

Digital Certificate Operation in a Complex Environment
*A project within the Joint Information Systems Committee's Authentication,
Authorisation and Accounting middleware programme*

Biannual report – months 7-12

Project abbreviation	DCOCE	
Project Title	Digital Certificate Operation in a Complex Environment	
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	
Lead Institution	University of Oxford (Computing Services; Library Services; e-Science Centre)	
Duration of award	1 January 2003 to 31 December 2004	Total amount (JISC): £245,506
Period of report	1 July 2003 to 31 December 2003	Total co-funding: £382,182
Key abbreviations	Manchester Information and Associated Services (MIMAS), Oxford e-Science Centre (OeSC), Oxford University Computing Services (OUCS), Systems and Electronic Resources (SERS) at Oxford University Library Services.	

1. Confirmation Statement

I confirm that the project development is being conducted under the terms agreed in the initial contract with JISC.

2. Aims, Objectives and Methodology

There have been no changes to the original aims, objectives or methodology as detailed in the project plan.

3. Highlights, Outcomes and Important Findings from project

The project web site (www.dcoce.ox.ac.uk) was launched and has been updated with background to PKI and ideas for architectures. It has been generally well received by the target audience. The stakeholders group has been strengthened and consolidated. On 3 December, the project held a stakeholders/consultation day where attendees heard an introduction to PKI, digital certificates and the project. They later gave much verbal feedback and completed questionnaires that will help to design the architecture and the evaluation processes for the project.

There were twenty-two attendees, mostly from the Departments and Colleges of Oxford University. Other interested individuals and partners played an active part, including David Orrell of Athens and

an interested party from Bristol University. The day was a great success from the point of view of the project team and the feedback is currently being analysed.

4. Changes to original award

There have been no major changes to the original project plan. The consultation day for stakeholders and other interested parties was held much later than anticipated, but there were few critical dependencies resting on this milestone. As anticipated in the last report, finding good 'study sites' for the background review for workpackages 3 and 4 has been far more difficult than originally assumed, but we do not anticipate this causing any major delays. The greatest threat to deadlines still remains as the delay in recruiting members of the project team. Currently, this has had little medium term effect and the team is now at full complement, but it has caused a slight delay to workpackage 2 (stakeholder group) and the 'review' phases in workpackages 3 and 4 (architecture modelling). We hope that we will be able to make up time in the modelling phase, as this has already started, and by actively inviting secondments to the project. Nevertheless there remains a potential risk to the timely delivery of future workpackages due to delays in recruiting experienced project staff. We are currently investigating the paid secondment of internal staff or consultancy to complete the groundwork for the later workpackages.

5. Project staff

The project comprises the following staff:

- Mark Norman (project manager, 1.0 FTE)
- Alun Edwards (OUCS-based evaluator 0.5 FTE)
- Christian Fernau (systems developer, 1.0 FTE)
- Johanneke Sytsema (SERS-based evaluator 0.5 FTE)

Christian began work on the project on 4 August 2003, Johanneke began work with us on 11 November 2003 and Alun Edwards moved from 0.2 FTE to 0.5 FTE on 1 November 2003.

We did make use of a very short (part-time) secondment to us from within OUCS in August and September 2003. This was useful for the technical side of the project, and we are considering using this option more during the next few months.

6. Involvement with Programme

None in this six months.

7. Publications and Publicity

The project web site (www.dcoce.ox.ac.uk) was launched and expanded during the last six months. Much background and documentation is already available from the site. We also have an extensive PKI/Security glossary that we wish to maintain. A document concerning possibilities for development of the project was produced during October 2003 and appears at <http://www.dcoce.ox.ac.uk/ideas/>. This was publicised on the mailing lists and at the meeting outlined below.

Some 'publicity' activities were combined with the DCOCE stakeholders/consultation event of 3 December. Architecture ideas and prompts for discussion were circulated on our DCOCE-ADVISORY and DCOCE-DISC JISMAIL mailing lists. We are currently working on an extended evaluation report, which we will publish on our web site and advertise to the lists soon.

7.1. Presentations relating to the project:

- 2 December 2003, Christian Fernau, Cryptographic File Systems, Oxford University IT Support Staff Services seminar (see <http://www.dcoce.ox.ac.uk/docs/CryptoFS2Dec03.pdf>).
- 3 December 2003, Mark Norman. Public Key Infrastructure and Authentication (see <http://www.dcoce.ox.ac.uk/docs/PKIntroTalkToStakeholders3Dec03.ppt>).
- 3 December 2003, Alun Edwards and Mark Norman. Consultation/Stakeholders Meeting main presentation (see http://www.dcoce.ox.ac.uk/docs/consultation_stakeholders3Dec03.ppt).
- 5 December 2003, Mark Norman. DCOCE Report from Consultation/Stakeholders Meeting: presentation to OeSc Security Work Group (see <http://www.dcoce.ox.ac.uk/docs/ReportToOeSCSecurityWkgp5Dec03.ppt>).

7.2. Calling of and attendance at meetings

- Mark and Christian attended the e-Science workshop *Practical security for e-Science projects* at the National e-Science Centre on 24-25 November 2003.
- Mark and Christian met with Sandy Shaw and other members of the Technologies for Information Environment Security (TIES) project at the Edinburgh University Data Library on 25 November 2003 (TIES produced its final report in September of this year and this has proved very useful to DCOCE).
- Mark and Christian have also joined the Oxford e-Science Security Work group (established 14 November 2003).
- Mark and Christian attended the Open Source Software Watch Inaugural Conference on 11 December 2003, and Mark chaired a workshop session.

8. Engagement with Potential Outcomes Users

Much work has been carried out in consulting users and stakeholders (see sections 3 and 7 above). Some output from these consultations has been included on the project web site (<http://www.dcoce.ox.ac.uk>) already. Further, more detailed output will be included soon.

9. Detailed Progress and Future Plans

9.1. Workpackage 2

Workpackage Title:	Stakeholder group
Partner Responsible:	OUCS, SERS
Other Partners Involved:	MIMAS, Athens, OeSC
Start Date:	March 2003
End Date:	June 2003

Progress: At the stakeholder/consultation meeting on 3 December, much was gleaned that will feed directly into the modelling of the architecture. Further, these 'issues' will eventually contribute to the criteria with which the project will be evaluated.

9.2. Workpackages 3 and 4

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

Progress and future plans: We looked into the LUCIE certificate issuing engine and have found out about other implementations via a questionnaire and other analyses.

Modelling is now underway.

9.3. Workpackage 5

Workpackage Title:	Development and initial implementation
Partner Responsible:	OUCS, SERS
Other Partners Involved:	OeSC
Start Date:	February 2004
End Date:	May 2004
Objectives:	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.

10. Financial summary

[Finances removed in this public version.]

Mark Norman. 30 January 2004