Digital Certificate Operation in a Complex Environment

Final implementation and evaluation report

Project abbreviation	DCOCE
Project Title	Digital Certificate Operation in a Complex Environment
Start Date	1 January 2003
End Date	31 December 2004
Report to	Joint Information Systems Committee (JISC), UK.

Contents

1. Executive and extended summaries 5
1.1. Executive summary 7
1.2. How to use this document 8
1.3. Extended summary 10
1.4. Acknowledgements 22
2. Framework for design 25
2.1. Introduction 27
2.2. Issues for consideration 27
2.3. Report of requirements gathering meeting 31
2.4. Requirements obtained 36
2.5. Notes from other PKI implementations 37
3. Overview of technical architecture 41
3.1. Introduction 43
3.2. Requirements and constraints 44
3.3. Architecture and components 47
3.4. Architecture and procedures 48
3.5. Technical description of components 66
3.6. Weaknesses and gaps 78
4. Evaluation conclusions 81
4.1. Introduction 83
4.2. Suitability of client digital certificates 83
4.3. Usability of client digital certificates 84
4.4. Scalability of client digital certificates 85
4.5. Security considerations 85
4.6. Cultural considerations of the “complex environment” 86
4.7. Design variations 86
5. Evaluation of user feedback 89
5.1. Introduction 91
5.2. Evaluation of the questionnaires returned by test users 96
5.3. Feedback about understandability 97
5.4. Feedback about learnability 102
5.5. Feedback about operability 105
5.6. Feedback about attractiveness 114
6. User and technical evaluation (details) 119
6.1. Introduction 123
6.2. The components 123
6.3. Evaluation categories 124
6.4. Requirements recap 127
6.5. User pre-request out of band and human interaction 128
6.6. RA/user human interaction (request first procedure) 132
6.7. User request on-line interface 135
6.8. User request technical interface (and transport to server(s)) 139
6.9. Java applet based interface 142
6.10. Request database and central RA system 147
6.11. RA interface 150
6.12. Appointment and authorisation of RAs 152
6.13. Server interaction with CA 154
6.14. Structure of certificate and fields in certificate (request) 158
6.15. Notification of users of certificate readiness 161
6.16. User download of certificate 164

6.17. Use of certificates 167
6.18. Authorisation mechanisms (technical) 173
6.19. Authorisation mechanisms (human) - how the RAs authorise people 176
6.20. Revocation of certificates 179
6.21. Expiry and Renewal 181
6.22. Special section: use of cryptographic hardware devices 183
7. User scenarios and requirements review 189
7.1. Introduction 191
7.2. Test scenarios 191
7.3. Requirements review 198
APPENDICES 201
1. Appendix one: Example certificate 203
2. Appendix two: Browser and operating system support 205
2.1. Browser support 205
2.2. Operating system support 206
2.3. Notes 206
3. Appendix three: DCOCE Instructions for Registration Authorities (RAs) 208
4. Appendix four: Further reading 211
4.1. PKI and other implementations 211
4.2. Authentication and authorisation 212
4.3. Cryptography 212
4.4. Other access management 212
4.5. Privacy 212
4.6. JISC middleware programmes and projects 212
4.7. Miscellaneous 213
4.8. Evaluation and surveys 213

7. User scenarios and requirements review

Contents

7.1. Introduction 191
7.2. Test scenarios 191
7.2.1. Definitions 191
7.2.2. Basic scenarios: University users 192
7.2.3. Basic scenarios: non-University users 193
7.2.4. Sounds like real-world scenarios 196
7.3. Requirements review 198

7.1. Introduction

As outlined in the *Framework for design* chapter, during the requirements gathering phase, we built up a set of user scenarios and a list of requirements for the PKI. In the sections that follow, these scenarios are explored to check that they are successfully covered by the architecture and procedures that the project attained. This chapter should also illustrate the challenges that face each type of user and highlight some of the improvements that would be needed.

In the sections that follow, there are four basic scenarios each for University and non-University users, followed by five *Sounds like real-world* scenarios (see page 196) that should make far more entertaining reading. These are considered in turn. For the sake of argument, it is assumed that certificate-based client authentication has been adopted on a large scale. This is due to the inherent difficulties that would ensue, should only a small or sub-group of users be issued with certificates. In that case, certificate-based authentication and IP range authentication would be working side by side and this would make our analysis difficult.

Section 7.3 (see page 198) reviews the original requirements and briefly evaluates of how each was met.

7.2. Test scenarios

7.2.1. Definitions

7.2.1.1. Basic Oxford University electronic services

"Basic Oxford University electronic services" can be taken to mean on-line resources (that are currently protected by IP restrictions), such as some staff pages in departments, or resources that use very basic authentication, such as OXAM (Oxford Examination Papers Online) or the IT-support staff (ITSS) pages.

7.2.1.2. The University IP range

"The University IP range" implies University, Colleges and Departments etc. The main point being that it is within a network managed by University, College or University-related research or educational organisations. Furthermore, the user is *likely* to have access to technical support and may have a managed desktop.

7.2.2. Basic scenarios: University users

7.2.2.1. University user - one computer in one place - accessing basic Oxford University electronic services

An Oxford University user employing one computer in one place to access basic Oxford University electronic services from:

- an office in the University IP range;
- home (i.e. on a - non-University - public network);
- an office at another institution.

Were digital certificates to be fully implemented throughout the university, such a user would be able to access all resources to which they have been granted rights, provided that they have downloaded their certificate to their computers, both in their office and at home. Were they to visit another institution and to have a computer with their own log-in account, they should have the same experience from that place as well. Therefore, this scenario is met entirely by our PKI recommendations.

7.2.2.2. University user - one mobile computer - accessing basic Oxford University electronic services

An Oxford University user employing one computer (most likely a laptop or a mobile device) in different places to access basic Oxford University electronic services. These places will be multiple, but will include:

- personal computer on a (non-University) public network;
- personal computer on the University network.

The certificate stored on their computer will function the same regardless of whether the user is within the University network or outside of it. Therefore, this scenario is met entirely by our PKI recommendations.

7.2.2.3. University user - many computers, many places - accessing basic Oxford University electronic services

An Oxford University user employing several computers in different places to access basic Oxford University electronic services. These places will be multiple, but will include the places listed under 7.2.2.1 above as well as a public machine in the Oxford IP range (e.g. in a library). In summary, computers at:

- an office in the University IP range;
- another office in the University IP range;
- home (i.e. on a - non-University - public network);
- an office at another institution;
- a public machine in the Oxford IP range.

So long as the user has stored their certificate in the LICS, and downloaded it to each computer they wish to use it from, they should be able to access all resources they are entitled to. Therefore, this scenario poses no problems to our PKI recommendations until you reach the requirement regarding a public machine.

At present, users should not install their long-term (yearly) certificates to a public machine unless they have a separate account on that machine. It may be possible to access certificate-

restricted resources from public machines by issuing short-term certificates, or by storing certificates on a portable cryptographic hardware device (although it is unlikely that all computers will be able to read from such a device). For further information, see section 1.3.6.3 (page 16 of the *Executive and extended summaries* chapter) for a short summary of the problem, and section 3.4.4 (page 61 of the *Overview of technical architecture* chapter) for a detailed analysis and our proposed solution.

7.2.2.4. University user - no primary computer – access from many places (internal and external) to basic Oxford University electronic services

An Oxford University user that does not have a 'primary' computer (i.e. regular point from where most work is done), but accesses basic Oxford University electronic services from:

- any office machine in the University IP range, presumably shared with several other users;
- any 'public' machine in the University IP range, presumably shared with several other users (e.g. in a library, department or college etc.);
- any public machine outside the University IP range (e.g. Internet café machine).

The use of digital certificates from computers shared between a limited number of users would be permitted within the DCOCE guidelines, provided that each user has a unique personal log-in (account) at that computer. Therefore, most shared office computers could be used to access resources, so long as the user has stored his certificate key in the LICS, and downloaded his certificate to each computer he wishes to use it from. Users must not download their (annual) certificates to machines shared with others without separate log-ins, as this compromises security. Most library machines, and all Internet Café machines, would therefore be prohibited. Section 7.2.2.3 above details the problem and gives references to other paragraphs regarding our thinking on these matters.

In this scenario, the user would probably be able to use his long-term certificate from the office machine (assuming he has his own account on that computer). However, our PKI as developed in the project, would not support him in the other two situations, unless he were to use a cryptographic hardware device. Our recommendations regarding public computers may meet these requirements (see section 3.4.4 on page 61 of the *Overview of technical architecture* chapter).

Note that users with cryptographic hardware devices (such as iKeys) may use their certificates securely from shared public computers, provided the appropriate drivers are installed to recognise such hardware devices.

7.2.3. Basic scenarios: non-University users

The following scenarios concern non-University users (people who are not issued with University cards). Examples of situations include:

- a visiting academic;
- someone on a short course (not long enough to be issued with a University card);
- someone on a correspondence course (not - or rarely - visiting the University);
- a collaborator on a research project;
- temporary staff.

In the sections below, it should be noted that there is a general problem with non-University users having walk-in and unlicensed access to on-line resources (see the note on page 61 of the *Overview of technical architecture* chapter). It should be noted that, our scenarios are concerned with 'basic Oxford University electronic services'. These services would be covered; it is the licensed services supplied by third parties that could be problematic due to contractual reasons.

Further, it should be noted that, whilst at Oxford, non-University members could visit the RA of the OU where they are working. This is described in section 3.4.5.2 on page 63 of the *Overview of technical architecture* chapter. However, see the following section (3.4.5.3) within that chapter regarding the problem for remote users, and the concept of trusting RAs in other institutions.

7.2.3.1. Non-University user - one computer in one place - accessing basic Oxford University electronic services

A non-(Oxford) University user employing one computer in one place to access basic Oxford University electronic services from:

- an office in the University IP range;
- home (i.e. on a - non-University - public network);
- an office at another institution;

Non-University users at Oxford could be issued with certificates allowing specific rights for a certain fixed period of time. Such certificates would function in the same manner as standard certificates issued to University members, and should therefore allow access to resources from the above locations. Therefore, this scenario would be covered by the DCOCE solution.

It is impossible, however, to ignore the use of the digital certificates to access remote services. As noted on page 61 of the *Overview of technical architecture* chapter, and above, this could be problematic due to licences. A possible solution could be to have all non-University users belonging to a special organisational unit (OU). This is not a perfect solution, as service providers would probably wish to interpret the holding of a valid Oxford University digital certificate as denoting full membership of the University (see section 3.4.5.4 on page 64 of the *Overview of technical architecture* chapter for further details).

This grey area is symbolic of that which already exists regarding users at Oxford holding library cards (Bodleian reader cards). Most University members hold a University Card, which is also a Bodleian reader card. The cards are used to access library services, but it occasionally becomes problematic when the library card is being used to access electronic services that are licensed to University members only. It is this situation that is being transposed into the world of digital certificates.

7.2.3.2. Non-University user - one mobile computer - accessing basic Oxford University electronic services

A non-(Oxford) University user employing one computer (most likely a laptop or a mobile device) in different places to access basic Oxford University electronic services. These places will be multiple, but will include:

- personal computer on a (non-University) public network;
- personal computer on the University network.

Non-University users at Oxford could be issued with certificates allowing specific rights for a certain fixed period of time. Such certificates would function in the same manner as standard

certificates issued to University members, and should therefore allow access to resources from the above locations. Therefore, this scenario would be covered by the DCOCE solution.

The text regarding licensing issues above is also applicable here.

7.2.3.3. Non-University user - many computers, many places - accessing basic Oxford University electronic services

A non-(Oxford) University user employing several computers in different places to access basic Oxford University electronic services. These places will be multiple, but will include the places listed under 7.2.3.1 above as well as a public machine in the Oxford IP range (e.g. in a library). In summary, computers at:

- an office in the University IP range;
- another office in the University IP range;
- home (i.e. on a - non-University - public network);
- an office at another institution;
- a public machine in the Oxford IP range.

Note: Some situations that meet the above scenario sound contradictory or paradoxical. However, there must be exceptions that will fit with this, scenario, e.g. researcher in a 'virtual organisation'.

Non-University users at Oxford could be issued with certificates allowing specific rights for a certain fixed period of time. Such certificates would function in the same manner as standard certificates issued to University members. The same restrictions would apply regarding public machines, as given in 7.2.2.3 above.

Therefore, notwithstanding the licence-related issues addressed above (section 7.2.3.1) this scenario is met by our design with the possible exception of the public machine, for which we have already stated that we have design recommendations (see section 7.2.2.3 above).

7.2.3.4. Non-University user - no primary computer – access from many places (internal and external) to basic Oxford University electronic services

A non-(Oxford) University user that does not have a 'primary' computer (i.e. regular point from where most work is done), but accesses basic Oxford University electronic services from:

- any office machine in the University IP range, presumably shared with several other users;
- any 'public' machine in the University IP range, presumably shared with several other users (e.g. in a library, department or college etc.);
- any public machine outside the University IP range (e.g. Internet café machine).

Non-University users can be issued with certificates allowing specific rights for a certain fixed period of time. The use of digital certificates from computers shared between a limited number of users would be permitted within the DCOCE guidelines, provided that each user has a unique personal log-in (account) at that computer. Therefore, most shared office computers could be used to access resources, so long as users have stored their certificates and private keys in the LICS, and downloaded their certificates to each computer from which they wish to use them. Users must not download their certificates to machines shared by

many users that do not have separate log-ins, as this compromises security. Most library machines, and all Internet café machines, would therefore be prohibited. Section 7.2.2.3 above details this issue and gives references to other paragraphs regarding our thinking on these matters.

In this scenario, the user would probably be able to use her short-term certificate from the office machine (assuming she has her own account on that computer). However, our PKI as developed in the project, would not support her in the other two situations, unless she were to use a cryptographic hardware device. Our recommendations regarding public computers may meet these requirements (see section 3.4.4 on page 61 of the *Overview of technical architecture* chapter).

As mentioned in section 7.2.2.4, users with cryptographic hardware devices (such as iKeys) may use their certificates securely from shared public computers, provided the appropriate drivers are installed to recognise such hardware devices.

7.2.4. Sounds like real-world scenarios

7.2.4.1. Test scenario one

> *Joan Black is a part-time IT support officer for St Bland's College and, in her spare time, is pursuing the Department of Continuing Education's online Diploma in Computing. Her manager delegates to her the monthly checking of the latest Oxford University Computing Services (OUCS) username and routing deletions. Because she works only part-time and because OUCS are not always consistent in when the monthly deletions are announced, she occasionally undertakes this task from home. As part of her course, she would also like to access the full text of specific electronic journals from home. Currently she uses VPN to do this but this slows down her elderly family PC and she would prefer a more direct form of access.*[1]

Joan would require two separate digital certificates, one from her college (that has certain IT support authorisation attributes associated with it), the other from the Department of Continuing Education for accessing resources relating to the diploma (such as the electronic journals). Provided that she stores her certificates and private keys in the LICS, both certificates could be downloaded to her home computer and used from there. The digital certificates should provide simplified access to the on-line resources and the VPN client should not be needed.

7.2.4.2. Test scenario two

> *Dr Henry Brown is a researcher at the University of Hudson's Bay, Canada. His colleagues at Oxford University have managed to obtain a grant from the United Nations Global Collaborations Programme and have formed a virtual organisation that includes Dr Brown. Dr Brown must be able to access resources protected by Oxford University access management systems and world-wide resources to which his team (using money emanating from Oxford) have subscribed.*

Dr Brown would presumably have to receive his digital certificate without visiting Oxford. In the solution developed by the DCOCE project, there is no provision for this scenario. However, we make some suggestions regarding using remote RAs to physically authenticate remote users (see section 3.4.5.3 on page 63 of the *Overview of technical architecture*

[1] VPN stands for 'Virtual Private Network' and is used to 'tunnel' through a network (or the Internet) and makes the remote user appear that she is actually attached to the organisation's local area network (i.e. she will apparently have an IP address which belongs to the organisation, rather than to her internet service provider).

chapter). If this were possible, Dr Brown could be issued with a digital certificate with an organisational unit of "alien" (or similar, as outlined in section 3.4.5.4 that follows the above reference).

7.2.4.3. Test scenario three

> *Miss Pearl White is a part-time researcher in genetics at Old College as well as a data clerk with the University Chest/finance division. She has a permanent computer in both offices (college and University) and likes to travel with her laptop computer. Ideally, she would like similar access to systems via all three computers (but it is possible that she may not be allowed access to certain financial systems whilst off site, in any case).*

Pearl would require two certificates, one from her college granting permission to access academic resources, another from the University administration permitting access to the financial databases. By storing the certificates and private keys in the LICS, both certificates could be downloaded to each of the three computers, enabling Pearl to access either set of resources from any of her computers. As discussed in the *Extended summary* (section 1.3.6.2, page 14), it may be prohibited for her to put the certificate that allows her access to the University Chest in the LICS. Nevertheless, it would be possible to put this certificate and private key onto all of her three computers, but she may require some IT support to be able to do this. Access to sensitive financial information, however, might be restricted to users from within the University IP range, so as to provide an additional level of security, in which case Pearl would not be able to access this information on her laptop unless it was plugged in to a University Ethernet socket.

7.2.4.4. Test scenario four

> *Mr Dai Green occasionally works for Oxford University Computing Services (OUCS) as a consultant for short periods of time. He also frequently avails himself of short courses and correspondence courses run by the Department of Continuing Education. Although he is on short-term contracts and short periods of study, he needs access to the appropriate resources from his office at OUCS and from his home PC during these times (when he has a contractual relationship with the University).*

Mr Green's contractual access requirements should be met by issueing him with short-term (i.e. for the duration of his contracts) certificates from the RA at OUCS (as in scenarios 7.2.3.1 and 7.2.3.2). For his short courses at the Department of Continuing Education, he will need another short-term certificate covering the periods of study (also covered by scenarios 7.2.3.1 and 7.2.3.2). Both of these (sets of) certificates can be stored in the LICS and so, as long as he does not work from a public computer and restricts himself to his own office computer, home computer and possibly laptop, the DCOCE solution will meet his requirements. The licensing issues, as outlined in the cited sections would apply to him, however.

7.2.4.5. Test scenario five

> *Miss Scarlett is an undergraduate student at Brassknocker College. She lives at the college. As she does not own a computer of her own, she uses the college computer facilities, when they are available. If there is no college computer available, she goes to the nearby Internet café to check her e-mail and to undertake brief, focused searches of online resources provided by the university. She doesn't surf on the internet from the internet café as that might become expensive for her. She leaves internet surfing until she is in the library, where she can access on-line library resources and the internet for free.*

Miss Scarlett should obtain a digital certificate from her College and store it in the LICS. Assuming that she has her own log-in account on the shared college computers, she will be able to download her certificate to the college computers and use it to access online resources. She would not be permitted to download her certificate to a publicly available machine in an Internet café. Possible ways to overcome her Internet café problem include the use of portable cryptographic hardware devices, or very short-term certificates. For more information, see the solutions discussed in section 1.3.6.3 (page 16 of the *Extended summary*) and section 3.4.4 (page 61 of the *Overview of technical architecture* chapter).

7.3. Requirements review

The requirements were introduced on page 46 and are considered in turn here.

7.3.1. *The perceived level of security should be as good as that required/used by the majority of current University administered services that use authentication, but better than the system of passwords "used in the clear".*

This requirement was met. The least secure part of the design is the LICS (introduced because of the usability requirements) and this is easily as secure as most current authentication procedures in the University. For the most part, the perceived level of security with the DCOCE PKI is far higher than anything in place currently, and the actual level of security is also a good deal higher.

7.3.2. *It should be possible to devolve registration to departments and colleges.*

This requirement was met by the DCOCE design. This requirement was highlighted as a major bottleneck for scalability and therefore took a very high priority in the development efforts.

7.3.3. *The PKI needs to be easily integrated with existing staff and student University registration procedures.*

This requirement was met in that the same individuals can easily perform their registration duties as well as act as a RA for the DCOCE PKI. However, we were only able to recommend the close integration of the certificate issuing database with the institutions central directory service (LDAP). This could not be carried out during a pilot project.

7.3.4. *Where possible, the best current technology and standards should be used for good interoperability.*

We believe that our design meets this requirement. All components are open source and standards have been followed, where they exist.

7.3.5. *Everything must be easy to use for the non-technical user.*

On the whole this requirement was met. Some improvements are clearly possible, especially with respect to accessibility criteria and the Java applets.

7.3.6. *The number of times a pass phrase must be entered by the user should be minimised.*

This requirement was met successfully. Even though the pass phrase was actually 'needed' several times, the Java applets kept this in memory so that the user only needed to supply a pass phrase once.

7.3.7. *The authentication mechanism and the certificate format must allow for integration with authorisation protocols.*

It is questionable as to whether this requirement was met fully. Certainly, the use of the certificates allowed for authorisation procedures to be adopted and there is nothing to impede the integration with authorisation protocols in the certificate format. However, little work was carried out in integrating with other authorisation protocols.

7.3.8. *The DCOCE PKI should support authentication using HTTP based and non-HTTP based protocols.*

This part of the DCOCE project was not completed. However, there is nothing in the certificate formats that preclude authentication via non-HTTP based protocols.

7.3.9. *The DCOCE PKI should provide the user with a secure mechanism to move his private key between different machines.*

This requirement was fulfilled with the development of the Local Institution Certificate Store (LICS).

7.3.10. *No private or sensitive information should be stored on the certificates.*

This requirement was met, via a compromise in that the organisational unit *was* to be included (see requirement 7.3.12, below). The latter requirement meant that the certificates did include this information, which could be conceived as being private. However, no other private or sensitive information appeared on the DCOCE client digital certificates.

7.3.11. *The user's name or personal details should not be discernable by a body outside of Oxford University. This is a common requirement for information environments and was adopted for the project in order that it meet the requirements of a wide variety of institutions.*

This requirement was met via the use of pseudonyms within the Common Name in the certificates.

7.3.12. *The organisational unit must be included on the certificate because colleges and departments may be registered for separate services.*
(This requirement gives rise to a difficulty where individuals belong to several departments or colleges and blurs the boundary between authentication and authorisation).

This requirement was met, although see the reference in paragraph 7.3.10, above.

7.3.13. *The mechanisms employed by the DCOCE PKI should not preclude or mandate the use of cryptographic hardware tokens.*

This requirement was met. Cryptographic hardware tokens may be used with the DCOCE PKI, and the developers would wish to encourage this. However, there is no mandate to use such devices.

7.3.14. *The DCOCE* PKI *should provide a mechanism to allow the registration of users who cannot physically visit the University.*

The project did not develop any functionality to meet this requirement. However, recommendations were made that policies could be established whereby trustworthy individuals in other institutions could be called upon. Nevertheless, the problem remains as to how to physically authenticate the remote RAs.

7.3.15. *The DCOCE* PKI *should provide a mechanism to reduce the risk of leaving long-lived certificates (or the* private keys *for these long lived certificates) on public machines.*

The did not develop any functionality to meet this requirement. However, recommendations were made regarding the use of short-term certificates for use in such situations (see section 1.3.6.3 on page 16 of the *Extended summary* and section 3.4.4 on page 61 of the *Overview of technical architecture* chapter).

APPENDICES

1. Appendix one: Example certificate 203
2. Appendix two: Browser and operating system support 205
3. Appendix three: DCOCE Instructions for Registration Authorities (RAs) 208
4. Appendix four: Further reading 211

1. Appendix one: Example certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
# always version 3, by globalsign
        Serial Number:
            01:00:00:00:00:00:fe:6c:72:a5:c5
#determined by globalsign
        Signature Algorithm: sha1WithRSAEncryption
#determined by globalsign
        Issuer: C=BE, O=GlobalSign nv-sa, OU=PersonalSign Class 1 CA,
        CN=GlobalSign PersonalSign Class 1 CA
#determined by globalsign
        Validity
            Not Before: Aug 17 11:12:25 2004 GMT
            Not After : Sep 17 11:12:25 2004 GMT
#can be 1 month or 1 year
        Subject: CN=magdalen-6304cf1f, O=Oxford University,
            OU=magdalen
#fields CN, OU, email, C, ST can be chosen by us (or left blank)
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:e9:9c:cb:7d:a9:64:b9:41:3e:c0:7b:e7:69:c2:
                    f7:ca:93:b1:aa:eb:de:2f:b8:0b:86:25:0d:dc:e2:
                    35:dd:e7:44:7c:cc:8c:48:77:a7:cc:1e:b5:94:dd:
                    2e:53:a0:fb:cf:ed:2d:8b:4a:48:49:18:10:37:aa:
                    50:9d:67:2a:2a:27:01:9b:35:ea:80:14:78:94:a8:
                    65:5e:15:8c:e3:c0:e1:c1:bb:1e:db:63:f5:ed:8e:
                    9f:70:da:f5:54:c8:8d:57:98:bd:0f:e8:10:94:f7:
                    67:06:2a:07:85:7d:e4:c5:03:81:b6:75:76:e2:1c:
                    05:72:72:4d:72:d1:83:b3:2b:4b:99:4c:9c:b0:c6:
                    0f:43:5b:6a:07:b7:21:2b:65:70:b3:e7:53:37:8e:
                    f5:2b:c9:0e:7d:75:81:b9:5f:64:06:e3:f8:fc:15:
                    59:9b:55:e0:a8:fd:aa:77:1f:c7:d8:d7:26:2c:75:
                    19:69:30:25:2b:48:0a:15:37:04:c4:33:70:3e:72:
                    a4:4e:b0:50:30:02:03:42:67:39:63:96:8a:db:2a:
                    7e:98:17:05:27:54:63:1f:63:1f:dc:94:79:d1:b3:
                    85:2a:53:fe:ed:d7:82:37:b8:2b:b0:30:c0:74:6f:
                    08:e7:3b:3f:8e:4e:a1:1b:cb:df:1c:81:3d:b5:f8:
                    e6:07
                Exponent: 65537 (0x10001)
#Subject public key info is chosen by us. We have only tested
        <=2048bit RSA
#everything below is purely GlobalSign
        X509v3 extensions:
            Netscape Cert Type:
                SSL Client, S/MIME
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key
                Encipherment, Data
Encipherment
            X509v3 Authority Key Identifier:
```

```
keyid:0F:75:EE:F1:23:BD:75:42:EA:B7:89:40:46:BD:92:D2:72:EB:C5:E8

            X509v3 CRL Distribution Points:
                URI:http://crl.globalsign.net/PersonalSignClass1.crl

    Signature Algorithm: sha1WithRSAEncryption
        77:6d:9c:e6:27:4a:f2:c3:4d:84:43:1d:20:ee:f7:83:b1:de:
        e7:36:db:f2:80:f6:41:96:c0:12:84:d1:a7:ae:66:d0:e8:86:
        fb:93:07:c5:12:53:22:3d:53:59:9d:09:d7:5d:ce:7e:d9:b5:
        69:3c:f8:e3:eb:f1:fe:ba:50:ba:83:bf:f0:63:66:d0:9c:42:
        17:93:29:07:46:45:8d:12:f6:88:dd:93:02:e9:ab:24:67:b7:
        92:52:b2:b7:61:ea:54:5a:bb:c2:e5:7a:ee:77:7c:79:c4:b9:
        b7:75:3a:b8:5c:ed:c6:1a:0f:a8:be:a1:dc:a8:53:09:2a:4c:
        b9:15:33:cd:82:61:9f:54:32:1b:16:c4:64:a8:8d:2c:f4:b5:
        cb:8a:c4:12:62:e0:4d:f0:50:ad:38:b8:30:43:e6:8e:fc:3c:
        fe:b8:56:19:f3:e5:c8:a5:92:04:ab:1c:81:8a:bb:50:af:3a:
        73:44:ad:3b:ad:ad:93:21:2c:7c:c8:aa:9e:0d:40:75:0e:51:
        25:f8:00:b1:1c:32:ce:91:99:c0:04:aa:2c:e9:b2:0c:ac:02:
        4b:63:68:44:8e:c7:6b:dd:05:4b:b3:8a:c7:3a:eb:69:ed:2c:
        7b:f7:ce:76:3f:46:6d:d5:02:19:6b:5c:d7:7f:cf:b2:2e:fc:
        2b:c2:54:af
```

2. Appendix two: Browser and operating system support

2.1. Browser support

The following table shows the browsers that were tested with the DCOCE certificate issuing system. The 'Percent' column shows the popularity of the browser according to logs analysed by the VisitorVille.com company over the summer of 2004 (just prior to our evaluation phase).[1] Note that by the end of the DCOCE pilot study, the popularity of the Firefox browser had grown considerably within our users. However, we were (erroneously) discouraging its use during our trial due to perceived problems with certificate handling in the browser software. The entry in the 'Browser-request' column indicates whether browser based (i.e. non-Java-mediated requests) were used or tested successfully. Similarly, the 'Java-request' column indicates whether users of those browsers were able to make a request and download the keys and certificates using the Java applet.

Browser	Percent	Browser-request	Java-request
IE 6.0	75.12%	yes	yes
Unknown	4.19%	n/a	n/a
Mozilla 1.7	3.95%	yes	yes
IE 5.0	3.72%	yes	yes
IE 5.5	2.56%	yes	yes
Safari	2.56%	untested	yes (1)
Netscape 7.0	2.33%	yes	yes
Mozilla 1.0	1.40%	yes	yes
Firefox 0.9	1.40%	yes	yes
Mozilla 1.6	0.93%	yes	yes
Firefox 0.8	0.70%	yes	yes
IE 5.01	0.47%	yes	yes
Mozilla 1.4	0.47%	yes	yes
Netscape 7.1	0.23%	yes	yes
Firebird 0.6	unknown	no	no
Opera	unknown	yes	yes (1)

[1] See http://intelligence.visitorville.com/. These data were publicly available on the web. However, it is possible that VisitorVille.com is now charging a fee for access to current data.

2.2. Operating system support

The following table shows the browsers that were tested with the DCOCE certificate issuing system. The 'Percent' column shows the popularity of the operating system according to data published by the VisitorVille.com company over the summer of 2004 (just prior to our evaluation phase). The entry in the 'Browser-request' column indicates whether browser based (i.e. non-Java-mediated requests) were used successfully from those operating systems. Similarly, the 'Java-request' column indicates whether users of those operating systems were able to make a request and download the keys and certificates using the Java applet.

Operating system	Percent	Browser-request	Java-request
WinXP	57.91%	yes	yes
Win2000	14.65%	yes	yes
Win98	6.05%	yes	yes
Unknown	4.19%	n/a	n/a
WinNT	3.95%	yes	yes
MacOSX	3.49%	yes	yes (1)
MacPPC	3.26%	untested	yes (1)
WinME	2.33%	yes	yes
Linux	1.86%	yes	yes
Win95	1.40%	untested	untested
SunOS	0.93%	untested	untested

2.3. Notes

1) A Java-request can be made, but automatic installation into the key store is not supported. The user has to use the browser's PKCS#12 import functions to install the certificate.

2.3.1. Minimum requirements to be able to request and install a certificate

Technically, certificate requests can be made from every web browser that supports at least one of the following request methods. The browser must:

- understand Netscape's proprietary <keygen> tag or
- support a Java plug-in (>= 1.4.0) or
- support Microsoft's xenroll ActiveX component.

2.3.2. Additional requirements when using Java-based request:

For creating certificates requests and installing certificates, Sun's Java plug-in version 1.4.0 or greater is required. Creating a back-port to earlier versions of Java would be possible, but it would be a very time consuming task to port, support, and test multiple versions of the software. For this reason, we only supported version 1.4.0 (or greater) for the pilot.

When using Internet Explorer 6.0 (or greater) the only requirements were that the Java plug-in was working, and that the browser is able to import PKCS#12 encrypted containers. This is a requirement that most certificate-enabled software is able to fulfil.

When using the Mozilla/Netscape/Firefox browsers the certificate and private key is directly copied into the browsers key-store. This tight integration created quite a few compatibility issues. To request a certificate only a correctly installed Java plug-in (>= 1.4.0) is required, but to install the certificate a native library (JSS) is loaded to install the certificate directly into the key-store. For this reason we require at least Netscape 7.0 because older versions come with an incompatible version of the JSS library.

Firefox was always shipped with a compatible version of JSS, but because of implementation problems versions earlier then 1.0 will almost certainly fail to import the private key and certificate.

The native library required to install the certificate and private key into the browser key-store is available for the following platforms:

- HP-UX 11.00 B (64 bit);
- Linux (>=2.4);
- Windows 98, 2000, XP;
- Solaris sparc (8, 2.6).

JSS for Max OS X on Power-PC is currently not officially supported, but it should be possible to compile the library from sources for this platform. We did not attempt to do this.

3. Appendix three: DCOCE Instructions for Registration Authorities (RAs)

As a Registration Authority, you will be required to verify that each user who applies for a digital certificate is who he/she claims to be, and that they are a current member of the college or department that you represent.

There are two possible application procedures:

1) The user visits the *certificates** web site and requests a certificate. During their application they will be given a 6-digit code and should make a print-out of their details. They then approach their RA for authentication.

2) The user approaches their RA to request a digital certificate before making a certificate request from their computer.

For either case, step-by-step instructions for you as the Registration Authority are provided overleaf.

It is very important that an applicant is not authenticated unless he/she can display a valid photo ID and can be confirmed as a current student or member of staff at your college or department.

The following are acceptable forms of photo ID:

- A valid passport
- A valid driving licence with photograph
- An Oxford University card

Whichever procedure is followed, after you have authenticated the applicant, a request will be sent to the Certificate Authority (CA). The CA will then review the application and, if it is acceptable, will generate a certificate. This process should not take longer than 24 hours. Once this process has been completed, the user will be informed by email (if they have provided an email address) that their certificate is ready to download. The applicant should then download their certificate to their own computer from the *certificates** web site.

ITSS users require access to additional services. As RA, you will need to enable them to access these service. Instructions for doing so are provided on the third page.

* https://certificates.oucs.ox.ac.uk/.

If you require assistance with any aspect of the authentication process, please contact the DCOCE team at dcoce@oucs.ox.ac.uk

Procedure 1 – User has already requested a certificate

This procedure should be followed when an applicant has already applied online for a certificate. The applicant will come to your office for you to verify their identity.

1. Open https://certificates.oucs.ox.ac.uk/. Click on 'Access the RA pages'.
2. Select 'RA Pending' from the drop-down menu.
3. Click on the 'Select' button next to the applicant's name.
4. Ensure that the applicant has valid photo ID that accurately confirms his/her name.
5. Confirm that the applicant is listed as a current student or staff member of your college or department (using your own database or staff lists, etc.).

    - Do not proceed with authentication unless steps 4 and 5 are completed satisfactorily.

6. Check the details of the online form, ensuring that all fields have been completed correctly. The email address is optional.
7. If the authentication is acceptable, click on the 'Approve' button to confirm the certificate application.

Procedure 2 – User has not yet requested a certificate

Using this method, it is you as the RA who prepares the certificate application. The applicant will come to your office both to have their identity verified and to receive a 9-digit code enabling them to download their certificate.

1. Open https://certificates.oucs.ox.ac.uk/. Click on 'Access the RA pages'.
2. Click on the box labelled 'Preauthenticate a User'.
3. Enter the applicant's details into the online form. Select 'GlobalSign Demo' as the CA (Certification Authority).
4. Ensure that the applicant has valid photo ID that accurately confirms his/her name.

    - Do not proceed with authentication unless step 4 is completed satisfactorily.

5. Click the 'Submit' button on the request form.
6. Verify that the applicant's details have been entered correctly and click 'Proceed' to continue, or click the 'Back' button to correct anything.
7. Print out the 'Digital Certificate Application' page containing the 9-digit code and hand it to the applicant. They will require this code in order to download their certificate to the computer that they normally work from.

Instructions for enabling ITSS access

IT Support Staff require access to additional services. As RA, you will need to enable them to access to the ITSS pages.

1. Complete the relevant certificate request process as described on the previous page.
2. From the main RA page, select 'RA Confirmed' from the 'Show requests with status' drop-down menu.
3. Click the 'select' button next to the name of the applicant who requires ITSS access.
4. That applicant's details will now appear on screen. Scroll down to the section of the page entitled 'Current role memberships'.
5. In the 'Available roles' option box, highlight 'ITSS' by clicking on it.
6. Click on the '<<Add' button.
7. You should now see 'ITSS' in the 'Active roles' box.
8. Other roles may be added or removed by highlighting the relevant text and using the 'add' and 'remove' buttons.
9. Enter the applicant's university card number in the appropriate text box.
10. Click on the 'Save changes' button to store their details.
11. The applicant should now be able to access ITSS services with their certificate (once it has been generated and downloaded to their computer).

If you require assistance with any aspect of the authentication process, please contact the DCOCE team at dcoce@oucs.ox.ac.uk

4. Appendix four: Further reading

The following represents a list of reference material that the project accumulated during its research and development work.

4.1. PKI and other implementations

http://www.grid-support.ac.uk/ The UK Grid Operations Support Centre.

http://edina.ed.ac.uk/projects/ties/ The TIES Project (Technologies for Information Environment Security) was based at EDINA, Edinburgh University Data Library. (See, for example, the final report of the TIES Project (Technologies for Information Environment Security) http://edina.ac.uk/projects/ties/ties_23-9.pdf).

http://www.personal.leeds.ac.uk/~ecldh/lurcis/ Leeds University's LURCIS/LUCIE project.

http://www.microsoft.com/technet/security/topics/identitymanagement/smrtcdcb/sec3/smartc07.mspx#ECAA CA hierarchy guidelines from Microsoft.

http://www.diversinet.com/products/passcertauth_benefits.asp Example of the use of RA hierarchies.

http://www.pkiforum.org/whitepapers.html OASIS PKI Member Section Whitepapers and Notes.

http://www.ietf.org/html.charters/pkix-charter.html The IETF PKIX (X.509-based PKI) Working Group.

http://www.nhsia.nhs.uk/security/pages/cryptographic/guidance/ NHS PKI Policy and Guidelines (may be obsolete).

http://www.uth.tmc.edu/netcenter/middleware/digital-id/index.html University of Texas Health Science Centre at Houston PKI implementation.

http://www.ea.mtu.edu/resources/pki.shtml PKI resources listed by Michigan Technological University.

http://www.dga.co.uk/customer/publicdo.nsf/0/4471C26D38117191802568B70055FFD9?OpenDocument ELLISON, C and SCHNEIER, B. Ten Risks of PKI: What you're not being told about public key infrastructure. *Computer Security Journal*, 11(1), 2000.

http://middleware.internet2.edu/hepki-tag/ Internet2 Higher Education PKI Technical Activities Group (HEPKI-TAG).

http://www.gla.ac.uk/projects/scotmid/gendocs/imppki-smp.html BLAIR, E and AITON, A. Issues in the Implementation of PKI in UK HE/FE. *University of Glasgow web publication*, 2001.

http://www.verisign.com/repository/crptintr.html8 Verisign's Introduction to Public Key Cryptography.

4.2. Authentication and authorisation

http://dsd.lbl.gov/Akenti/ Akenti project regarding policy-based access control using PKI standards.

http://www.permis.org/ PrivilEge and Role Management Infrastructure Standards Validation (PERMIS) project at the University of Salford, UK.

4.3. Cryptography

http://lasecwww.epfl.ch/~oechslin/publications/crypto03.pdf The improved cryptanalytic time-memory trade-off is described in this paper, by Philippe Oechslin, published on-line.

http://www.cs.auckland.ac.nz/~pgut001/tutorial/index.html Peter Gutmann's godzilla crypto tutorial.

GARFINKEL, S and SPAFFORD, G. Web Security, Privacy and Commerce. Second Edition. *O'Reilly & Associates Inc.*, USA, 2002.

SCHNEIER, B. Secrets and Lies: digital security in a networked world. *Wiley Computer Publishing*, USA, 2000.

4.4. Other access management

http://www.athensams.net/ Eduserve's Athens - an Access Management system for UK higher and further education and National Health Service sectors controlling access to web based subscription services.

http://www.athensams.net/development/devolved_authentication/ Athens Devolved Authentication.

http://shibboleth.internet2.edu/ The Shibboleth initiative.

4.5. Privacy

http://www.ala.org/alaorg/oif/ethics.html Code of Ethics of the American Library Association (1995).

http://www.law.georgetown.edu/faculty/jec/read_anonymously.pdf
COHEN, J.E. A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace. *Connecticut Law Review, 28*(4), 1996, 981-1039.

4.6. JISC middleware programmes and projects

http://www.jisc.ac.uk/index.cfm?name=middleware_announce Latest (at time of writing) middleware projects, many involving Shibboleth.

http://www.jisc.ac.uk/index.cfm?name=circular_06_02 The JISC call for Projects in Authentication, Authorisation and Accounting (June 2002) for which the DCOCE project formed a successful bid.

http://www.angel.ac.uk/index.html The Authenticated Networked Guided Environment for Learning group of projects based at the London School of Economics.

http://edina.ed.ac.uk/projects/ties/ The TIES Project (Technologies for Information Environment Security) was based at EDINA, Edinburgh University Data Library. (See, for example, the final report of the TIES Project (Technologies for Information Environment Security) http://edina.ac.uk/projects/ties/ties_23-9.pdf).

http://www.personal.leeds.ac.uk/~ecldh/lurcis/ Leeds University's LURCIS/LUCIE project.

4.7. Miscellaneous

http://www.safenet-inc.com/products/ikey. Rainbow Technologies (later SafeNet) provided the DCOCE project with a set of iKeys to evaluate.

http://www.dcoce.ox.ac.uk/glossary/ A very useful glossary

http://www.w3.org/WAI/WCAG1AA-Conformance Web Content Accessibility Guidelines from the W3C.

http://xml.coverpages.org/techSociety.html#security Useful list of resources on Security, Privacy, and Personalisation from OASIS.

4.8. Evaluation and surveys

http://www.useit.com/alertbox/20040202.html Nielsen, Jakob. "Keep Online Surveys Short". Jakob Nielsen's Alertbox, February 2, 2004.

http://downloads.peter.baumgartner.name/gems/peter/articles/eval_easa97.pdf BAUMGARTNER, P. and PAYR, S. Methods and practice of software evaluation: The case of the European Academic Software Award (EASA). In*: Proceedings of ED-MEDIA 97 - World Conference on Educational Multimedia and Hypermedia*, Edited by . Charlottesville: AACE, 1997, 44-50.

British Standards Institute. Information technology – Software product quality – Part 1: Quality model; ISO/IEC 9126-1:2001, BSI, 2001.

http://www.tickit.org/measures.pdf DISC TickIT Office. Getting the measure of TickIT, guidance and information about the emerging ISO measurement standards for improving software processes and how they relate to ISO 9001: 2000, London .

http://www.dcs.shef.ac.uk/~katerina/EACL03-eval/eacl-doc/King.pdf KING, M. Living up to standards, TIM/ISSCO, ETI, University of Geneva.