



# Guidance Notes

Using PGP:  
two case  
studies

James Currall  
Elaine Blair  
University of Glasgow

Alison Aiton  
University of St Andrews

GD/NOTE/002



# Contents

1	Introduction .....	5
2	The Use of PGP for Examination Results Transfer at Glasgow .....	5
2.1	Introduction .....	5
2.2	Pretty Good Privacy (PGP) .....	6
2.3	Procedures .....	6
2.3.1	Setting up PGP at Crichton .....	6
2.3.2	Using PGP for examination mark transfer .....	7
2.4	Evaluation .....	7
2.5	Conclusions .....	8
3	The Use of PGP by the Executive at St Andrews .....	8
3.1	Introduction .....	8
3.2	Procedures .....	8
3.3	Results .....	9
3.4	Evaluation .....	9
3.4.1	Was it sensible to ask people to be entirely self-reliant? .....	9
3.4.2	Problems with PGP and Eudora .....	9
3.4.3	Other issues .....	9
3.5	Current situation .....	10
4	Conclusions .....	10
5	References .....	11



# 1 Introduction

There is a growing literature on how easy or otherwise a Public Key Infrastructure (PKI) is to use for encryption, and for the creation and verification of digital signatures. What is becoming clear is that a universal signature that serves all purposes, in the way that the actual scribble of a hand-written signature does, is unlikely to work with digital signatures.

At the Universities of Glasgow and St Andrews, problems which might be solved by processes involving PKI presented themselves, and two projects were set up. This document describes the problems, the way in which the technology was deployed to tackle them, and the results of the projects.

Both projects used the same software package - Pretty Good Privacy (PGP) - but they used it in different ways as parts of very different processes. PGP was used because it is available in a reasonably user-friendly form for desktop machines of all the major types and is free for non-commercial use. The package has been used for a number of years by individuals wishing to exchange information in a secure manner. The PGP trust model, unlike that of X.509 which is the alternative, does not require a Certification Authority (CA) hierarchy and is therefore very straightforward to implement in small-scale trials.

Two usability studies, which have recently been reported, are of relevance to these projects. The first [4] reports on an experiment in which a group of people were given a task to do that required them to use PGP. They were given the task, the software and the manuals and their progress was monitored. The success of the participants in this study was not very high because they had difficulty understanding exactly what they were doing with the software and the relationship between Public and Private Keys.

The second [2] reports on an attempt to convert an existing examination paper preparation process involving question setters, administrators, examination boards and external examiners into a digital process using e-mail and PKI, without changing the process. This study was beset by many problems, including participant motivation, hardware, software and the fact that the process really needed changing to get it to work in a digital form.

This paper was prepared as part of the Scottish Middleware project, a two-year project funded by the Scottish Higher Education Funding Council, involving collaboration between the Universities of Glasgow, St Andrews, Paisley and the Royal Scottish Academy of Music and Drama. Details of the project are available at:

<http://www.gla.ac.uk/scotmid>

The technology behind the use of digital signatures are outlined in Currall and Blair (2001) [3].

The policy and process behind the use of digital signatures are described in Blair (2001) [1].

## 2 The Use of PGP for Examination Results Transfer at Glasgow

### 2.1 Introduction

The University of Glasgow, in common with many institutions, has its activities spread over a number of geographically separated campuses. In 1999, a new campus on the site of the Crichton Hospital in Dumfries opened to students. After the first diet of examinations in January 2000, the results had to be transmitted to the central Registry in Glasgow by courier and the certified results for display at Crichton had to be transferred from the Registry to Crichton by courier. The round trip of examination results from the examiners' meeting to the Registry and back took several days, whilst the same process takes only a few hours on the main University campus at Glasgow.

The problem with doing the whole thing digitally over e-mail revolves around the following requirements:

- that the Registry has the sheet of results signed by the examiners before the results are processed;
- that the examination results should be transferred securely to the Registry;
- that the Registry and the Senate are confident that the results have not been altered in transit between the examiners and the Registry.

The staff at Crichton and the Registry were anxious to develop a set of procedures such that the students at Crichton would get their results as quickly as the students at Glasgow. The problem therefore centres on getting examination results, and appropriate assertions that they represent what the examiners have agreed to, from remote locations (such as the Crichton campus) to the Registry in a timely manner.

The University Registry approached the Computing Service to ask if a solution to this problem could be found. The Computing Service decided that a process involving Public Key Encryption using the software package PGP could provide the answer and in June 2000 PGP was used successfully for examination results transfer from Crichton to the Registry.

## 2.2 Pretty Good Privacy (PGP)

PGP is a software package that is freely available to anyone who wants to use it for non-commercial purposes. It provides for privacy, authentication, integrity and non-repudiation through the use of encryption and digital signatures. Messages and files can be encrypted (scrambled) so that they can only be read by the intended recipient. A digital signature on a document establishes the identity of the author, proves that the document has not been altered and means that the author cannot deny signing the document. PGP is normally used in conjunction with an e-mail package to send encrypted and/or signed messages or files, although it can also be used to store encrypted files on a computer.

To use PGP you need to have it installed on your computer and on the computers of parties with whom you wish to communicate. You then need to create a key pair (matching Private and Public Keys) for yourself. The installation process for PGP guides you through both installation and key pair creation. The Private Key should be available only to its owner and is used to sign and decrypt messages. It must be kept secure and is protected by a passphrase (a longer version of the sort of password frequently used with computer systems). The Public Key should be made known to anyone who needs to send you messages and everyone who needs to verify your signature, and is used to encrypt messages or files and verify signatures. Whilst there is a relationship between the Public and Private Keys, it is considered impossible to derive the Private Key from the Public Key. To send an encrypted message to someone or to verify his or her signature you therefore need to obtain his or her Public Key. You can obtain Public Keys from e-mail messages or web pages but you need to confirm that you have the correct key. One way of doing this is to telephone the person, compare copies of the key and check that both parties see the same unique fingerprint for the key. Once you have confirmed that you have the correct key, you can countersign it so that your copy of PGP will trust it in future transactions.

## 2.3 Procedures

### 2.3.1 Setting up PGP at Crichton

During May 2000, James Currall from the Computing Service and Vivien Stewart from the Registry devised a process by which examination results could be transferred securely from Crichton to the Registry and whereby the Registry could have confidence that the results were identical to the ones on the sheets signed by the examiners. Documents were written which outlined the set-up processes, the examination mark encryption and signing, and the examination mark signature verification and decryption.

James Currall visited Crichton in June 2000 to install PGP on the computers of the staff who were to take part in the results transfer process. The staff created their key pairs which were countersigned by James. The Public Keys were e-mailed to Vivien at the Registry who telephoned the staff individually to cross-check the key fingerprints of both the individuals' Public Keys that she had received and the Registry Public Key that James had installed on their machines. All participants made backup copies of their keys on floppy disks and their passphrases were placed in sealed envelopes. Both floppy disks and sealed envelopes were

put in separate safe places known only to the individual concerned, so that problems arising from forgetting passphrases and computer breakdowns could be overcome. All keys had a short expiry period as this was a pilot project.

Later James gave a presentation to the majority of the academic and administrative staff at Crichton on the use of PGP in the examination mark transfer process. Only four members of staff were to actively take part in the results transfer, but all the staff at Crichton wished to understand the process and how it would benefit their students. After the presentation, those who were involved in the examination marks transfer went back to their rooms and sent a test set of results to the Registry. All four individuals managed this task without any help or assistance except for the document outlining the process.

The document detailing the process used in the examination mark encryption and signing which emphasises the purpose of signing the examination results file, and the document detailing the process used in the examination mark signature verification and decryption at the Registry are available separately.

### 2.3.2 Using PGP for examination mark transfer

Setting up basic technology and producing keys in PGP is relatively straightforward. The more difficult task is to work out the procedures to follow when installing the technology, exchanging keys and actually using PGP for examination mark transfer. There is a need to ensure that no-one involved is in a position to falsify any of the keys or, once the procedures are in use, the examination results themselves. Confidence is required that the results:

- were not tampered with in transit;
- were not viewed in transit;
- came from the right person;
- were genuine and accorded exactly with the paper copy which the examiners signed at the end of their meeting.

In this example, a responsible individual not associated with the examination itself undertakes to forward a spreadsheet containing a copy of the marks approved by the examiners to the Registry. In attaching their digital signature, they are explicitly asserting that the examination results are as on the examiners sheet, that the results have been signed by the examiners and that they have the paper copy signed by the examiners. The individual forwarding the results is acting as a surrogate for the examiners, which simplifies the technology required to complete the process. Each examiner could have been set up with a key pair and they could all produce digital signatures of the file containing the results, but there are a number of difficulties with this:

- the external examiners would have to generate key pairs on the day that they were at Crichton for the examiners meeting;
- all the examiners would have to understand what digital signatures are and what they mean;
- a series of signatures would have to be verified individually by the Registry.

A process of this nature would be complex, time consuming and error prone, and would be likely to fail.

In summary the procedure followed at Crichton, and which will be implemented elsewhere, is as follows.

One person (from a small pool of signatories) takes responsibility for a particular set of examination results. This person is not an examiner for the examination in question. This signatory produces a digital signature for the file of examination results using his or her Private Key. Signatories are made aware that their signature attests to the fact that they have in their possession a printed copy of the examination results signed by the examiners at the close of their meeting and that the file is complete, accurate and genuine. This digital signature along with the file of results, encrypted (scrambled) with the Registry Examinations Public Key, is sent to the Registry who use their Private Key to decrypt (unscramble) it. The Registry checks the digital signature using the corresponding Public Key, to ensure that the file is unaltered and that it was signed by the right person. If everything is in order, they proceed to process the examination results and print them on a printer in a secure room at Crichton a short time later.

## 2.4 Evaluation

The technology is fairly easy to set up and use. PGP guides the user through the installation process and key pair creation. Two of the users at Crichton have had to change their machines

since the original installation and have managed to repeat the process with minimal help and advice over the telephone. These users managed to replace their keys from the floppy disk on which backup copies were stored.

The importance of fully understanding the implications of having a Private Key and keeping it secure should not be underestimated, nor should a thorough understanding of what it means to make a signature using it. The greatest challenge in this project was working out the procedures to follow and then fitting the technology into the process. Devising and documenting the process and getting the approval of the Clerk of Senate took about three days of effort, whilst installation and training took a half day.

## 2.5 Conclusions

Both the Registry and Crichton were happy using PGP for examination mark transfer in June and again in September (2000) and will continue to use this method in the future. It is likely that the procedure will be offered to other geographically remote campuses of the University in the coming year.

Technology such as PGP can support digital processing for particular applications when the processes are well understood. It is easier to manage encryption and digital signatures when the people involved are known to each other and can trust each other's Public Keys, and where there are a small number of people who need to have PGP and manage their own Private Keys.

# 3 The Use of PGP by the Executive at St Andrews

## 3.1 Introduction

There is a need for people within the University to be able to exchange confidential digital information in a way that ensures:

- that it has not been altered en route;
- that it actually comes from the source from which it appears to come;
- that it can only be read by the person it for whom it is intended.

Not everyone is aware that e-mail can be intercepted (and possibly altered) without much difficulty. Even if they are aware of it, they may dismiss it as something that is 'not going to happen to me'. The very widespread use of e-mail these days has bestowed on it some of the features attributed to the postal service - reliability and trustworthiness. This does not mean that there is a belief that the mail will necessarily arrive, but rather that no-one will actively interfere with it on its journey between sender and recipient. This is not always the case, and PGP offers a possible solution. It provides a method of encrypting messages and files and of attaching a digital signature to them. The software is free and widely available and is available for both Mac and Windows platforms. It also has a plug-in for Eudora, the mail system widely used by University staff.

## 3.2 Procedures

The project team in St Andrews decided to try out the system with a small group initially. Given that members of the University Executive might well have to exchange important and/or confidential information securely, it was decided to start with this group. The participants were therefore: the Acting Principal, the Secretary, the Proctor, the Provost and the Assistant Principal.

The team were aware that the overall Intranet project has a limited life-span, and that future support for users might well be limited. Given also that a group of this sort might be expected to be motivated and computer-literate, it was decided that the team should try to make them as self-starting and self-reliant as possible.

Members of the group were all provided with documentation on how to acquire and install the necessary software i.e.:

- the mail handler Eudora (sponsored version) V 5.0;
- PGP 6.5.3;
- Aladdin Expander (to unzip the PGP file).

They were also provided with an extensive set of user notes on:

- how to create a Public/Private Key pair;
- how to exchange Public Keys with the other group members;
- how to verify the authenticity of the keys;
- how to use PGP to send and receive signed and/or encrypted e-mail via Eudora;
- general issues of key management, validation, etc.

### 3.3 Results

Of the group of five, only two succeeded in installing all the software themselves due to genuine and unanticipated difficulties. However, once their keys were generated, they all succeeded in sending a copy of their Public Key to Alison Aiton via Eudora. Once Alison had gathered all five Public Keys and verified their authenticity (checking fingerprints by phone), she signed them, pasted them all into an e-mail and sent a copy to each member of the group.

There was no obvious higher authority existing in the University of St Andrews to sign these keys, so for the purposes of this pilot the group members were content to accept Alison Aiton's signature on the keys (as Certification Authority). This issue remains to be addressed, however. The existing keys can have an 'official' St Andrews CA signature added at a later date.

There seemed to be no difficulty in importing those keys to individual keyrings.

### 3.4 Evaluation

#### 3.4.1 Was it sensible to ask people to be entirely self-reliant?

The group members, although motivated and capable, were also all extremely busy individuals. They had not a great deal of time to spend persevering with installing recalcitrant software, and when things went wrong they needed to have them put right immediately.

For instance, the experiment required each member to select and download the appropriate version of Eudora. If they were not extremely careful about where they installed the software, they found all their old mailboxes inaccessible and these were individuals who could not afford to be in a position where they could not access their mail.

#### 3.4.2 Problems with PGP and Eudora

Although generating keys was not found to be particularly difficult, ensuring a smooth interface with Eudora was more problematic.

For example, St Andrews has two separate (though similar) domain names: st-and.ac.uk and st-andrews.ac.uk. Eudora is often set up to add @st-and.ac.uk to the 'To:' field in an e-mail header, although frequently the user is unaware of this. If encryption is to a Public Key with a different ending (i.e., st-andrews.ac.uk) Eudora will not be able to identify it automatically. On the PC, PGP launches a dialogue box asking the user to choose the appropriate key to encrypt to, but this is visible for only a split second before Eudora grabs centre-stage, hiding the PGP box. As far as the user is aware, the box has disappeared. The only way to get it back is to press Alt/Tab, which is not a particularly intuitive procedure.

There are a number of ways of avoiding this problem:

- the key owner can attach both extensions to the key via PGP keys/Keys/Add/Name (but if the key has already been distributed, it must be amended and re-distributed);
- the sender can ensure the full address is always specified when sending e-mail;
- the sender can choose to set up a Eudora nickname for each correspondent using the full extension.

None of the above are particularly difficult, but they add a complication which the user could do without.

#### 3.4.3 Other issues

The scale on which the experiment was carried out meant that there was no real need to look at certain issues.

If the pilot is extended to another, larger group, then the following will have to be examined:

- Public Key distribution, possibly via a web page;
- revocation issues;
- the use of corporate keys i.e., a key for 'Personnel' or 'Registry', which could be used for the transmission of low-level security documents;
- hierarchies - should there be group key-signers (e.g. Head of Personnel to sign all Personnel keys);
- cross platform compatibility.

The last of these issues is complex: St Andrews University has as almost as many Macs as it does PCs. Sending signed or encrypted e-mail from one platform to the other is not a problem, but signing an MSWord document and sending it to a different platform can be. For instance, PC to Mac is fine if both versions of MSWord are the same (e.g., Office 98 for Mac and PC). But as soon as a signed file is sent to a different version of Word, the file undergoes a conversion procedure which renders the signature invalid. Detached signatures are fine, although specific procedures must be carefully followed to avoid problems.

### 3.5 Current situation

Since the system was set up, no particular difficulties have been encountered. Group members do not use it for all e-mail communication, however. They confine its use to only those messages that they perceive to be highly confidential.

## 4 Conclusions

The two case studies illustrate the importance of having a clearly defined process into which the PKI technology is inserted. The PKI technology does not in itself solve problems relating to encryption and digital signature. The technology addresses an aspect of a process that cannot be solved conveniently by traditional means. This conclusion suggests that the PKI technology (such as PGP) needs to be carefully tailored to fit its niche in the process in each case and adds further evidence that a 'one size fits all' approach is unlikely to be successful.

In both these projects the people involved were very enthusiastic to use the systems. They recognised a problem with the existing paper-based systems and were keen to find solutions. This contrasts with the two studies outlined in the introduction, in which a clear lack of motivation (if not outright resistance) was evident.

The case studies contrast two different approaches to introducing the technology. In the Glasgow case, a presentation with question and answer session preceded issue of documents describing the use of the technology itself, whilst in the St Andrews case the busy schedule of the executive members resulted in them being entirely self taught using documentation supplied to them. This difference may have been a factor in the smaller number of difficulties experienced at Glasgow than at St Andrews, but it was obviously compounded by the fact that the St Andrews' executive members installed their own software, whilst the Glasgow staff had it installed for them (although two Glasgow staff subsequently re-installed the software themselves).

Without doubt the introduction of processes using PKI at Glasgow and St Andrews solved the problems with the paper based systems and those processes will continue for the foreseeable future. In both cases the number of participants was relatively small, which made key distribution fairly simple. Projects involving much larger numbers of participants would need to spend a considerable amount of time investigating this aspect and it is an area which the Scottish Middleware Project is currently addressing.

One of the main issues in scaling the sort of projects outlined to more widespread use is the matter of key distribution. In the Glasgow examinations situation, the problem rises in direct proportion to the number of departments or faculties sending in their results, as there is only exchange between an individual department and the Registry. In the St Andrews Executive situation, however, the problem rises as a function of the square of the number of participants, since each participant needs the keys of all the others. Further development of these projects will require a well thought out and implemented scheme for key management.

Extending this work into other information exchange activities will require careful attention to the processes in each case and explicit procedures based on those processes being developed.

## 5 References

- 1 Blair, E (2001) "An Introduction to Digital Signatures: policy and process" UKERNA Guidance Notes GD/NOTE/003 (02/01)
- 2 Chadwick, D W, Tassabehji, R and Young, A (2000), "Experiences of using a public key infrastructure for the preparation of examination papers", *Computers and Education* 35, 1
- 3 Currall, J and Blair, E (2001) "An Introduction to Digital Signatures: the technology" UKERNA Guidance Notes GD/NOTE/004 (02/01)
- 4 Whitten, A and Tygar, J.D. (1998) "Usability of Security: A Case Study"  
<http://reports-archive.adm.cs.cmu.edu/anon/1998/abstracts/98-155.html>



## Tell us what you think

Guidance Notes are produced and published by UKERNA for use within the JANET Community. We welcome your comments on all aspects of this document and on any other UKERNA publication. Please direct feedback to JANET Customer Service, at the address below, or e-mail us directly at:

documentation@ukerna.ac.uk

UKERNA manages the networking programme on behalf of the higher and further education and research community in the United Kingdom. JANET, the United Kingdom's academic and research network, is funded by the Joint Information Systems Committee (JISC).

For further information please contact:

JANET Customer Service  
UKERNA  
Atlas Centre, Chilton, Didcot  
Oxfordshire, OX11 0QS

Tel: +44 (0) 1235 822 212  
Fax: +44 (0) 1235 822 397  
E-mail: service@ukerna.ac.uk

Copyright:

The content of this document is copyright the Universities of Glasgow and St Andrews. Parts of it, as appropriate, may be freely copied and incorporated unaltered into another document unless produced for commercial gain, subject to the source being appropriately acknowledged and the copyright preserved.

The reproduction of the JISC and UKERNA logos without permission is expressly forbidden. Permission should be sought from JANET Customer Service.

Trademarks:

JANET®, SuperJANET® and UKERNA® are registered trademarks of the Higher Education Funding Councils for England, Scotland and Wales. The JNT Association is the registered user of these trademarks.

Disclaimer:

The information contained herein is believed to be correct at the time of issue, but no liability can be accepted for any inaccuracies.

The reader is reminded that changes may have taken place since issue, particularly in rapidly changing areas such as internet addressing, and consequently URLs and e-mail addresses should be used with caution.

Neither the University of Glasgow, the University of St Andrews, nor the JNT Association can accept any responsibility for any loss or damage resulting from the use of the material contained herein.

Availability:

Further copies of this document may be obtained from JANET Customer Service at the above address.

This document is also available electronically from:

[http://www.ja.net/documents/gn\\_pgp.pdf](http://www.ja.net/documents/gn_pgp.pdf)



© The JNT Association 2001

**Joint Information  
Systems Committee**

