

# Digital Certificate Operation in a Complex Environment

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

## PROJECT PLAN

**Project abbreviation** DCOCE

**Project Title** Digital Certificate Operation in a Complex Environment

**Start Date** 1 January 2003

**End Date** 31 December 2004

**Lead Institution** University of Oxford (Computing Services; Library Services; e-Science Centre)

**Project Director** Prof Paul Jeffreys  
**Co-Director** Dr Mike Fraser

**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

**Partner Institutions** 1) Manchester Information and Associated Services (MIMAS)  
2) EduServ (Athens)

### Document History

Version	Date	Comments
1.0	12 June 2003	

## 1. Introduction

The Digital Certificate Operation in a Complex Environment (DCOCE) project forms part of the Authentication, Authorisation and Accounting (AAA) middleware programme, funded and stimulated by the Joint Information Systems Committee (JISC).

### 1.1. Background

There is extensive background to the programme on the JISC website at [http://www.jisc.ac.uk/index.cfm?name=programme\\_aaa](http://www.jisc.ac.uk/index.cfm?name=programme_aaa). However, the excerpt below is taken from the programme description in order to contextualise the DCOCE project.

*Although many resources on the JANET network and the wider Internet are freely accessible, many of those of greatest interest are copyright material licensed from the rights holders, or are resources whose use needs to be controlled for other reasons. Managing access to such resources involves a number of processes, i.e.*

- *authentication - identifying the person requesting the access*
- *authorisation - determining from that person's identity, and often using other sources of information, what privileges the individual has and hence whether access should be allowed or not*
- *accounting - maintaining logs of events for the purpose of generating management information on resource usage*

*International standards in these areas are beginning to emerge and the JISC works actively with partner institutions in other countries to facilitate this development. The programme is designed to advance practical understanding of the latest developments in the UK academic and research community. It is intended to address both the general needs for access management to electronic library materials and learning objects, and also the more specialised needs of the e-science research programme.*

### 1.2. The Digital Certificate Operation in a Complex Environment (DCOCE) project

Where the Digital Certificate Operation in a Complex Environment (DCOCE) project fits in here is within the 'authentication' part of the programme. Digital certificates have been implemented in less complex organisations in the UK and – to a certain degree – within large universities in the USA. They have also been used within universities in the UK to a lesser extent. The aim of this project, as proposed below, is therefore to investigate the issues and implications arising from a 'real world' implementation of digital certificates and public key infrastructure (PKI) within a relatively complex environment – in terms of users, mobility and the diversity of services accessed – namely the University of Oxford.

The University of Oxford is one of the world's leading higher education institutions undertaking teaching and research across a very wide range of academic subjects. The University's full time student population numbers almost 18,500, of whom about 5,500 are engaged in postgraduate work. In addition, the University offers one of the UK's most extensive programmes of lifelong learning, and every year more than 16,500 people take courses offered by the University's Department for Continuing Education. The University maintains one of the largest Local Area Networks in Europe both in terms of geographic extent and the number of nodes connected to it. Within the network the University has

developed an extensive collection of digital resources, combining local and subscription-based collections, many of which are derived from the JISC collections. The University of Oxford is also a regional e-Science Centre, based at the Computing Services and the Computing Laboratory. The University of Oxford is therefore a highly complex organisation that shares much in common with the complexity of other large educational institutions and higher education as a whole within the UK.

## **2. Aims and Objectives**

### **2.1. Overall aim**

The overall aim of the project described in this bid is to provide a detailed implementation and evaluation report of 'real world' digital certificate services at the University of Oxford.

#### **2.1.1. Objectives within this aim**

- a) Development for, and implementation of, a public key infrastructure using digital certificates that will form a pilot project involving a selection of users within the University of Oxford.
- b) Evaluations, both technical and user-oriented of a wide variety of aspects surrounding the implementation of PKI at higher education establishments within the UK. The evaluations will be collated into a final report.
- c) Dissemination of a series of reports – via web pages, email lists and at real ‘events’ – of the progress of the project, documenting successes and failures and points of difficulty. These and the final report should be disseminated in a form that will be useful to others considering PKI within the higher and further education sector in the UK.

### **2.2. Further aims**

The project should:

- attempt to learn from the experience of other implementations in this area<sup>†</sup>;
- work in partnership with organisations involved in devolved authentication and/or interested in using certificates themselves;
- work in partnership with organisations having an interest in promoting the use of digital certificates and public key infrastructure.

#### **2.2.1. Objectives arising from these aims**

- a) The project should demonstrate successful authentication for access to external resources protected by the Athens Access Management System.
- b) Similarly, integration should be achieved with the Zetoc (Z39.50-compliant access to the British Library's Electronic Table of Contents) resource managed by Manchester Information and Associated Services (MIMAS).
- c) The project should work closely with (and be advised by) the national e-Science Grid via the Oxford e-Science Centre. It is hoped that the findings of the project will be of use to the e-Science Grid and all endeavours will be made to ensure that this is so.
- d) The project should conduct a brief review of a few public key infrastructure implementations. This is to inform the choice of methodologies and technologies to be piloted. Publication and evaluation in this area will be limited.

---

<sup>†</sup> Although this is an overall aim, a full review of existing methodologies and technologies is not anticipated.

### **3. Overall Approach**

#### **3.1. Review of existing technologies and implementations**

The overall approach of the project is to roll out a digital certificate/public key infrastructure implementation to a group of users across the University of Oxford. One major challenge when planning this project was to avoid lengthy delays in reviewing existing technologies and picking the best practice. Therefore, it is likely that a brief review of other implementations will be undertaken before selecting an administration and technical architecture. Thus, a balance between ‘best of breed’ and ‘pragmatic choice at this time’ will have to be struck. The Research Technologies Service (RTS) at Oxford University Computing Service (OUCS) has a commitment to open standards and open source software. The project will abide by these commitments as much as is pragmatically possible. However, if it would take too long to develop an open source solution during the project, then the decision will be taken to use whatever is available at the time.

#### **3.2. Evaluation**

During the development and rollout, all steps will be taken to publish decisions, findings and progress on the world wide web. These evaluations will be largely formative, but where the process allows – and where it would be most useful – summative evaluations will be adopted.

Evaluative procedures are to be carried out at each stage and can take the forms of:

- recording decision-making processes;
- summative evaluation of software/system choices;
- user needs evaluation (but this will likely be combined with the above);
- summative performance/utility evaluation;
- formative evaluation with respect to repeating a pilot or undertaking a major rollout.

#### **3.3. Development/implementation**

The development phase is likely to overlap with other phases of the project, especially evaluation and – to some degree – rollout. It is possible that the Project Board will decide against a high degree of novel development, given the time constraints, and either an ‘off the shelf’ commercial or open source ‘package’ will be implemented or an implementation methodology from another site/project will be adopted. There is likely to be some development required for whichever model that is eventually adopted (e.g. integration of existing directory information/attribute services at Oxford with the new public key infrastructure requirements).

Implementation – by definition – is likely to be complex and part of the aim of the project is to evaluate and document the process for the benefit of future similar implementations.

### 3.4. Rollout

The rollout phase of the project will deliver digital certificate mediated services to:

- University IT support staff distributed amongst the colleges and departments of the University;
- a sample cross-section of users requiring access to remote resources served by Oxford University Library Services;
- (if possible) academic visitors to the University requiring access to Grid resources served by the Oxford e-Science Centre.

Access to remote services (the Athens Devolved Authentication service and the Zetoc resource, as introduced above) is also planned as part of the rollout. If possible, services associated with the national Grid via the Oxford e-Science Centre will also be mediated using the digital certificates issued under this project.

It is expected that the rollout process will raise issues of note relevant to the overall evaluation of the project and that rollout will overlap heavily with the development/implementation phase. Further, as certificates are initially to be issued to very few users, it is likely that issues will be raised that provide useful information for partial re-development and documentation before the majority of the certificates are issued to participants.

### 3.5. Revocation and exit strategy

During the rollout phase, issues surrounding the revocation (*conceptually similar to withdrawal*) of certificates are to be investigated. At the end of the practical part of the project, the certificates will be revoked as per an agreed exit strategy.

At this stage, and throughout the project, an exit strategy will be considered for a full-scale implementation of digital certificates within a public key infrastructure in a complex environment, such as the University of Oxford.

### 3.6. Publication/Dissemination

During the project, important information for stakeholders and other interested parties will appear from time to time. Suitable outlets for this information include:

- specific pages on the project web site;
- reports accessible from the project web site;
- discussion lists, either directly pertaining to the project, the programme, or other relevant projects and groupings;
- physical meetings, organised or attended by the programme, the University of Oxford Computing Services or by the Project Team.

At the end of the project, a series of reports and an overall summary will be produced. These are likely to be disseminated in the same ways as those listed above. Academic and practitioner-oriented journals and other outlets will also be considered at this stage in order to disseminate the project findings as far as possible.

## **4. Project Consortium**

The external partner institutions are as follows: Manchester Information and Associated Services (MIMAS) and EduServ (Athens). The project is to be based within Oxford University Computing Services and local institutional partners are the Systems and Electronic Resources Service at Oxford University Library Services (SERS, OULS) and the Oxford e-Science Centre (OeSC).

### **4.1. Manchester Information and Associated Services (MIMAS)**

MIMAS host Zetoc (more verbosely the *Z39.50-compliant access to the British Library's Electronic Table of Contents*). This is a system whereby users can search for keywords and text to discover journal articles and conference proceedings and register to receive alerts. This can be done via a web interface or through other software that is Z39.50 compliant. Usually, obtaining a password for Zetoc depends on authentication from the user's institution. The DCOCE project will investigate and – if possible implement as part of the pilot scheme – direct access to Zetoc, including personalisation services, via digital certificates.

This means a form of devolved authentication and MIMAS will work with the main project developers at Oxford University Computing Services to ensure that the use of the digital certificates and the certification practices statement meets with their approval, general standards and longer term aims.

Further to the above, MIMAS is also working with Manchester Computing and the e-Science Centre for the North West to conduct a technical evaluation of the authorisation system, Akenti. The authorisation evaluation will be conducted through access to Zetoc. The system will be made accessible both as a web server (through digital certificates embedded in the user's web browser alongside traditional Athens authentication – see below) and as a web service (using the Globus Grid Security Infrastructure authentication). The end date of this project – named ‘Akenti Access to zetoc’ (A2Z) – is November 2003. Thus, MIMAS has an excellent background in working with digital certificates for authorisation and authentication, and this experience will be invaluable.

It is envisaged that one or more representatives at MIMAS will be part of the stakeholder group. Workpackage eight has been designated as the Zetoc rollout and testing phase of the project. However, MIMAS will be involved at an earlier stage during the initial review and modelling (workpackages three and four), possibly a little during development and testing (workpackage five) and will have input to the certification practices statement (workpackage nine). MIMAS may assist and advise during the user evaluation and possibly more generally during the evaluation and reporting phase at the end of the project.

### **4.2. EduServ (Athens)**

Athens is primarily an access management system for controlling access to web-based subscription services, open to the UK Higher Education and Health communities. In the parlance of public key infrastructure and access management, Athens is mostly concerned with authentication and authorisation. Authorisation is the aspect of access management that controls privileges and entitlements to resources. Decisions on authorisation are commonly made on user attributes; for example that the user is a member of Institution *x*, or that they are a postgraduate. Athens has a Devolved Authentication Service (AthensDA) that encourages *local* authentication so that the initial single sign on is performed using local credentials, which may be X.509 certificates.

The DCOCE project aims to interface with the devolved authentication service using X.509 digital certificates as well as possibly interfacing directly with the authentication mechanisms

at Athens. Guidance from Athens/EduServ staff will be sought regarding the certification practices statement, general standards pertaining to certificate use and any associated issues.

It is envisaged that one or more representatives from Athens (possibly within the AthensDA team) will be part of the stakeholder group. Workpackage seven has been designated as the Athens rollout and testing phase of the project. However, Athens/EduServ will be involved at an earlier stage during the initial review and modelling (workpackages three and four), possibly a little during development and testing (workpackage five) and will have input to the certification practices statement (workpackage nine). Athens/EduServ may assist and advise during the user evaluation and possibly more generally during the evaluation and reporting phase at the end of the project.

#### **4.3. Systems and Electronic Resources Service at Oxford University Library Services (SERS, OULS)**

The Systems and Electronic Resources Service at Oxford University Library Services have an interest in access to external resources and sources of information for users at/via Oxford. In the University of Oxford's IT Strategic Framework (2000, <http://www.ox.ac.uk/it/strategy/2000/index.html>), one of the elements within the Libraries Curators' Strategy is to address "...the issues of user authentication and database access and licensing with a view to optimising provision (perhaps through a single log-on)". This shows how authentication plays a role in licensing of access to resources through the libraries, but it is also true that simplicity and ease of access is also a factor. These and other disparate issues, including the use of the virtual private network (VPN) makes SERS input to the project invaluable.

SERS will have a leading strategic role in the project and will provide evaluation resources for the project. Staff from SERS will act as stakeholders in the project and will contribute to the Project Board. Its involvement will be throughout.

#### **4.4. Oxford e-Science Centre (OeSC)**

A very substantial e-Science activity, underpinned by the Grid, has grown up in the University over the last two years (<http://www.e-Science.ox.ac.uk>), which embraces computer services and computer science, and underpins leading scientific research.

Oxford is a key player in the UK National Grid, and has a number of flagship projects, including, in particular, a digital mammography project named e-DiaMoND: (<http://www.Gridoutreach.org.uk/docs/pilots/ediamond.htm>).

The growth of e-Science has some important consequences, as it:

- enables, and encourages world-leading research underpinned by and driven by the requirements of e-Science;
- is a hybrid between Computer Services and Computer Science;
- leads to new technical challenges.

The technical challenges include:

- authentication and authorisation;
- Quality of Service, often associated with higher network bandwidth demands;

When looked upon in the long-term, such issues begin as challenging new IT requirements, and gradually move to become 'general utility' and part of the IT infrastructure.

Oxford has a particular responsibility within the national e-Science programme. It is endeavouring, through OUCS, to create a bridge between the e-Science middleware developers and the university computing services across the country. It is leading the way towards the creation of a production Grid that will provide users with the rich resources available, without their needing to be experts in Grid software. Absolutely key to this is a full understanding of the use of digital certificates in complex higher education establishments, and it is anticipated that the e-Science programme and the DCOCE project will be complementary.

Oxford is working closely with CCLRC to create the bridge and have, together, organised a series of workshops where e-Science middleware experts and computer service technical experts have been brought together.

## **5. Project Management**

### **5.1. Project management structure**

The project is comprised of a small Project Team, largely working within Oxford University Computing Services and Oxford University Library Services. Project partners are to be consulted regularly, although there are scheduled phases that involve partners and much of the collaborative work is likely to be performed during these phases. See Figure 5.1 for a summary of the overall project structure, showing the reporting lines.

### **5.2. Project Team**

The Project Team comprises a project manager, a systems programmer and one full time equivalent evaluation officer. The evaluation officer post is made up of two half time equivalent people – one based in Oxford University Computing Services and the other in Oxford University Library Services. The Project Director has a direct role in ensuring the success of the project as the pilot implementation requires the cooperation of different bodies and users across the University. Other staff within Oxford University Computing Services will be active within the project on an occasional basis and the use of these *ad hoc* resources will be coordinated by the project manager.

### **5.3. Project Board**

The Project Board will comprise:

- one senior member of staff within Oxford University Computing Services
- the Project Director and co-Director
- one senior member of staff within Oxford University Library Services
- one senior member of staff from the Oxford e-Science Centre
- one other person to be appointed if the board requires another area of expertise

The Project Director will chair the Project Board.

The Project Board will meet on a regular basis, probably monthly, or as required by the Project Director.

The Project Manager will usually report to the Project Board. However, any one of the Project Team may be required to appear at Project Board meetings.



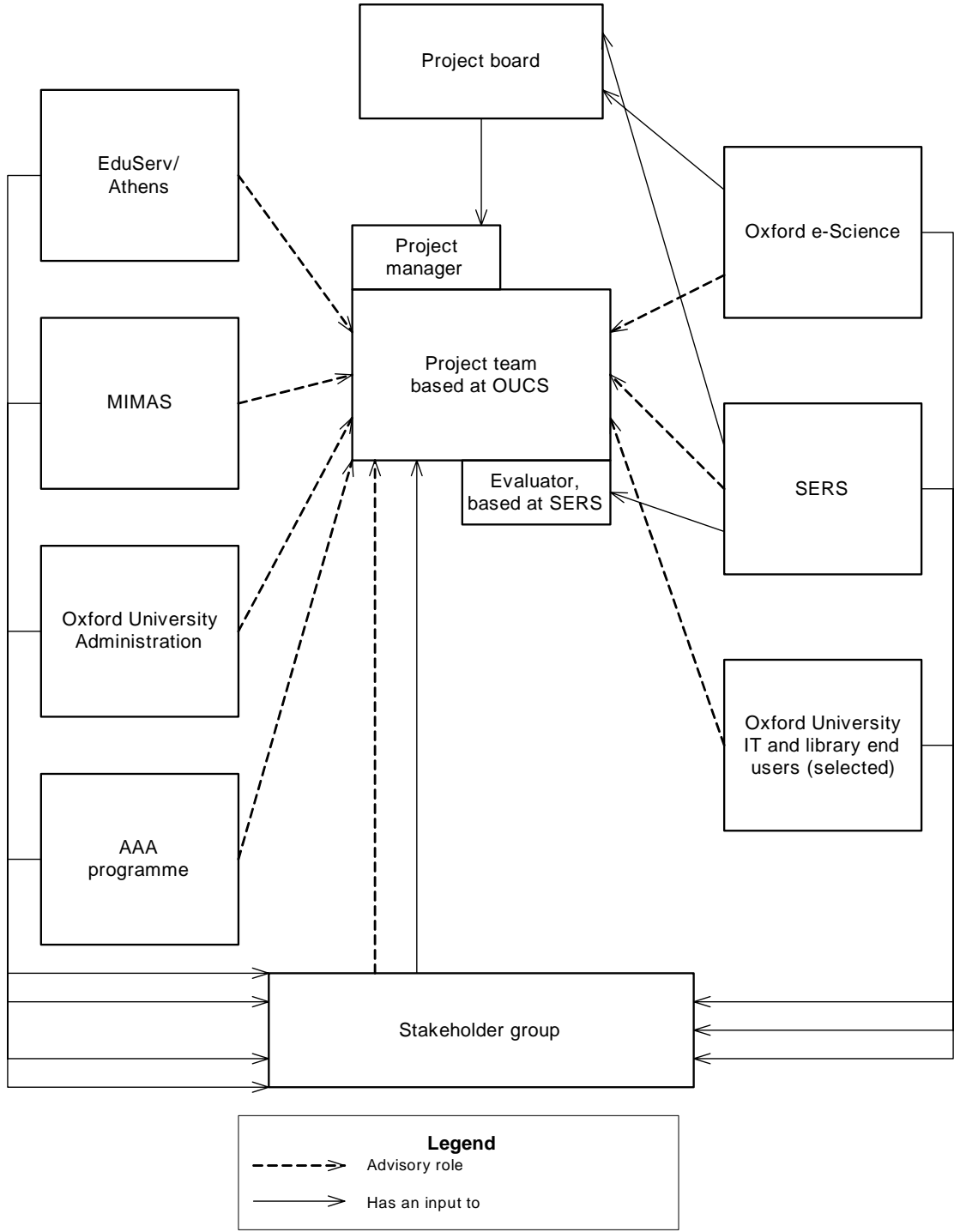


Figure 5.1 DCOCE project management structure and communication lines.

### 5.4. Stakeholder and user groups

The stakeholder group will be consulted after most of the major milestones. The consultation may be via email or other means, but several attendance-based meetings will take place during the lifetime of the project. There will also be scope for a technical group, nominated by the main stakeholders so that stakeholders can attend or consult with a technical person from within their own organisation. It may even be useful at some stage to host a meeting made up entirely of the technical nominees.

The main stakeholder group is likely to be comprised as follows.

- staff from Oxford University Computing Services
- staff from Oxford University Library Services
- staff from EduServ (Athens)
- staff from Manchester Information and Associated Services
- staff from Oxford e-Science centre
- a representative from the JISC Authentication, Authorisation and Accounting middleware programme
- selected end-users within the IT services at Oxford
- selected end-users within the library services at Oxford
- others with an interest in digital certificates or the success of the project (possibly from other projects within the programme)
- relevant University central administrative staff, probably from MIS
- A representative nominated by the Oxford University IT users group

The stakeholder group will be chaired by the project manager and will be consulted regularly as a source of expertise and experience. The stakeholder group may encompass a user group in terms of membership and therefore the formation of a specific user group may not be necessary.

If required, a user group will be formed later in the project. As this is a middleware project, it may, however, prove useful to form user (or working) groups from users involved in the administration (clerical) of issuing the certificates and from those involved in the technical support of the certificates. These people may have interesting input for the evaluation and the end reports. Oxford University Computing Services has two communities of users/experts involved in authentication and authorisation and it is expected that these communities will have an input to the project as an advisory resource and as stakeholders and users.

## **5.5. Reporting and escalation lines**

On a daily basis, the evaluation officers and the system developer report to the project manager, who in turn reports to the project director and the Project Board. Major unforeseen decisions pertaining to the project will be put to the project board for a rapid decision. Any changes to the project plan must be addressed to the Project Board. Such important issues will be discussed with the stakeholders at the nearest convenient time. Stakeholders will be alerted via email and will have the opportunity to comment and have meaningful input via email discussion lists.

## 6. Overall Project Structure

### 6.1. Project summary

Figure 6.1 shows the main workpackages (WKPs) and their dependencies.

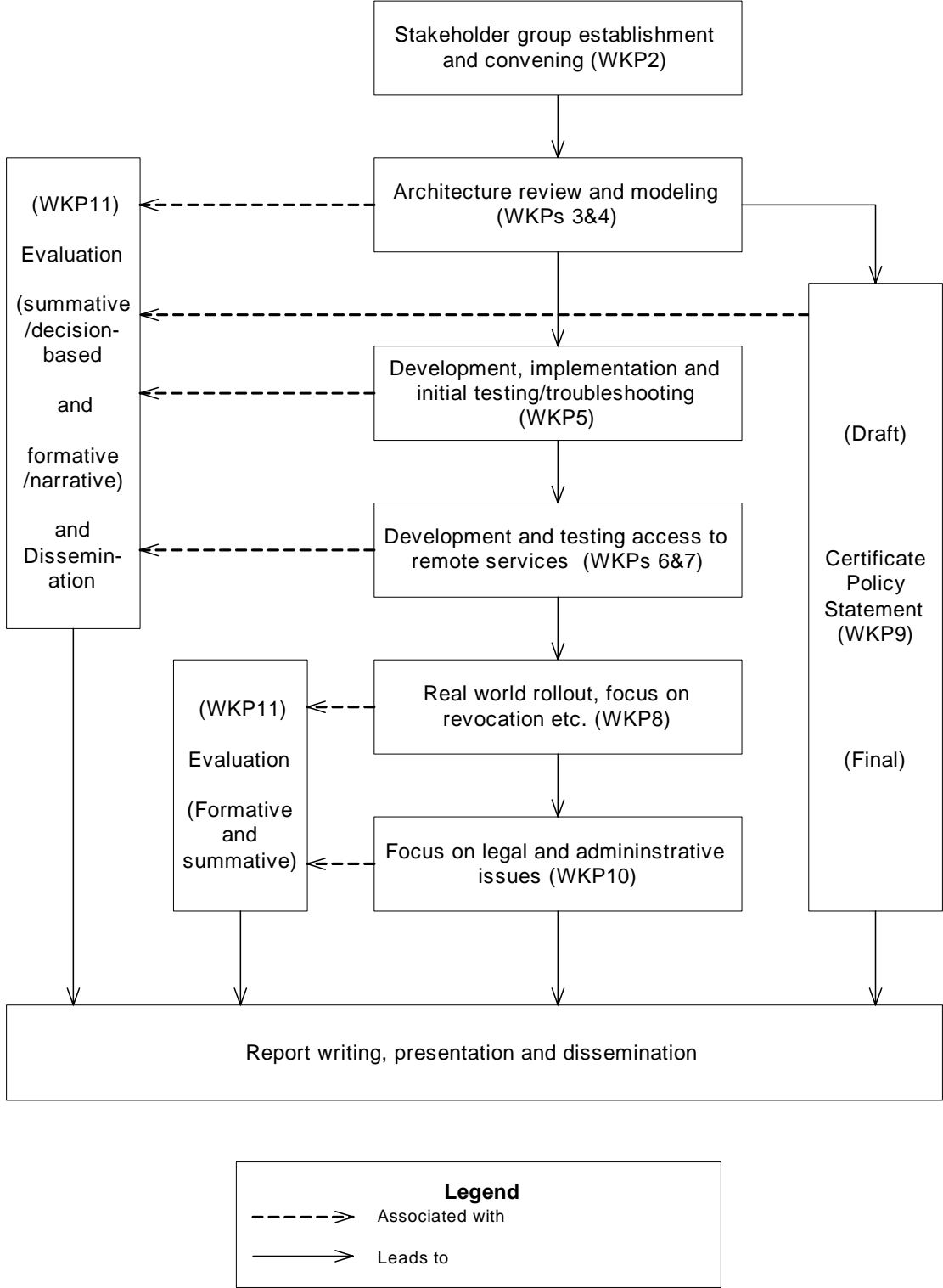


Figure 6.1 Diagrammatic representation of the work packages and their dependencies

6.2. Project time line

Figure 6.2 shows the estimated project timeline.



Figure 6.2 Project time line for the DCOCE project

## 7. Detailed Project Plan

### 7.1. Workpackage 1

**Workpackage Title:** Project management  
**Partner Responsible:** OUCS  
**Other Partners Involved:** 1 January 2003  
**Start Date:** 24 December 2005  
**End Date:**

**Objectives:** Ensuring the project completes to schedule, budget and within reasonable scope.

**Brief Description of Work:** Management of DCOCE project, development of a detailed workplan; ensure adequate liaison and reporting between the project and stakeholders including funding bodies.

**Quality Assurance and Review:** The JISC guidelines regarding project management and reporting will be followed. The Project Board will monitor the overall project management.

**Outputs including reports:** Project workplan; reports as required by stakeholders; overall project deliverables.

#### 7.1.1. Task Descriptions

Task	Title	Partners	Description
1.1	Project Management		Overall management of project, including budgeting, planning, execution and reporting.
1.2	Workplan		Development and maintenance of a detailed workplan.
1.3	Reporting		Liaison and reporting between the Project Team and stakeholders, partners and JISC.
1.4	Milestone reports and consultation		Ensuring that stakeholders and partners are made aware of progress after each major milestone

## 7.2. Workpackage 2

<b>Workpackage Title:</b>	<b>Stakeholder group</b>
<b>Partner Responsible:</b>	OUCS, SERS
<b>Other Partners Involved:</b>	MIMAS, Athens, OeSC
<b>Start Date:</b>	March 2003
<b>End Date:</b>	June 2003
<b>Objectives:</b>	Ensuring the project has an active, informed and informative stakeholder group.
<b>Brief Description of Work:</b>	Select and engage stakeholders. Keep stakeholders informed and process received feedback.
<b>Quality Assurance and Review:</b>	The Project Board, other stakeholders and partners are very likely to highlight any stakeholders that are initially missing from the group. The terms of reference of the group will be debated fully and openly before acceptance.
<b>Outputs including reports:</b>	Establishment and convening of group. Establishment and maintenance of reporting procedures. Stakeholders will be made aware of milestone reviews as they appear or are published.

### 7.2.1. Task Descriptions

Task	Title	Partners	Description
2.1	Establish group	OeSC, MIMAS, Athens	Consult widely and establish who should take part. Contact these players and set-up email distribution lists.
2.2	Convene group		Call first real meeting.
2.3	Terms of reference		Circulate terms of reference before meeting, to be agreed <i>at</i> meeting.
2.4	Project web site		Establish web site with goals and publish to stakeholders. Consult on web site.

### 7.3. Workpackage 3

**Workpackage Title:** Modelling of administration architecture  
**Partner Responsible:** OUCS, SERS  
**Other Partners Involved:** MIMAS, Athens, OeSC  
**Start Date:** October 2003  
**End Date:** February 2004

**Objectives:** Review existing projects and plan Oxford implementation alongside Workpackage 4.

**Brief Description of Work:** Select four PKI implementations and review briefly. Use this knowledge to build an administration architecture model for Oxford. Athens, MIMAS and OeSC to advise and ratify choice of four projects and to review initial proposals for models.

**Quality Assurance and Review:** The Project Board will monitor the work of the Project Team throughout this workpackage. Protocols for decision-making form part of the work of the evaluation workpackage (WKPG 11). These protocols will be published before they are used in order for feedback to be received. The eventual model will be reviewed with stakeholders over email and at actual meetings.

**Outputs including reports:** Documented administration architecture model that is realistic alongside the system architecture model.

#### 7.3.1. Task Descriptions

Task	Title	Partners	Description
3.1	Select group of projects	OeSC	Through consultation, choose four projects to review lightly.
3.2	Review projects		Review projects in terms of admin. architecture alongside work for Workpackage four on system architecture.
3.3	Review Athens and Zetoc admin. requirements	Athens, MIMAS	
3.4	Build use-case/policy scenarios and requirements for PKI/certificate use	OeSC	

---

<b>Task</b>	<b>Title</b>	<b>Partners</b>	<b>Description</b>
3.5	Build administration architecture proposal	OeSC	Build proposal alongside system architecture (workpackage four).
3.6	Review models with stakeholders	OeSC, Athens, MIMAS	Ensure proposals meet the requirements of all stakeholders. If this is not possible, then document major issues in depth.



## 7.4. Workpackage 4

<b>Workpackage Title:</b>	<b>Modelling of system architecture</b>
<b>Partner Responsible:</b>	OUCS, SERS
<b>Other Partners Involved:</b>	MIMAS, Athens, OeSC
<b>Start Date:</b>	October 2003
<b>End Date:</b>	February 2004
<b>Objectives:</b>	Review existing projects and plan Oxford implementation alongside Workpackage 3.
<b>Brief Description of Work:</b>	Briefly review the four selected PKI implementations. Use this knowledge to build a system architecture model for Oxford. Athens, MIMAS and OeSC to advise and ratify choice of four projects and to review initial proposals for models.
<b>Quality Assurance and Review:</b>	The Project Board will monitor the work of the Project Team throughout this workpackage. Protocols for decision-making form part of the work of the evaluation workpackage (WKPG 11). These protocols will be published before they are used in order for feedback to be received. The eventual model will be reviewed with stakeholders over email and at actual meetings.
<b>Outputs including reports:</b>	Documented system architecture model that is realistic alongside the admin. architecture model.

### 7.4.1. Task Descriptions

Task	Title	Partners	Description
4.1	Review selected projects for system architecture		Review projects in terms of system architecture alongside work for Workpackage three on admin. architecture.
4.2	Build use-case/policy scenarios and requirements for PKI/certificate use	OeSC	Work alongside admin. architecture (workpackage three).
4.3	Build system architecture proposal	OeSC	Build model/proposal alongside admin. architecture (workpackage three).
4.4	Build deployment plan	OeSC	
4.5	Review models with stakeholders	OeSC, Athens, MIMAS	Ensure proposals meet the requirements of all stakeholders. If this is not possible, then document major issues in depth.

## 7.5. Workpackage 5

<b>Workpackage Title:</b>	<b>Development and initial implementation</b>
<b>Partner Responsible:</b>	OUCS, SERS
<b>Other Partners Involved:</b>	OeSC
<b>Start Date:</b>	February 2004
<b>End Date:</b>	May 2004
<b>Objectives:</b>	To implement, and where necessary develop, the systems and administrative processes to support a certificate life-cycle within a public key infrastructure according to the models designed in earlier workpackages.
<b>Brief Description of Work:</b>	Development of architectures and very small-scale rollout. Development or implementation of (or integration with) a certificate authority. Initial testing. OeSC to play advisory role during the development and initial rollout phase.
<b>Quality Assurance and Review:</b>	The Project Board will monitor the work of the Project Team throughout this workpackage. Development/implementation will be carried out to the models that arose from workpackages three and four. Any unforeseen practicality that necessitates a deviation from the model will be reviewed immediately with the Project Board and/or the stakeholders.
<b>Outputs including reports:</b>	Working infrastructure (system and administrative). A few end-users using digital certificates (Project Team and a few IT support staff).

### 7.5.1. Task Descriptions

<b>Task</b>	<b>Title</b>	<b>Partners</b>	<b>Description</b>
5.1	Development of attribute server		
5.2	Certificate Authority 'back end' work	OeSC	This depends on the architecture chosen, and could be an implementation and/or a development task.
5.3	Certificate storage	OeSC	Checking that storage and delivery mechanisms work or development of new mechanisms.
5.4	Administration 'front end'		Development or configuration of user interface for administrators.

<b>Task</b>	<b>Title</b>	<b>Partners</b>	<b>Description</b>
5.5	User 'front end' as necessary		Any remaining user interface development or configuration (including delivery mechanism).
5.6	Communication/ bindings		Development and configurations of all connecting pieces.
5.7	Deployment and documentation		Plans for deployment and technical documentation
5.8	Certification revocation mechanism	OeSC	Technical and administrative implementation of revocation system.
5.9	Very limited rollout	OeSC	Rollout to very few users and troubleshooting at this stage.
5.10	Initial testing/ verification	OeSC	Testing within the confines of the few staff to have been issued with certificates at this stage.
5.11	Implementation/ training for admin. architecture		Bring in administrators for certificate management and revocation.
5.12	User groups		If necessary establish user-groups as well as involving the stakeholders. User groups will define who is part of the wider rollout (Workpackage eight).
5.13	Rollout to IT support staff	OeSC	Focus on providing IT support staff (centrally and throughout the colleges) access to information applications certificate compliant.

## 7.6. Workpackage 6

<b>Workpackage Title:</b>	<b>Athens Devolved Authentication</b>
<b>Partner Responsible:</b>	OUCS, SERS
<b>Other Partners Involved:</b>	Athens
<b>Start Date:</b>	June 2004
<b>End Date:</b>	June 2004
<b>Objectives:</b>	To enable access to remote resources subscribed to by Oxford compliant with Athens single sign-on (SSO) via digital certificate authentication.
<b>Brief Description of Work:</b>	Examining Athens requirements and standards. Ensuring certificates and 'presentation' (presentation) mechanisms comply and PKI can be trusted.
<b>Quality Assurance and Review:</b>	The mechanisms of access to Athens mediated services will have been published as part of workpackages three and four. Testing and feedback from users and Athens will be sought as part of workpackage eleven. Therefore, the quality of the plan and the provision should be high enough to meet the requirements.
<b>Outputs including reports:</b>	Compliant certificate authentication mechanism for Athens SSO implemented and tested. Report on requirements, issues, decisions and consequences.

### 7.6.1. Task Descriptions

<b>Task</b>	<b>Title</b>	<b>Partners</b>	<b>Description</b>
6.1	Establish requirements	Athens	Early during the main work of Workpackages three and four a set of requirements is to be established.
6.2	Design any specifics for Athens	Athens	During the main development work (workpackage five), any specific development will be carried out.
6.3	Testing access to Athens SSO services.	Athens	Testing and troubleshooting.
6.4	Reporting as within workpackage 11.	Athens	Feedback from Athens regarding reports and success.

## 7.7. Workpackage 7

**Workpackage Title:** MIMAS (Zetoc)  
**Partner Responsible:** OUCS, SERS  
**Other Partners Involved:** MIMAS  
**Start Date:** June 2004  
**End Date:** June 2004

**Objectives:** To enable access to remote Zetoc/British Library resources via digital certificate authentication mechanism.

**Brief Description of Work:** Examining MIMAS/Zetoc requirements and standards. Ensuring certificates and 'presentation' (presentment) mechanisms comply and PKI can be trusted.

**Quality Assurance and Review:** The mechanisms of access to the remote Zetoc/British Library resources will have been published as part of workpackages three and four. Testing and feedback from users and MIMAS will be sought as part of workpackage eleven. Therefore, the quality of the plan and the provision should be high enough to meet the requirements.

**Outputs including reports:** Compliant certificate authentication mechanism for Zetoc implemented and tested.  
 Report on requirements, issues, decisions and consequences.

### 7.7.1. Task Descriptions

Task	Title	Partners	Description
7.1	Establish requirements	MIMAS	Early during the main work of Workpackages three and four a set of requirements is to be established.
7.2	Design any specifics for Zetoc	MIMAS	During the main development work (workpackage five), any specific development will be carried out.
7.3	Testing access to Zetoc service.	MIMAS	Testing and troubleshooting.
7.4	Reporting as within workpackage 11.	MIMAS	Feedback from MIMAS regarding reports and success.

## 7.8. Workpackage 8

<b>Workpackage Title:</b>	<b>Real world rollout</b>
<b>Partner Responsible:</b>	OUCS, SERS
<b>Other Partners Involved:</b>	Athens, MIMAS, OeSC
<b>Start Date:</b>	July 2004
<b>End Date:</b>	August 2004
<b>Objectives:</b>	To distribute successfully the certificates much more widely, to test and to document the issues arising. Also to examine revocation and recovery issues.
<b>Brief Description of Work:</b>	A more extensive set of users will receive certificates. Users to include IT support staff in devolved roles throughout the University as well as selected end users of many types and roles. Trialling of (or all-hands focus on) revocation and recovery/re-issuing mechanisms. OeSC to provide advice during troubleshooting. Athens and MIMAS to assist with or advise in evaluating users' experiences in accessing remote services.
<b>Quality Assurance and Review:</b>	During and following the rollout, the opinions and input from end users and stakeholders will be sought. These form a major part of workpackage eleven and will be disseminated widely. Feedback is therefore of paramount use to the evaluation process.
<b>Outputs including reports:</b>	Knowledge of issues and problems arising from the 'real world' rollout. Fixing of minor problems. Active input to the evaluation process from technical members of the Project Team, especially regarding distribution, revocation and recovery. Successful exit strategy.

### 7.8.1. Task Descriptions

Task	Title	Partners	Description
8.1	Distribution of certificates to devolved IT support staff	OeSC	Registration process and distribution to selected users.
8.2	Troubleshooting of distribution issues	OeSC	
8.3	Distribution of certificates to selected remote services users	OeSC	

<b>Task</b>	<b>Title</b>	<b>Partners</b>	<b>Description</b>
8.4	Input to evaluation	OeSC, MIMAS, Athens	c.f. workpackage 11, but development time needed.
8.5	Revocation trial		Testing of revocation mechanisms with real users.
8.6	Focus on recovery issues	OeSC	Focus on procedures regarding if a user has compromised his/her certificate – i.e. re-issuing. Also forgotten password/recovery issues.
8.7	Total revocation and exit strategy	OeSC, MIMAS, Athens	All partners need to be reassured that the certificate trial is over and access will not be performed via this mechanism in the near future.

## 7.9. Workpackage 9

**Workpackage Title:** Certificate Policy Statement  
**Partner Responsible:** OUCS, SERS  
**Other Partners Involved:** MIMAS, Athens, OeSC  
**Start Date:** January 2004  
**End Date:** August 2004

**Objectives:** To develop and publish a detailed Certificate Policy Statement (CPS) in accordance with the Internet Engineering Task Force Public Key Infrastructure X.509 Certificate Policy and Certification Practice Statement Framework.

**Brief Description of Work:** An early draft of the statement will be produced and consultation carried out within the partners and more widely as to trust issues. The final version of the CPS will be produced after rollout, after all consultation has ended and after any practical amendments have to be made. **Note** that there may be some dependency on workpackage ten with respect to Legal Services. OeSC, Athens and MIMAS to play an advisory role.

**Quality Assurance and Review:** Stakeholders and partners will review the Certificate Policy Statement. Furthermore, an 'external' reviewer should review the statement for trustworthiness.

**Outputs including reports:** A final Certificate Policy Statement along with a detailed evaluation of issues, assumptions and institutional decision-making processes.

### 7.9.1. Task Descriptions

Task	Title	Partners	Description
9.1	First CPS draft	OeSC, MIMAS, Athens	Production of first draft after consultation with stakeholders and partners.
9.2	Publicity of CPS and associated documents		The CPS forms the backbone of the trusted PKI and it is important to publicise and criticise this document.
9.3	Seek 'external' reviewer for CPS	OeSC, MIMAS, Athens	An external body, agency or knowledgeable individual should be sought for eventual review of trust aspects of the CPS.



---

<b>Task</b>	<b>Title</b>	<b>Partners</b>	<b>Description</b>
9.4	Process criticisms and comments regarding CPS		
9.5	CPS considered by external reviewer		This consultation exercise can serve to extend the pilot project much wider. The external reviewer can judge whether an external body would be likely to trust Oxford University issued certificates.
9.6	Final draft of CPS and associated documentation	OeSC, MIMAS, Athens	

## 7.10. Workpackage 10

<b>Workpackage Title:</b>	<b>Focus on legal and administrative issues</b>
<b>Partner Responsible:</b>	OUCS, SERS
<b>Other Partners Involved:</b>	OeSC
<b>Start Date:</b>	June 2003
<b>End Date:</b>	December 2004
<b>Objectives:</b>	To elicit input from Oxford University Legal Services regarding issuing and revoking certificates as well as running the PKI. This may affect the final Certificate Policy Statement (CPS). Also to investigate the administration issues of managing a registration authority and certificate authority and revocation list.
<b>Brief Description of Work:</b>	Research of legal and administration issues. Presentation to Legal Services and processing of the feedback from both sources. OeSC to play an advisory role.
<b>Quality Assurance and Review:</b>	The Project Board will monitor and inform the work of the Project Team throughout this workpackage. Quality of feedback should be enhanced through an approach of approaching responders early in the project for feedback/consultation to be sought later in the timeline.
<b>Outputs including reports:</b>	Documented analysis of the legal issues. Reliable CPS. Documented analysis of administration issues.

### 7.10.1. Task Descriptions

Task	Title	Partners	Description
10.1	Research legal issues	OeSC	Project Team look into legal issues for presentation to Legal Services
10.2	Research admin. issues	OeSC	Research into human administration issues of managing registration authority, certification authority and revocation lists. <b>Note</b> that much of this work is done within workpackage three, but that a separate focus is needed for evaluative purposes.
10.3	Preliminary report on legal issues		Findings from the above research in a form readable by the Legal Services team.
10.4	Early presentation to Legal Services		Presentation of the above findings and stimulation of the consultation exercise. Carried out early in the project so that good feedback can be sought later.

---

<b>Task</b>	<b>Title</b>	<b>Partners</b>	<b>Description</b>
10.5	Detailed feedback from Legal Services		To be received later in the project.
10.6	Final report on legal and legal-related matters		This report may be combined with any evaluative report on the administration infrastructure.
10.7	Final report on administrative issues		This and the above report may be combined if deemed convenient and relevant to do so. The report should cover background issues but focus on the learning experience from this project.

## 7.11. Workpackage 11

**Workpackage Title:** Evaluation and dissemination  
**Partner Responsible:** OUCS, SERS  
**Other Partners Involved:** Athens, MIMAS, OeSC  
**Start Date:** June 2003  
**End Date:** December 2004

**Objectives:**

- a) To produce evaluations, both technical and user-oriented of a wide variety of aspects surrounding the implementation of PKI at higher education establishments within the UK. The evaluations will be collated into a final report.
- b) To disseminate a series of reports – via web pages, email lists and at real ‘events’ – of the progress of the project, documenting successes and failures and points of difficulty. These and the final report should be disseminated in a form that will be useful to others considering PKI within the higher and further education sector in the UK.

**Brief Description of Work:** Formative evaluation of decisions made during the project as well as summative evaluations of some of the decision-making processes and the experiences of end users etc. Also effective dissemination of these findings. See section 3.2 for more details. OeSC, Athens and MIMAS to play an advisory role.

**Quality Assurance and Review:** The Project Board will monitor and inform the work of the Project Team throughout this workpackage. Discussions for templates for reports and overall content will be discussed with stakeholders as much as possible as will much of the published reports themselves.

**Outputs including reports:** Clear and effective reports documenting the project and its findings. Good quality dissemination and handling of feedback for further dissemination. (Most of the tasks in the table below will produce output as written reports, although more than one task may contribute to each report).

### 7.11.1. Task Descriptions

Task	Title	Partners	Description
11.1	Establish project web site		Establish the architecture and some content for the project web site

<b>Task</b>	<b>Title</b>	<b>Partners</b>	<b>Description</b>
11.2	Tracking architecture review		Track and document findings during the architecture review (workpackages 3 and 4).
11.3	Formulating evaluation mechanism for architecture decisions		Research and design scoring protocol (rubric) for key decision making processes. This system itself may form a critical part of the final documentation.
11.4	Track modelling decisions		Track decisions made using the scoring protocol as well as the more unforeseen or pragmatic decisions made.
11.5	Tracking Certificate Practice Statement decisions		Track decisions made during the drawing up of the CPS (may be closely allied with the modelling decisions).
11.6	Tracking development and testing	OeSC	Documenting aspects of the rollout. Problems encountered etc.
11.7	Tracking access to remote services	Athens, MIMAS	Athens and Zetoc – successes, failures, difficulties.
11.8	Designing summative evaluation for rollout phase	OeSC	Designing scoring mechanisms to evaluate the success of factors in the rollout phase. (Also to include feedback from admin. staff).
11.9	Real world rollout formative and summative evaluation	OeSC	Performing the summative evaluations and tracking the rollout. Evaluating access to local services and remote services.
	Evaluation of system architecture		Focus on the mechanics and associated issues regarding the system architecture.
11.10	Managing feedback and user group meetings		For formative and summative evaluation.
11.11	Evaluate input of legal services and University Administration		Performed via meetings and presentations (and, where possible, summative evaluation).
	Report on revocation and associated issues		Focus on revocation, recovery and other associated issues.
11.12	Report editing and work on consolidation and presentation		Editing of final reports and re-appraisal of presentations of previous reports

<b>Task</b>	<b>Title</b>	<b>Partners</b>	<b>Description</b>
11.13	Recommendations report	Athens, MIMAS, OeSC	Production of recommendations, following consultation with stakeholders and partners (equivalent to exit strategy for an actual rollout).
11.14	Dissemination (throughout this workpackage)		Dissemination to a variety of media (via web pages, email lists and at real 'events') throughout the workpackage. The final report must be disseminated in a form that will be useful to others considering PKI within the higher and further education sector in the UK.
11.15	Management of stakeholder meetings (throughout this workpackage)		Part of the evaluation and dissemination work will be to provide stakeholders and partners with pertinent information and to process their input.

## **8. Dissemination**

Dissemination is a major objective of this project and workpackage eleven (see page 28) deals with this matter explicitly. Some introductory and explanatory text also appears in sections 3.2 *Evaluation* (page 4) and 3.6 *Publication* (page 5).

## **9. Project Board and Stakeholder Group**

The makeup and role of these two groups are outlined in sections 5.3 (page 8) and 0 (page 9), respectively.

## **10. Quality Assurance and Evaluation**

The quality of each stage of the project should be assured through the constant supervision of the Project Board over the working of the Project Team (see page 8). Each major milestone will be documented in the form of reports that will be published immediately and stakeholders and partners will thus have the opportunity to question any findings. Feedback will be sought at most stages of the project as part of the general methodology and therefore quality should be maintained throughout. It is possible that some of the final output of the project may appear in peer-reviewed journals, but this is likely to be towards the end of the project.

As this project has evaluation as part of the overall aim, evaluation is explicitly considered as part of workpackage eleven and is considered fully on page 28.

### **10.1. Standards and interoperability**

Adherence to standards to ensure future interoperability is important to the project. However, the prime focus of this project is to complete a pilot rollout of digital certificates and to document the associated issues. If the desire for interoperability would mean that too much time-consuming prime development were required, it is possible that we may have to adopt existing non-standard solutions and products. This experience will, however, feed in heavily to the evaluation procedures and final documentation and will, thus, be of use to a future rollout.

### **10.2. Usability**

Usability issues, including for those users with disabilities, will form an integral part of the evaluation procedures.

### **10.3. Sustainability**

The long-term sustainability of the digital certificates beyond the end of the project is not a prime focus as it is intended that all certificates be revoked at the end of the technical stages. However, Oxford University Computing Services, Oxford e-Science Centre and several other bodies within the University have a great interest in authentication and authorisation. There is already some expertise in these areas and the expectation is that this expertise will grow and be reinforced by the DCOCE project. The future use of digital certificates in some manner by the University will be greatly encouraged by the successful conclusion of the project.

## 11. Risk Assessment

### 11.1. Introduction

The following risk assessment focuses on each workpackage in turn. The risks at each stage and around each milestone are explored. Risks are assessed primarily for their impact upon the budget, timing and the scope of the project and a rough estimate is made of the likelihood and severity of each threat. These are scored on a basis of 1-3 (1=relatively unlikely or non-severe; 3=more likely or very severe if the theoretical problem arises). Any theoretical issue with a risk product of greater than six is explored in greater depth at this stage.

### 11.2. Stakeholder group

Possible risk	Likelihood	Severity	Risk factor (LxS)
Non-availability or non-co-operation of key elements of stakeholder group.	1	2	2
Emergent conflict of interest between elements of stakeholder group.	2	2	4
Members of stakeholder group change (e.g. due to work pressures, change of roles) during project.	3	1	3
Difficulty in scheduling meetings. <b>Risk:</b> Time. <b>Mitigation:</b> Schedule all future meetings at first stakeholder meeting. Amend this schedule when necessary.	3	2	<b>6</b>

### 11.3. Modelling of administration and technical architectures

Possible risk	Likelihood	Severity	Risk factor (LxS)
Chosen project for review is unavailable or cannot be scheduled near the start of this project. <b>Risk:</b> Time (possibly scope, although unlikely). <b>Mitigation:</b> Contact all candidate projects as soon as possible and schedule meetings early. Hold a shortlist of more than four candidate projects for review.	2	3	<b>6</b>
Project system programmer unavailable for part of the review process.	2	2	4
Some reviews take more time than anticipated	2	2	4
Expertise required in modelling beyond the experience of Project Team. <b>Risk:</b> Scope, possibly time. <b>Mitigation:</b> Already considered. Involvement of several members of OUCS staff is expected on a consultancy and/or occasional basis.	3	2	<b>6</b>
Stakeholders reject administration and/or technical model(s).	1	3	3



#### 11.4. Development and initial implementation

Possible risk	Likelihood	Severity	Risk factor (LxS)
Information published during development that criticises or finds loophole in security of the chosen methodology.	1	3	3
Unforeseen hardware problem	2	2	4
Unforeseen software problem	2	2	4
Unforeseen administration or user understanding problem.	2	1	2
Underestimate of time taken to develop or implement chosen infrastructure	2	3	6
<b>Risk:</b> Time.			
<b>Mitigation:</b> Encourage involvement of other OUCS staff during this period. If a problem occurs, there is therefore a high possibility of assistance being found from outside the immediate Project Team.			
Unforeseen technical problem.	3	2	6
<b>Risk:</b> Time, possibly scope and budget in worst-case.			
<b>Mitigation:</b> Already mitigated-for by generous allocation of time. Very likely that these 'problems' will add to the value of the project.			

#### 11.5. Athens and Zetoc integration

Possible risk	Likelihood	Severity	Risk factor (LxS)
Unforeseen technical problem.	3	2	6
<b>Risk:</b> Time, possibly scope and budget in worst-case.			
<b>Mitigation:</b> Already mitigated-for by generous allocation of time. Very likely that these 'problems' will add to the value of the project.			

#### 11.6. Real world rollout, troubleshooting and feedback

Possible risk	Likelihood	Severity	Risk factor (LxS)
Unforeseen technical problem.	3	2	6
<b>Risk:</b> Time, possibly scope and budget in worst-case.			
<b>Mitigation:</b> Already mitigated-for by generous allocation of time. Very likely that these 'problems' will add to the value of the project.			
Feedback difficult to recover.	1	3	3

## 11.7. General

Possible risk	Likelihood	Severity	Risk factor (LxS)
Loss of member of Project Team.	1	2	2
Loss of member of Project Board.	2	2	4
Lack (or loss) of co-operation from partner (Athens, MIMAS, OeSC, SERS, Oxford legal).	1	3	3
Inability to recruit a member of the Project Team (in good time).	3	3	<b>9</b>
<b>Risk:</b> Time.			
<b>Mitigation:</b> Informal involvement of many at OUCS and SERS. Internal recruitment and secondment options to be fully investigated as well as the possibility of technical consultancy.			
Under-spend of budget due to delays in recruitment, unforeseen staff movement etc.	2	2	4

## 12. Acronyms and abbreviations

Abbreviations used throughout this document are summarised below.

Athens	<p>Service provider to higher education and health organisations for access to many web-based (and a few non-web based) information services, searchable databases etc. Users obtain an Athens username and password and can then access the multiple services.</p> <p>Athens, a service of EduServ, was designed and developed in 1994. The service has been in active use since 1996 in the UK Higher Education community, providing access to many centrally-funded web-based services. Athens is the de-facto standard in UK Higher Education, Further Education and Research Councils for Access Management and was awarded a JISC contract in August 2000, for the provision of Authentication Services to these communities.</p> <p><a href="http://www.athensams.net">www.athensams.net</a></p>
AthensDA	<p>An Access Management System for controlling access to web-based subscription services. Athens has developed the technology to accept X.509 certificates as an alternative means of authentication but AthensDA will usually be configured to return the user to their home institution and then for the institution to pass them back to Athens with an authentication token (plus a component called a 'permission set' which is concerned with authorisation).</p> <p><a href="http://www.athensams.net/development/athensssoandda.html#6">http://www.athensams.net/development/athensssoandda.html#6</a></p>
DCOCE	<p>Digital Certificate Operation in a Complex Environment (the name of this project).</p> <p><a href="http://www.oucs.ox.ac.uk/dcoce">www.oucs.ox.ac.uk/dcoce</a></p>
EduServ	<p>EduServ is a not-for profit company and UK-registered charity providing leading edge ICT services to education and the public sector.</p> <p>Hosts Athens, CHEST (Combined Higher Education Software Team - software and online licences), NISS (National Information Services and Systems). Based in Bath.</p> <p><a href="http://www.eduserv.org.uk">www.eduserv.org.uk</a></p>
e-Science	<p>The term 'e-Science' refers to the large scale science increasingly carried out through distributed global collaborations enabled by the Internet. Typically, a feature of such collaborative scientific enterprises is that they will require access to very large data collections, very large scale computing resources and high performance visualisation back to the individual user scientists.</p> <p>The UK e-Science Programme is a cross-funding-council activity supported by the Department of Trade and Industry. Much of the work of the programme is focussed on using and developing the <i>e-Science Grid</i>.</p> <p><a href="http://www.nesc.ac.uk">www.nesc.ac.uk</a></p>

e-Science Grid	<p>The Grid is the name that describes the next significant development in Internet computing. A term first coined in the mid '90s to describe a vision for a distributed computing infrastructure for advanced science projects, the Grid was first properly explained by Ian Foster and Carl Kesselman in their book <i>The Grid: Blueprint for a New Computing Infrastructure</i> (Morgan Kaufmann, 1999; ISBN 1-55860-475-8). In this vision, the Grid will be to all computational resources what the World Wide Web presently is to documents containing information. Grid users will have at their disposal distributed high performance computers able to access and process terabytes of data stored in global databases, plus the appropriate tools to control these resources.</p> <p>The e-Science Grid is a grid devoted to e-Science projects.</p> <p><a href="http://www.escience-grid.org.uk">www.escience-grid.org.uk</a></p>
Globus Grid Security Infrastructure	<p>The Globus Grid Security Infrastructure (<b>GSI</b>) is based on public key encryption, <i>X.509 certificates</i>, and the Secure Sockets Layer (SSL) communication protocol. Extensions to these standards have been added for single sign-on and delegation. The Globus Toolkit's implementation of the GSI adheres to the Generic Security Service API (GSS-API), which is a standard API for security systems promoted by the Internet Engineering Task Force (IETF).</p> <p><a href="http://www.globus.org/security">www.globus.org/security</a></p>
JISC	<p>Joint Information Systems Committee.</p> <p><a href="http://www.jisc.ac.uk">www.jisc.ac.uk</a></p>
MIMAS	<p>Manchester Information and Associated Services.</p> <p><a href="http://www.mimas.ac.uk/">http://www.mimas.ac.uk/</a></p>
OeSC	<p>Oxford e-Science Centre.</p> <p><a href="http://e-science.ox.ac.uk/">http://e-science.ox.ac.uk/</a></p>
OUCS	<p>Oxford University Computing Services.</p> <p><a href="http://www.oucs.ox.ac.uk/">http://www.oucs.ox.ac.uk/</a></p>
OULS	<p>Oxford University Library Services.</p> <p><a href="http://www.lib.ox.ac.uk/">http://www.lib.ox.ac.uk/</a></p>
PKI	<p>Public Key Infrastructure</p> <p>(<a href="http://www.ietf.org/html.charters/pkix-charter.html">http://www.ietf.org/html.charters/pkix-charter.html</a>) and e.g. <a href="http://www-itg.lbl.gov/Akenti/docs/secPrimer/index.htm">http://www-itg.lbl.gov/Akenti/docs/secPrimer/index.htm</a>)</p>
Revocation	<p>Causing a digital certificate to be invalid. Revocation means that the certificate may have been valid, but is valid no longer and authentication should not go ahead. Revocation occurs when a user has compromised his/her certificate and needs a new one or (for example) when they are no longer a student or member of staff within an institution. This process is usually managed via a certificate revocation list (CRL).</p>
SERS	<p>Systems and Electronic Resources at Oxford University Library Services.</p> <p><a href="http://www.sers.ox.ac.uk/">http://www.sers.ox.ac.uk/</a></p>

X.509 certificates	<p>X.509 is an ITU-T recommendation detailing aspects of digital certificates and PKI. X.509 digital certificates are certificates that conform to this specification. X.509 is the most widely used 'standard' for digital certificates, but remains a 'recommendation' and therefore such certificates and <i>PKIs</i> have been implemented in different ways.</p> <p>(ITU-T is the International Telecommunication Union Telecommunication Standardization Sector. A standards body).</p> <p><a href="http://www.ietf.org/rfc/rfc2459.txt">http://www.ietf.org/rfc/rfc2459.txt</a></p>
Z39.50	<p>In basic terms, Z39.50 is a network protocol which allows searching of (usually remote) heterogeneous databases and retrieval of data, via one user interface. It is most often used for retrieving bibliographic records, although there are also some non-bibliographic implementations.</p> <p><a href="http://www.ukoln.ac.uk/dlis/z3950">http://www.ukoln.ac.uk/dlis/z3950</a></p>
Zetoc	<p>Z39.50-compliant access to the British Library's Electronic Table of Contents (ETOC). Managed by <i>MIMAS</i>.</p> <p><a href="http://zetoc.mimas.ac.uk/">http://zetoc.mimas.ac.uk/</a></p>