Experiences of Using a Public Key Infrastructure for the Preparation of Examination Papers

By David W Chadwick, Rana Tassabehji and Andrew Young, IT Institute, University of Salford

Abstract

A project that piloted the secure electronic preparation of examination papers ran during the first semester of the academic year 1998-99 at the University of Salford. The examination papers were transferred between the participants (lecturers, administrators and external examiners) using secure electronic mail. Security was provided by a managed public key infrastructure. Users were profiled and interviewed in order to determine the likely success of further roll out within the institution, as well as the user friendliness of the existing paper based and proposed electronic systems. The project found that, while the technology worked for some participants, others had severe problems with installation of the software and failed to grasp key concepts. There appear to be formidable obstacles to extending the system to cover the whole university, including compatibility of equipment and the reliability of the network infrastructure.

1. Introduction

Universities need to find more efficient ways of working, because of the limited resources that are available and the continual changes that are taking place such as:

- shortening time scales for examinations due to semesterisation,
- broadening the number of degree courses, and options within degree courses, to widen their appeal,
- increases in student numbers.

One area that is resource intensive as well as time critical, is the collation, preparation and distribution of examination papers. Very little contingency time is available during the examination preparation period, with the consequence that staff are already taking short cuts which could potentially compromise the security and integrity of the examination process. Example from our university include:

- e-mailing examination questions as plain text,
- faxing examination papers to remote sites.

When short cuts are not taken, the alternatives are expensive and time consuming. For example it costs up to £80 and takes up to 3 days to courier examination papers overseas. The University of Salford regularly sends its examination papers to such places as Greece, Spain, Hong Kong and Malaysia. Many universities have joint degree courses or external degree courses with other institutions, which all need to widely distribute their examination papers to overseas students during re-sits. If universities were able to use secure electronic mechanisms for the preparation, validation and distribution of examination scripts, this could save them a significant amount of time, and could be more secure than current mechanisms. The validity of this hypothesis was tested at the University of Salford during the first semester of the academic year 1998/99, with a pilot project to securely exchange electronic examination papers during their preparation and quality checking.

2. Aims and Objectives

The project was undertaken primarily to determine if the time and costs of the examination administration process could be reduced by using the existing e-mail system along with the University's intranet and the Internet. Examination papers could then be exchanged electronically, between the internal and external stakeholders (exam originators, internal quality assessors, external examiners and internal exam administrators). As the preparation of examination papers is a business critical process to a university, security must be paramount. Consequently, the electronic examination questions and model answers must be secured very strongly so as to ensure both their confidentiality and authenticity.

However, change management is equally as important as the technological aspects of the project. Therefore the participants in the pilot should be profiled, in order to obtain a description of their relevant user attributes. This profiling should provide valuable information in determining the different types and categories of users, so as to indicate whether and how the full-scale introduction of such a system in the future is likely to be a success or a failure. Finally the "user friendliness" of both the current paper based and the new electronic systems should be ascertained via user interviews in order to see if there are any areas where future improvements may be necessary.

3. Methodology

The population of examination papers was categorised and a controlled random selection was made. Control had to be introduced, as some papers were not suitable for transfer electronically. A variety of methodologies were used for data collection from the users, in order to capture relevant information at different stages in the pilot. In depth interviews were carried out with the department heads and administration staff at the start of the project. Data was collected from pilot participants at the start and end of the project using written questionnaires. Semi-structured observations were used during the training sessions, taking particular note of a participant's behaviour, actions and comments.

4. Sample Selection

Two academic departments were selected to participate in the pilot, along with the Examinations office of the Registrars Department. The short time scales available to us meant that we required volunteer departments with a reasonable percentage of examination papers already prepared in electronic form, so the departments were partially self selecting. The academic departments were the Computer and Mathematical Sciences department (CMS), and the Information Technology Institute (ITI). University departments are often quite autonomous in the way they operate and usually have their own cultures and norms. It would therefore be instructive to see what differences were detected between two departments implementing the same electronic process. The CMS department was selected because it is one of the oldest established departments in the University and has a past history of being late in its submission of examination papers to the examination office. The ITI was selected because it is one of the newest departments in the University, is technology oriented, organises its own printing and distribution of examination papers and thus has no problems with late submission and production of examination papers (from the perspective of the Examinations office). By taking these two extreme cases, participant attributes and pilot results may be expected to be more pronounced.

Note that both participating departments are heavy users of computers on a day-to-day basis. Further study is clearly needed to assess whether the same results are obtained from departments that use computers less frequently. If the project succeeds in a computer literate department, it may fail in a computer-naïve department (for example, if there is some underlying technical competence assumed by the software). Equally, if it fails in a computer literate department, it could succeed in a computer-naïve department (for example, it is possible that novice staff are more willing to listen to and follow strict instructions whereas experts dabble and take short-cuts).

A random sample of examination papers from the two departments was needed for the pilot. The total population, i.e. all the examinations usually set for semester one by each department, numbered 54 examination papers for CMS and 17 for the ITI. The examination papers were classified in order to:

- ensure that the random sample selected is representative of the population as a whole, and
- identify the range of situational factors likely to affect the successful deployment of an electronically based examination procedure.

Information used to gather the data for classification was obtained directly from conversations with heads of department, examination officers, and from past examination papers, model answers, and current examination schedules. Based on the classification, 6 examination papers were selected from the total population for each department.

4.1. Exam Paper Classification

The table below describes the classification criteria for the population of examination papers.

Classification Attribute	Description
Subject	A breakdown of the subject categories e.g. Information Technology/Business/Mathematics/Software Development
No. of people involved with setting questions	This will give an indication of the level of co-operation/standardisation necessary to implement a system
How long has the course been running	This will give an indication of the relative "newness" of the course and the exam preparation techniques
Name of Internal Q/A	To ensure all participants are included but not duplicated
Name of External Examiner	To include her/him in the pilot
Name of Examination author	To ensure participants are not duplicated
How long has the current lecturer been running the course	This will give an indication of the propensity for the lecturer to change exam preparation techniques
Length of exam	In terms of duration and also in terms of number of questions/number of pages
Content of the exam and type	To assess the format of the examination paper e.g. Text, or Text & graphics, or Graphics only.

	Problem solving/essay/multi-choice
Format received (questions and answers)	Hand-written or electronic or both (for both Q&A) Note. Only MS Word or Wordperfect format were acceptable for the pilot
Date of the examination	For administrative purposes

As this was a live pilot project in a critical area with tight deadlines, certain selection criteria had to be pre-determined. These were as follows:

- All examinations had to be scheduled to run in January 1999 (because some modules are optional, not all examinations actually run each year).
- As encryption is only suitable for electronic data, hand written questions and/or diagrams had to be excluded.
- Mathematical examinations that were mainly a series of mathematical symbols and formulae, in either questions or solutions, constituting from our viewpoint non-electronic graphics and text, also had to be excluded from the sample. (The main reason for this is that this data is very hard to exchange electronically between different computer and word processing systems, due to the wide range of systems being used.)

In a future larger-scale project, it would be necessary to consider how the technology could be extended to cater for all types of examination question. A simple solution would be to use an optical scanner to convert such documents to a standard format for compressed graphics (TIFF or JPEG formats would be suitable, though JPEG format is better suited to images than text). The security software used must be able to exchange graphics files as well as word processor documents. The external examiner can return comments as a separate text file or can annotate the graphics file using suitable software.

Note that this would require the provision of extra equipment (scanners) and the training of staff. The resources for this were not available in the current project, and so such questions had to be excluded.

4.2. The Population

The population from which the sample was drawn was analysed in order to understand the degree to which the sample was representative of the overall population. This will then indicate the likely probability of future success in extending the implementation both department and university wide.

In CMS over 50% of the population had to be excluded from the sample because some or all of the questions and solutions were prepared by hand or were mathematical symbols and formulae. 75% of all courses have been running for more than five years, with only 8% being courses running for one year or less. Within the modules, for the maths courses, all have been running for more than 5 years and over a half of the lecturers have been running the courses for more than 3 years. With the technology oriented modules the courses have been running for relatively less time and a higher proportion have been running for 3 years or less. Similarly, the lecturers tend to have been running the courses for a shorter period of time, usually three years or less.

In the ITI, none of the population needed to be excluded from the sample. Nearly all the courses had been running for more than five years. However, the majority of lecturers (64%) have been running the course for two years or less.

Tables 1 and 2 summarise the respective populations of exam papers.

4.3. The Sample

From CMS the sample was selected only from the Information Systems and Computer Science subject areas. The Maths and Statistics related papers were excluded because the papers and answers are either prepared by hand, and therefore not in an electronic format, or the mathematical software used in some cases was extremely specialised which would have excluded the administrator, the examinations office and some external examiners from receiving the electronic papers. Six papers were selected randomly. Two of the papers for the courses selected had been running for more than 5 years. Two had been running for 3 years, 1 for 2 years and 1 course was new. One of the lecturers had been running the course for 5 years or more, 3 had been running the course for 3 years, 1 had been running the course for 2 years and 1 lecturer was new to the courses. This is shown in Table 1. However, of those papers selected, one was prepared manually and not electronically and thus subsequently had to be discounted.

All 6 papers from the IT Institute had been running for more than 5 years. Two of the lecturers had been running the courses for 5 years or more, 2 had been running the course for 2 years and 2 lecturers were new to the courses. All examination papers were prepared electronically. This is shown in Table 2.

Computer and Mathematical Sciences Department				
Subject Category	**No. of Papers**	**Length in Years (of Courses)**	**Length in Years (of Lecturer running the courses)**	**Comments**
Computer Science	12 (22%)	83% >5 years 8.5% 3 years 8.5% 2 years	58% > 5 years 17% 3 years 17% 2 years 17% New	
Information Systems	11 (20½ %)	27% > 5 years 27% 3 years 27% 2 years 19% New	27% > 5 years 27% 3 years 27% 2 years 19% New	
Maths (I)	11(20½ %)	100% > 5 years	57% >3 years 21% 2 years 7% 1 year 14% New	*Graphics, text, formulae also solutions are hand written*
Maths (II)	14 (26%)	100% >5 years	100% > 3 years	*Graphics, text and formulae also solutions are hand written*
OR & Statistics	6 (11%)	63% >5 years 33% New	63% >5 years 33% New	*Graphics, text and formulae also solutions are hand written*
Total Population	**54**	**78% >5years** **7% 3 years** **7% 2 years** **4% 1 year** **4% New**	**28% >5 years** **42% 3 years** **13% 2 years** **6% 1 year** **11% New**	
The Sample	**6**	**33.33% >5years** **33.33% 3 years** **16.67% 2 years** **0% 1 year** **16.67% New**	**16.67% >5 years** **50% 3 years** **16.67% 2 years** **0% 1 year** **16.67% New**	*4 Information Systems, 2 Computer Science*

Table 1. Categorisation and Selection of CMS Examination Papers

Information Technology Institute			
Subject Category	**Number of Papers**	**Length in Years (of Courses)**	**Length in Years (of Lecturer running the courses)**
Information Technology	**The Population 17**	**94% >5 years** **6% New**	**12% >5 years** **24% 4 years** **23% 2 years** **41% New**
Information Technology	**The Sample 6**	**100% >5 years** **0% New**	**16.67% >5 years** **16.67% 4 years** **33.33% 2 years** **33.33% New**

Table 2. Categorisation and Selection of IT Institute Examination Papers

5. Participant Analysis

All participating staff in participating departments were analysed, but the external examiners were not, due to the geographical distances involved.

5.1. The ITI Participants

All six participants were lecturers at the IT Institute with postgraduate qualifications. Half were male and half were female. Four were aged between 35-44, with one below and one above. All the males had home Internet connections, whilst only one of the females did.

All the participants use computers both at work and at home on a daily basis. Computer usage is mainly concentrated in the area of presentations, e-mail, Internet, word processing and spreadsheets. The main software used is Microsoft's Office suite of products. This minimises any software incompatibility problems that might arise. Nearly half the participants also use computers for software engineering.

Included in the questionnaire were statements that measured specific thoughts, attitudes and cognitions that people have when working with computers and technology or when contemplating working with technology. These statements have been psychometrically tested as a measure for technophobia (Rosen & Weil, 1999). Male participants tended to be more technology oriented, be more comfortable and confident with technology and computer usage than the female participants. This was further supported by the notes taken by the researcher whilst observing the participants. Male participants were more confident in their approach to and use of the security software used in the pilot. This may also be due to the fact that all the male participants had knowledge of or were currently using some kind of security software[1]. This is not to say that male participants were more competent, but rather they had more knowledge and experience of the technology being piloted.

Turning now to thoughts about computers and technology. In this case, the difference between male and female participants' thoughts on computers and technology was less distinctive than their attitudes, however, there was a tendency for male participants to have higher scores in the thoughts on technology and computers rating, which indicates an enthusiasm for technology and computerisation. This is supported by the fact that the higher the participants scored on the thoughts to computers and technology, the more likely it was that they had an Internet link at home.

5.2. The CMS Participants

In this department there is a quality assessment system, whereby originators send their questions to the internal quality assessors before submitting them to the examination administrator. As such, some of the papers selected have dual role participants. Thus the total number of papers selected was six, but the number of participants was nine. However, of those papers selected, one was prepared manually and not electronically and thus two participants had to withdraw. For another paper selected, the originator refused to co-operate mid-pilot and thus had to be discounted. Thus the total sample of participants was six.

[1] One respondent was familiar with Pretty Good Privacy (PGP), another was familiar with PGP and Entrust software, while the third was aware of the theory of encryption.

All the CMS department participants are lecturers with post graduate qualifications. Five out of the six participants were male. Four were 25-34, one was in the age range 35-44, and one was above 44. All the participants use computers both at work and at home on a daily basis. Computer usage is mainly concentrated in the area of presentations, e-mail, Internet, word processing and spreadsheet. The main software used is Microsoft's Office Suite and Lotus Notes. This begins to raise the problem of software compatibility between and within departments. Some of the participants also use computers for software engineering.

As with the ITI participants, included in the questionnaire were statements about thoughts, attitudes and cognitions to computers and technology. Because of the limited number of female participants in the project, no real comparison could be based on sex and in fact the scoring profiles of the participants were similar with no real distinctions. Information in this case was limited because of the lack of participant completion and co-operation in the project. One respondent's score on thoughts about computers and technology was significantly lower than for the other participants, which indicates that the respondent is not amenable to computerisation. This was borne out when the same respondent felt that implementing the new electronic process would be full of problems and that there were no benefits whatsoever. This respondent was in the 45-54 age category.

5.3. Examinations Office Participants

The users were in the younger age group (18-35), had no higher education qualifications, and did not use a computer or Internet connection at home. However, the users' attitudes and thoughts to technology and computer usage indicated that they were supportive of technology but apprehensive about new technology. Notes taken during installation revealed that although the users initially required quite intense support they were extremely responsive to and enthusiastic after training.

5.4. Analysis

Based on the research results (of an admittedly small sample), there emerges a profile of 3 types of user, and a picture of how the implementation of an electronic examination preparation process might best proceed for each type.

The Supporter

The supporter is a user who is enthusiastic about technology and computer usage. This user believes that automation will enhance the quality of examination paper production within the organisation, by improving the speed, convenience, administration and costs of the paper based examination preparation process. This user will actively support the implementation of technology and computers to potentially automate paper based processes and needs no real support post implementation. This user will actively look for ways to counteract problems that may occur during the implementation, so that the project can proceed. The profile of this type of user is that they:

- are relatively new to teaching the course (5 years or less),
- are between the ages of 25-44, but tend to be concentrated more in the 25-34 age group,
- score relatively highly on thoughts and relatively low on attitudes to computers and technology. This indicates they are more confident users and less intimidated by and more comfortable with and enthusiastic about

technology. They have positive thoughts and cognitions towards working with computers and technology,
- have an Internet connection at home,
- have some knowledge or understanding of security and encryption software.

The Potential Supporter

The potential supporter is a user who is enthusiastic about technology and computer usage, but needs more support with the introduction of new software and automated processes. This user also believes that automation will enhance the quality of the examination production process and is prepared to support it actively once the process is understood and there is an infrastructure to facilitate and assist users when necessary. The profile of this type of user is that they tend to:

- be newer lecturers with newer courses of about 2 years or less,
- be between the ages of 25-44 and tend to be women,
- need practice, training, and more support from documentation,
- are less likely to have an Internet connection at home,
- score relatively similar scores on attitudes and thoughts to computers and technology. This suggests they are relatively confident and enthusiastic about technology, but need more support.

The Resister

The resister is a user who is relatively neutral about technology and computer usage and prefers the more established paper based processes. This user needs to be shown proof positive that automation is an improvement, before they are prepared to implement and use any new electronic system. They see new processes as an inconvenience, a source of unnecessary extra burden on their current workload. Any technical hiccups during implementation will only serve to reinforce their viewpoint, and will give them an ideal excuse to delay or abandon the new electronic process. The profile of this type of user is that they tend to:

- have been course tutors or administrators for (sometimes considerably) longer than 3 years,
- be over the age of 44,
- see no current problems or inadequacies in the existing method of examination preparation,
- have lower scores on thoughts and attitudes towards computers. This suggests they are not very enthusiastic about technology and computerisation, and
- have no Internet connection at home.

6. The Examination Preparation Process

6.1. The Paper Based Process in the ITI

The current method of examination paper preparation and submission is described below.

Stage 1 - The lecturers originate the examination papers which are sent (by internal mail or handed personally) to the administrator.

Stage 2 - The administrator collates all the examination papers and then arranges for the relevant printed examination papers to be sent by registered mail to the relevant external examiner for feedback.

Stage 3 - The external examiner(s) returns the examination papers (with feedback) by courier/registered mail. The administrator receives the

examination papers and distributes them (by internal mail or personally) to the relevant lecturers for any necessary revision.

Stage 4 - The final stage is where the revised final versions of the examination papers are sent to the administrator for printing and copying for the examination.

In the ITI, the whole process is co-ordinated by the administrator. The total co-ordination time taken up to stage 4 (but not including printing and distribution, or the time for the external examiner to perform the review) is typically of the order of 6-8 days. This co-ordination time is primarily the time taken for the transit of the various examination papers between the participants, and it does not include the processing time of the respective participants e.g. proof reading or making changes, since this is variable.

6.2. The Paper Based Process in CMS

The current method of examination paper preparation and submission is described below.

Stage 1 – The lecturers originate the examination papers that are sent (by internal mail or by handing personally) to the internal quality assessor.

Stage 2 – The internal quality assessor returns comments to the originator (by email or internal mail).

Stage 3 – The originator sends the amended paper to the administrator (by internal mail or by handing personally).

Stage 4 - The administrator collates all the examination papers and then arranges for the printed examination papers to be sent by registered mail to the relevant external examiner for feedback.

Stage 5 – The external examiners return feedback by email to the administrator, who forwards the email to the originator. The feedback consists of comments only, and does not include the questions (due to the lack of security of conventional email).

Stage 6 – The originator updates the examination questions and sends them (by internal mail or by handing personally) to the administrator.

Stage 7 - The final stage is where the administrator sends a collection of examination papers (by internal mail or by handing personally) to the Examinations office for copying ready for the examination. If the university deadline is missed, the originator must take the examination paper himself to the Examinations office.

In CMS the whole co-ordination process is typically of the order of 6-8 days. This co-ordination time is primarily the time taken for the transit of the various examination papers between the participants, and it does not include the processing time of the respective participants e.g. proof reading or making changes, since this is variable. Whilst the CMS process contains more stages than the ITI process, it already allows for comments and feedback to be sent by unsecured email, thereby significantly reducing the time for two of the stages.

6.3. The Secure Electronic Process

The Secure Electronic Process was designed to mirror the traditional paper based process in both departments. Transmission was to be by secure email rather than by either physical or unsecured email delivery. The decision to mirror the traditional process was taken partly because the electronic process was running in parallel with

the paper-based process, and partly because there was no remit to undertake process redesign at this stage.

7. The Public Key Infrastructure

A Public Key Infrastructure (PKI) (Chokhani, 1994; Csinger & Siau, 1998) based on X.509v3 certificates (ITU/T, 1997) had previously been installed at the university as part of two European Commission IV Framework RTD projects that the authors are involved in. The underlying technology that is used is asymmetric encryption. Asymmetric encryption relies on two keys that work together as a pair - an encryption key and a decryption key. If a user generates a pair of keys, and makes the encryption key public, anyone can encrypt a message for the user, but only the user can decrypt the message with the corresponding private key. This technique is indirectly[2] used to encrypt the examination papers in this project, so that only the intended recipient can read it. Conversely if the decryption key is made public, and the encryption key is kept private, then only the holder of the private key can encrypt a message but anyone with the public key may decrypt it and thereby be assured who the sender was. This is the basis for producing digital signatures and authenticating electronic messages.

In this pilot project all users have two key pairs. One key pair is used for confidentially encrypting an examination paper, and the other is used for digitally signing the same paper thereby authenticating the originator.

The software used was Entrust (Entrust, 1999) software from Canada, and the university had already obtained a Canadian export license granting it the use of US domestic strength (128 bit) encryption technology (this is classified as munitions by the US). Symmetric algorithms with this length or key are believed to be effectively unbreakable by brute force attack, and the algorithms in use, either TripleDES or CAST, do not have any known (i.e. published) crypt-analytical attacks.

The distribution of public keys is a major issue with this technology, since if an attacker can successfully substitute his public key for that of an external examiner or an academic, it would be possible to either get an examination paper encrypted for the attacker to read, or for the attacker to pretend to be an originator of an examination paper. For this reason, public keys must be distributed and managed in a secure way. A certification authority is a trusted third party that validates and issues digitally signed public keys (called public key certificates, or certificates) so that recipients can be assured that they have the correct public keys of users. The Entrust system allows the management and use of public key certificates to be tightly controlled, so as to rule out the possibility of masquerade. This is in direct contrast to the current, mainly free, Internet web based certification authorities that will issue certificates to anyone in a more or less uncontrolled manner.

The certification authority server and public key directory (Chadwick, 1996) server used in this project were housed in a securely fortified room in the University, and certificates were only issued to the participants. The servers are accessible over the university intranet, via a firewall, minimising the possibility of them being hacked. Participants must have the Entrust client software installed on their PCs so that they

[2] An examination paper is actually symmetrically encrypted using a one-off session key, as this is much quicker. The session key is then asymmetrically encrypted using the recipient's public encryption key.

may communicate with the servers in order to be securely certified and to download the certified public keys of other users. If the university intranet is unavailable then the system is to a greater or lesser extent unusable.

7.1. User Installation

An integral part of the secure electronic process is the installation procedure. A trainer installed the software for members of university staff, so that no skill or knowledge was required of them. Installation went smoothly apart from delays caused by network outages (see later). However, installation for the CMS departmental administrator was more difficult. Although the PKI client security software should be able to work on any Microsoft Windows, Macintosh and Unix platforms, in this instance there was an installation problem with the administrator's computer probably caused by a combination of Windows 3.1 and Lotus Notes. It was not possible to install Entrust on this machine and although it is highly likely that this configuration was the cause of the problem, it was not possible to determine the exact cause. To counteract this, a replacement computer was brought from the ITI and installed solely for use with the security software. However, it was not possible to connect this machine to the university network, since the CMS building has 10-base-2 network connectors whereas the ITI building uses 10-base-T connectors, and no spare converters were available at the time. The failure to successfully install the CMS administrator led to a critical failure of the project in the CMS department, and there was then no point installing the CMS external examiners.

One of the ITI external examiners works at a nearby NW university (<50 miles), the other in another country (Republic of Ireland). It was decided to post the installation discs to Ireland, and the external examiner duly installed the software without any problems, with guidance and training being given over the telephone. The examiner in the NW was visited by the trainer, but installation failed due to the PC being of an unexpected configuration. However, the examiner was still extremely supportive of the whole experiment, and it was agreed that the installation discs would be posted to him. This was done, but after repeated requests for him to perform the installation it was never done. No reason was given.

The Examinations office did not have any version of Microsoft Office installed and were still on Windows 3.1. Their computing equipment was extremely old and the specification of their machines was such (486 processors with no CD ROM Drive) that they were unable to run the security software at any reasonable speed. Consequently the participants in the project had to exchange their equipment for Pentium processors so that the pilot software would run at an acceptable speed. The lack of Microsoft Office also meant that they were unable to process the examination papers, so licenses had to be purchased.

8. Results

8.1. Usage Statistics

Because of the failure to install the security software on the PC of one departmental administrator, this meant that half of the external examiners could no longer participate in the pilot project. One of the others gave no reason for pulling out, and consequently we were left with just one successful installation.

Sample Size	Successfully	Successfully	Successfully sent

	installed	received Exams	comments
4	1	1	1

Table 1. Statistics from External Examiners

All twelve lecturers were successfully installed, but for most CMS lecturers this was only after a delay of two weeks or more due to network problems (see later). Due to the time critical nature of the examination's process, many of these lecturers simply went ahead with the current paper based process and ignored the electronic process. Others knew about the installation failure of the administrator's system, and so decided to abort the project. Only one member of CMS staff persevered. In the ITI the success rate was much higher. The only lecturer who sent his examination via the existing paper based route had already completed his script before the electronic software was installed. The only lecturer who did not successfully get the electronic comments from the external examiner had forgotten his password by the time they arrived.

Sample Size	Successfully installed	Successfully sent Exam to internal QA	Successfully sent Exam to Administrator	Successfully received External's comments
12	12	2/6	5/6	2/3

Table 2. Statistics from Lecturers

Sample Size	Successfully installed	Successfully received Exam	Successfully sent to External	Successfully received External's comments
2	1	1	1	1

Table 3. Statistics from Administrators

One notable point is that once a secure PKI infrastructure is in place, participants are free to spontaneously devise new uses for it. As a case in point, one ITI lecturer obtained an electronic class list in spreadsheet format from the administrator, then marked some module assignments at home, inserted the marks into the spreadsheet and securely emailed this to the administrator for importing into the marks database. The infrastructure could also be used as an aid to distance learning, for example, for the secure electronic submission of assignments, for remote student registrations etc.

8.2. Time and Cost of the Processes

A measure of success of the electronic transmission process, is whether time and money were actually saved using the system. Thus, the time taken and the additional costs incurred for the examination papers in both the traditional and secure electronic systems were compared for the ITI and are summarised below. No comparison was possible for CMS.

The additional cost in the traditional process was the cost of sending the examination papers using the Royal Mail Registered Postal Service. This is the cost of first class postage plus a supplement of approximately £3.00.

METHOD OF PAPER TRANSMISSION	TIME THE PAPER IS IN THE SYSTEM ONCE COMPLETED BY THE ORIGINATOR						ADDITIONAL COST
	I	II	IIIa	IIIb	IV	Total Time	

A. Traditional	5 mins - 48 hours	1 day	3 days	1 day	1 day	**6-8 days**	**£7.30**
B. Secure Electronic	<1 hour	<1 hour	<1 hour	<1 hour	<1 hour	**4 hours**	**None**
Key: **I –** ***Originator to Administrator*** **II -** ***Administrator to External*** **IIIa -** ***External to Administrator*** **IIIb -** ***Administrator to Originator*** **IV -** ***Final Version From Originator to administrator***							

At the first stage of the traditional process, the transmission time was measured for a number of originators from the time they finished preparing their examination papers until they had delivered them to the administrator. The shortest time possible for an originator is approximately 5 minutes. This is for an originator who completes their examination paper on the University premises, copies it to floppy disk and actually walks to the Administrator in the same building to hand over the floppy disk. The longest time measured was 48 hours. This was for an originator who produced his examination paper at home. This delay was caused by the originator not coming into the university the next day, and then it involved the time taken for the originator to travel to the university and physically hand the examination to the administrator. If it had been posted by registered mail, this would have taken at least 12 hours and be an added cost to the originator. With home working, facilitated by telecommunications technologies, becoming more predominant, examination papers are increasingly being prepared off-site by originators, and so we can expect the time for the first stage to increasingly tend towards the longer time rather than the shorter one. If one takes into account conference attendance, project meetings or similar external events, then transfer times can soon stretch to seven days.

In the secure electronic case, the whole transition time took approximately 4 hours with no additional costs. This occurred with only one examination paper out of the 12 selected. The successful one was quite remarkable in itself, as both the originator and the external examiner were out of the UK at the time that the interchange took place (the external examiner was at the Irish University, the originator was at a conference in the USA, and the administrator was in the ITI). Thus, when the electronic submission process is used to its full potential, it is faster and more cost effective than the traditional transmission process.

9. Difficulties Encountered

9.1. By the Users

Several users encountered difficulties in encrypting documents for the intended recipients. There was a problem in understanding that the document had to be encrypted for a particular recipient in order that only they could decrypt it. This shows a necessity for explanation and documentation of the actual process of sending secure examination papers. Specific difficulties encountered by the various groups were:

I. **An Administrator** - found it difficult to grasp the concept of secure transmission of electronic papers and had a problem in understanding that the document had to be encrypted for a particular recipient. While the user does not have a home Internet connection and has never used security software, the attitude and thoughts scores indicated that this participant was not a technophobe, but rather needed more intensive and structured training in the use of the software and in understanding the process.

II. **The Originators** – There was a distinct difference in the needs and requirements of these users. Those who had not had experience or knowledge of security software before:
   - needed documentary support,
   - had a problem in understanding that the document had to be encrypted for a particular recipient.

   Other problems encountered by participants centred on their chosen password used to protect their use of the system (i.e. protecting their private key). With the Entrust software passwords have to be a minimum of 8 characters of which one has to be numerical and another uppercase. Participants found that after choosing a password with this combination of characters it was difficult to remember, and three of the six ITI originators forgot their passwords at some stage during the project. However those that did not, used a password that they regularly used elsewhere. This again suggests a necessity for explaining and educating users especially on the necessity for secure passwords. Practical suggestions need to be made that will aid users in remembering their passwords.

III. **The External Examiners** – The attitude and thoughts scores of both these participants were very similar. Both were technophiles, confident and comfortable with computer usage, and were enthusiastic about the project. However, the respondent who used the software successfully had previously used security software, had a home Internet connection and was in the age group 35-44. The respondent who did not use the software, had not used security software previously, did not have a home Internet connection and was in the age group 45-54.

9.2. The Supporting Network

Network difficulties delayed installation and training. There were two periods, one of a week and one of several days, when the University intranet was not fully operational due to the failure of a piece of hardware (a router). The technical support department that has the responsibility for dealing with the University network did not have the resources to fix the problem immediately, which lengthened the delay. They also did not have a spare router in stock when it finally failed and so had to wait several days for the ordering and delivery of a new one. These network problems occurred at the critical time when participants were due to have their security software installed, and be trained in the use of the software.

Further network problems also had an impact on the Entrust security software causing it to be unable to register new users. The problem was due to the university's network administrator modifying the DNS tables for the university, without notifying the Entrust administrator. The DNS tables translate user-friendly names into computer-friendly numbers (e.g. venables-0068.salford.ac.uk rather than 146.87.80.68). The software provided to end-users referenced the central server by its name rather than its number, as this improves mobility and failure recovery. Therefore, the unexpected change in the name of the central server caused the security software to fail.

Finally, the CMS Notes e-mail system went down for a period of a week just when lecturers were supposed to be e-mailing their papers to each other for QAing. Thus some lecturers were not able to participate in even the first stage of the pilot.

10. Lessons Learnt

There are many conclusions that can be drawn from this pilot project. These can be divided into 3 major areas of interest – the users, the technology and the examination preparation process itself. Overall the findings showed that once the security infrastructure is in place and the electronic examination preparation process is used to its full potential then it is effective as it:

- cuts operational costs (ignoring the costs of establishing the infrastructure),
- saves valuable time,
- improves efficiency, and
- allows other value added electronic services to be organically added to the security infrastructure.

Perhaps more importantly, the project found that there were some formidable obstacles to extending the pilot to a full roll out to the whole university. These are described below.

10.1. The Users

One of the problems that had a significant disruptive influence on this project is resistance to change by users. All participants in CMS, except one, were unwilling to participate in the project at the outset and had to be persuaded by explaining the project and using incentives (a book token). Before any kind of change can take place, a full assessment of the types of user in an organisation must be made. By identifying the types and the profiles of the respective users, it is possible to design an implementation process tailored to their differing needs and requirements. This is seen to be essential in order to facilitate a system change and increase its probability of success. The fact that some users felt the current paper based system was inconvenient, slow and antiquated whilst others (50% in the case of CMS staff) felt that it was satisfactory for its purpose, indicates a need for a more detailed analysis of the process and the involvement by all parties in a consultative stage. The stakeholders need educating in a way that will encourage their commitment to the process. Without a basic level of commitment, no project can be successful.

Secondly, the users not only need training in the use of the software but also require an appreciation of how the encryption software works so as to ensure that no mistakes are made when sending encrypted material.

Finally a special section is reserved for the issue of passwords. The user's password is his passport to unlocking his private key, and a forgotten password causes a significant amount of upheaval and administrative overhead in operating the system (not to mention the delay that it causes). Given that 50% of our users forgot their passwords in the short time between installation and training and actual use, a way needs to be identified to ensure that users do not forget their passwords, or do not need them. Smart cards with pin numbers are one possible way to avoid secure passwords, but this is a costly alternative, and the user still needs a pin number. Biometric authentication such as that offered by fingerprint readers, are a better alternative, but until these systems become more popular and cheaper then a way will need to be found to help novice users remember their passwords.

10.2. The Technology

The findings revealed many technological issues that are crucial to the successful implementation and operation of the secure electronic examination process. The first major finding is that an organisation's network infrastructure and support mechanisms must be adequate to support time critical systems such as the secure electronic examination process. The university thought that it had reliable network and email systems, but our pilot showed they were not sufficient for mission critical functions. Not only were there problems with the basic network infrastructure, e.g.

- incompatible components,
- insufficient spare components in stock, and
- no adequate back up system to support users in case of longer-term infrastructure problems,

but the technical support services were not to a standard that allowed them to deal effectively and efficiently with problems that arose, within a time scale that caused minimal disruption to the users. E-mail communication with the support staff revealed that they were under-staffed and/or over committed, thereby causing significant delays to their duties. No organisation would tolerate its telephone system or postal system to be out of action for a week or longer, but during the course of this pilot various network and e-mail components were unavailable for nearly 3 weeks.

This project also highlighted the problem of hardware and software incompatibility within an organisation. The diverse types of hardware, network infrastructures, operating systems and software that exist in different departments within the organisation, had a large impact on the successful operation of the pilot. This caused problems with:

- installation of the security software,
- opening and printing electronic documents sent between the different parties.

These issues must be addressed before an organisation-wide electronic process can be successfully introduced. A policy to enforce common hardware and software throughout an organisation is needed, particularly in the area of word processing, to ensure intra-organisational compatibility, and the ability to transfer examination papers between systems without formatting or other changes being surreptitiously introduced into the documents.

10.3. The Examination Preparation Process

The current paper based process is centred on the administrator. The administrator performs two essential functions:

- manages the process, ensuring that all staff submit their examination papers on time,
- is a common interface to the external examiner, reducing the costs to the organisation (only one registered mailing is needed) and the time of the academic who does not need to know the name or address of the external examiner.

Simply converting the paper based document flows into electronic ones will not gain the best improvements in cost, time and efficiency from the new system. Our findings reveal that the administrator now becomes a bottleneck in the new system, rather than providing a value-added function. The administrator has to needlessly process the electronic scripts, by decrypting them when they arrive from the lecturer and then re-encrypting them to the external examiner. This process is repeated when the comments come back from the external examiner. Not only this, but the administrator

also becomes a source for the introduction of errors, by forwarding the encrypted mail from the lecturer straight to the external examiner (or vice versa) who then cannot decrypt and read it. Consequently we believe that the administrator should no longer be the central hub in an electronic process. When questioned about the role of the administrator, the majority of lecturers felt that the administrator should oversee and manage the flow of electronic documents between them and the external examiners but should not actively participates in the process. Therefore we conclude that process redesign should be a necessary and early step in the introduction of a secure electronic examination preparation process.

11. Conclusions

The project attempted to take a current paper based process and provide a direct electronic equivalent. It found a variety of results, with the extremes being:

- For one examination paper, both setter and external examiner had no problems installing and using the software and achieved a very impressive result;
- For one entire department, a crucial user had difficulty installing the software and the entire department was unable to achieve any result.

These show the best and worst results that can be obtained. Further study of the failures shows that many of the problems were caused by aspects of the university's IT infrastructure such as it's intranet and the specification and compatibility of PCs used by administrators. Other problems were exacerbated by central points of failure in the manual processes being studied.

We therefore conclude that computerisation of an existing paper-based process is not an appropriate solution to the problem of examination paper preparation, but that new processes should be designed explicitly to make more effective use of the technology. The project thus becomes a classic one of change management, where users need to be persuaded about the benefits of the new system (some more than others) and then educated and trained in its effective use. Two critical success factors that we found were: having a proper understanding of the process of encrypting a document for a particular recipient, and not forgetting the password that protects a user's private key. We also conclude that a computerised process cannot be more reliable than the underlying computers and networks, and that a university must treat it's IT infrastructure as a business critical resource in order to gain maximum benefits from it.

Acknowledgements

The authors would like to thank Entrust Technologies for making their security software available to the University for this and other research projects, without whose help this pilot project would not have been possible.

12. References

Chadwick, D.W. (1996) *Understanding X.500 – The Directory*, International Thomson Computer Press, (out of print but now available at http://www.salford.ac.uk/its024/X500.htm)

Chokhani, S.(1994): Toward a national public key infrastructure. *IEEE Communications Magazine*, v. 32, p. 70-74

Csinger, A., & Siau, K. (1998). The global public key infrastructure: terms and concepts. *Computer*, v. 31 no9, 30-31.

Entrust Technologies (1999), see http://www.entrust.com/
ITU/T (1997) *X.509 The Directory: Authentication Framework*
Rosen,L. & Weil,M. (1999). *Technophobia Measurement Instruments*. See http://technostress.com/BBexam.htm
Ford, W., & Baum, M.S.(1997) *Secure Electronic Commerce*, Prentice Hall, ISBN 0-13-476342-4