key for other uses (e.g. signing or encrypting email)?

Authentication and security/encryption

In the questions that follow, please indicate where your answer refers to web-based authentication or non-web-based mechanisms.

3.4.	By which mechanism is authentication achieved? *(Web/non-web?)*	e.g.1 user presents certificate, service checks signature, service checks user. e.g.2 user *X* says "I'm *X*", service looks up certificate, service checks user. e.g.3 via short term token/certificate method

Question		Notes
3.5.	What transport security is there? *(Web/non-web?)*	e.g. HTTPS, SSL v1, SSL v3, TLS
3.6.	Do you use encryption algorithms for public/private keys other than RSA? *(Web/non-web?)*	RSA tends to be the default encryption algorithm used – do you use any others? As well as? Instead of?
3.7.	Does the service check the timestamps and certificate validity correctly? (If yes, did you write this software/process yourself?) *(Web/non-web?)*	This has been an issue with some PKIs. Please give some details here.
3.8.	Is the digital certificate authentication mechanism a completely new process or did it integrate with your existing authentication mechanism? *(Web/non-web?)*	
3.9.	Are there separate authentication mechanisms for access via VPN (or other remote access routes)? *(Web/non-web?)*	Please also consider all mechanisms where remote users connect 'in' to a machine and are authenticated later for access to further services.
3.10.	Did you have to over-ride IP-mediated authentication, or did you just add to this? *(Web/non-web?)*	
3.11.	In which language(s) is/are these processes written? *(Web/non-web?)*	

Question	Notes
3.12. Were you able to use open-source software, and to what extent? Please indicate any licensing issues and other related issues in this area. *(Web/non-web?)*	
3.13. What do the service(s) need to see in the certificates to work correctly? *(Web/non-web?)*	Does each service work in the same way for this? Please indicate differences.
3.14. How does a (each) service check the CA signature on the certificate? *(Web/non-web?)*	

4. Infrastructure

General

4.1. Have you carried out any auditing of the security of the system (formal or informal)? Were any weaknesses identified? What were these and how were they resolved?	
4.2. Have you any estimations of the following costs (time/money/people) to: a) issue a certificate b) reissue an expired certificate c) reissue a revoked certificate (and is this passed on to the user?)	e.g. where the user was at fault for losing the certificate.

Question		Notes
Server hardware/components		
For any servers (e.g. key server, certificate server, attribute server), please assist us with the following questions (and indicate which hardware/component/server is being described):		
4.3.	How secure is the location of this particular piece of hardware?	Please indicate where the component or server is on the same machine etc.
4.4.	Can you give an indication of the 'up front' and ongoing costs?	
4.5.	Please give some details of the hardware you use (CPU, memory and disks)	Are you using software or hardware raid?
4.6.	Is there redundant hardware on site?	
4.7.	How quickly can you (do you) replace failed hardware?	
4.8.	What protocols are you using for key services relating to the PKI?	
4.9.	Which other services are run on the same server/machines as the components of the PKI?	i.e. does a machine just contain servers/services that are part of the PKI or do other servers/services co-exist on the same machine?
4.10.	How secure are the servers?	Please give indications of access controls, firewalls or packet filters etc.
4.11.	Are there any scalability issues with respect to hardware?	e.g. will the hardware need to be upgraded (more powerful) or will more nodes solve any scalability problems?
Server-side software		
4.12.	Did you use open source software for any components (and if so, which)? What is the user community like? Can you buy support/customisations?	

Question	Notes
4.13. Can you give an indication of the 'up front' costs for proprietary software? On-going costs? Have you bought customisations from a vendor and were you happy?	
4.14. Are there any scalability issues relating to the above software?	How are you planning to overcome these?
4.15. On which operating systems are the services/components run?	
4.16. On which operating system *can* the services/components run? Are there any issues (now or in the future) relating to this?	
Client hardware/components/platforms For any servers (e.g. key server, certificate server, attribute server), please assist us with the following questions (and indicate which hardware/component/server is being described):	
4.17. What is your range of operating systems that work (usefully) with the PKI?	What operating systems *can* the PKI components run on? Are there any issues (now or in the future) relating to this?
4.18. For web services, which browsers can be used to access the certificate-mediated services?	Are there any plans or obstacles in expanding this list? Is it the policy to not expand (or even to contract) this list?
Client software	
4.19. Did you use open source software for any components (and if so, which)? What is the user community like? Can you buy support/customisations?	

Question	Notes
4.20. Can you give an indication of the 'up front' costs for proprietary software? On-going costs? Have you bought customisations from a vendor and were you happy?	