



# Guidance Notes

An Introduction  
to Digital  
Signatures:  
the technology

James Currall  
Elaine Blair  
University of Glasgow

GD/NOTE/004



# Contents

1	Introduction .....	5
2	Encryption .....	5
3	Digital Signatures .....	6
4	Pretty Good Privacy (PGP)GP .....	6
5	Public Key Certificates .....	7
5.1	The PGP Model .....	7
5.2	The X.509 Model .....	8
6	Private Keys and Passphrases .....	8
7	Uses of Encryption and Digital Signature .....	9
7.1	Feasible .....	9
7.2	Possible (some difficulties) .....	9
7.3	Not Feasible at Present .....	9
8	References .....	10



# 1 Introduction

Encryption and digital signatures have potential uses in universities and colleges to improve the security and the confidence that may be placed on digital information exchange. Both are based on technologies which are collectively referred to as Public Key Infrastructure (PKI). This paper explains the basics of encryption, digital signatures and related concepts. It briefly describes a package called Pretty Good Privacy (PGP) which delivers this technology to desktop computers and it gives example of situations within universities where such technologies might be employed easily and with more difficulty.

Universities rely heavily on information exchange between individuals and groups of individuals. Twenty years ago much of this exchange was on paper wrapped up in an envelope. The envelope served the purpose of keeping the information from the eyes of those who should not see it (sealed if it was really confidential, otherwise perhaps not). In the intervening period digital means of exchanging information, such as e-mail, have taken over the role of paper for many purposes. Although to most of us e-mail from one person to another might as well be in a sealed envelope, given our ability to intercept other people's e-mail, standard e-mail is about as confidential as a holiday postcard. An additional facet of paper communications is that, when it is important, it is often signed with a flourish of the pen. This gives the recipient more confidence that it is truly from who purports to have signed it. Sadly this reassurance is lacking in e-mail (and other digital forms of information exchange). Where confidentiality or the authenticity of a communication are important in the digital world there are technologies which can address them, but they are neither in routine use nor without implementation difficulties. The technologies involve encryption (for confidentiality) and digital signatures (for authenticity or verification).

This document 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>

Projects exploring the use of digital signatures are outlined in Currall, Blair and Aiton (2001) [3].

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

# 2 Encryption

Encryption is the sort of technique that has been used for centuries to allow armies to pass messages to each other without the enemy being able to intercept them. In the pre-digital era, perhaps the most famous was the Enigma machine used by the Germans in WW II. What encryption does is to scramble the message in some way that can only be unscrambled by the use of a special code (often called a key). Traditional encryption uses the same key to scramble and unscramble the message (just like you use the same key to lock and unlock a door) and has always presented the problem of 'How does the sender get the key needed to unscramble the message to the recipient without the enemy also getting hold of it?'. In the 1970s and 80s a technique was developed which uses two keys, one to scramble and the other to unscramble. This technique is called Public Key Encryption, which can be used as shown in this example.

- Alice wishes to send Bob a message.
- Bob produces a pair of keys. One of them is used to scramble the message and can be safely given to anyone who wishes to send Bob a message. It is called Bob's Public Key. It can be made freely available to all and cannot be used to work out the second, or Private, Key which only Bob has.
- The other key is used to unscramble the message and Bob keeps this Private Key secret, for use only by himself. He uses it to unscramble messages intended for him to read.

### 3 Digital Signatures

A traditional signature serves three purposes: authentication (establishing the identity of the author), integrity (that the document signed is unchanged), non-repudiation (so that the author cannot deny it). These three functions work well with top copy documents, but in a world full of photocopies all sort of changes could have been made or signatures added from other documents, etc., unless the copies are verified by the parties involved. A digital signature is designed to serve the three purposes, rather than to look like a traditional signature. It is in fact a small incomprehensible file. It relies on an action being performed using something to which only the signatory has access, combined with a unique attribute of the item to be signed. Digital signatures vouch that a particular person has signed a document but of course do not say anything about the trustworthiness of that individual. A digital signature contains a date and time stamp, but this may not be reliable since it is taken from the computer's clock which may be set incorrectly. These facets are of course no different from traditional signatures. The technique used to produce a digital signature also involves Public Key Encryption, which is used like this.

- Bob wishes to sign a file. He uses something to which only he has access, his Private Key, which is used to scramble a small unique summary of the file called a digest.
- On receipt of Bob's file and the scrambled digest (referred to as a digital signature), Alice can use the same method to make her own digest, unscramble Bob's digest using his Public Key and see if they match.
- If they do match then it follows that Bob (and only Bob) signed the file and that it is unaltered, since he is the only person with access to Bob's Private Key. Any alterations, however small, to Bob's file will result in a different digest and if the digital signature was formed with any other Private Key it will not unscramble with Bob's Public Key.

Remember from the encryption section that Public Keys may be widely distributed and so anyone can in principle check Bob's digital signature. Also remember that signatures cannot be transferred from one file to another as they contain a digest specific to a particular file.

A signature for a file signed by James Currall looks like this:-

```
-----BEGIN PGP SIGNATURE-----  
Version: PGPfreeware 6.0.2i  
  
iQA/AwUAOVMeDypYUisnmBwEQLh6QCePfQXRriaPoHaZifxYqSAn+0QwjIAN3lh  
TxSvy2tQZS1vEPkFi/5dl6bq=u9gB  
  
-----END PGP SIGNATURE-----
```

### 4 Pretty Good Privacy (PGP)

Encryption and digital signatures have been available in principle for quite a long time, but the stumbling block has always been the lack of easy-to-use software to generate and manage keys, carry out the encryption/decryption of files or e-mails and produce/validate digital signatures. In the last few years such a programme has become available for PCs, Macs and many other types of computer. This programme is called Pretty Good Privacy (PGP) and is available free to anyone who wants to use it for non-commercial purposes. All the operations such as encryption, signature, decryption and verification of signature are carried out automatically once the user has indicated his or her intentions.

The minimum that you need to use PGP is to have it installed on your computer and 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. After that you need to swap Public Keys with other people with whom you wish to exchange files or e-mail and who have also installed PGP on their computers. You can send people your Public Key by e-mail, but you should then verify that it really is your key. If the recipient of your key telephones you, you can both examine your copies of the key in PGP and check that its unique fingerprint is the same. In this way you can be sure that you have exchanged the correct Public Key.

## 5 Public Key Certificates

Certificates are electronic files used to verify the identity of the certificate holder, which can for example be a person, a company or a web site. They do this by binding an identity, usually a name, to a corresponding Public Key. Certificate based authentication is generally stronger than password based authentication and is much easier to make completely transparent to the user. The two main types of certificate are PGP and X.509. PGP certificates are often used for secure information exchange with text based mailers to authenticate people, and X.509 certificates are commonly used to assert the identity of web servers in secure transactions (such as those involving credit cards) on the Web. X.509 certificates can also be used to assert individual identity from a web browser.

Although many of the problems associated with making the unscrambling key have been overcome by Public Key Encryption, there is still the problem of knowing that a Public Key which you have really does match the appropriate Private Key and is not one made available by an impostor. The approach to this problem is that Public Keys are distributed as Public Key Certificates. A Public Key Certificate contains the Public Key and some identity information such as a name and e-mail address, signed by the Private Key of the Owner and/or other responsible individuals. Those individuals may be responsible for such matters at an institution, or may just be people that can vouch for the fact that the Public Key really does belong to the person to whom it purports to belong.

There are two models for the countersigning of Public Keys to produce certificates, the PGP model and the X.509 model.

### 5.1 The PGP Model

With PGP this system of people countersigning each other's keys may be informal, based on what is referred to as a 'Web of Trust'. In this model, people sign the keys of people that they know and exchange keys as required. It is possible to build a system based on Certification Authorities (CAs - see the X.509 Model below) as a special case of a 'Web of Trust', but it requires clear guidelines to users as such a model is not enforced.

You decide whether or not to trust a PGP key by looking at the trust statements (signatures on Public Key certificates) made about the key holder, in the same way that you decide whether to trust someone who you have met (who may be known to others that you know or a complete stranger). Anyone can sign a PGP certificate if they are happy that the Public Key belongs to the person to whom it purports to belong. With PGP you have control over who you trust and how you verify their identity.

A Public Key certificate for James Currall in PGP is shown below:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 6.0.2i

mQGIBDa5fFwRBAD06/x17fzISimCjtYKf2rJBccIIMSrMiFid86esNGKuKPZpIKh
KdQ0L6g4+pRsACwLtxDeYj+oRrqqQZw0PV5Yu8cr0NwFvNudhaBkvR+oZ+0IP6u5
J195s2kq7jgBEMZ22Iu3DYmpLF3IMFY//jkG36wLVP9dF22bIH8knuZYJQCg/2YH
ElazlvnKdCawBZ7ZI7jrEFkD/13fBXgXZ/FELOeOZwotRMxUr4RZDLuOrIpl+CgW
syYlv7/eSsqYtJGYBIiZrMDfZKf46SIB/T9n8WLQCZkZqE3nBUXJyPIsqpd1as+f
/hALLk26XfNC9GrNjbx6/0sxd1VSFpclvJ1jqBRWc24nr8dpsincpbe2l6gU8lG4
D3yQBADCumjMNC9MuPROaD9y3Szy5k+zvjj8e/2Hmrnqdeqhy1u2ni/NI2VmFu6
R+w1DntFVYXEu2EnQR1zLJAiERTmrNkHJpvXq6LTYRcR+sR9S4hIsLdl/8IfzU1m
7Ys2vchYSe63Lr0EeflCC8vgf00ZhP6iEWx+NS0lPnNMxoxcPrQsSmFtZXMgQ3Vy
cmFsbCA8ai5jdXJyYwxsQGNvbXBzZXJ2LmdsYS5hYy51az6JAEsEEBECAAsFAja5
fF0ECwMCAQAKCRAqWFkP55gcLjMAKCP019hPIr9e9eCGqF+vJK+ZaBmDACg9rt7
PhvL5g3gDhm8+XinDFThJUy0JUphbWVzIEN1cnJhbGwgPGphbWVzQHN0YXRzLmds
YS5hYy51az6JAEsEEBECAAsFAjky1sQECwMCAQAKCRAqWFkP55gcPkUAJ41ZU91
Wb05TSjeMenPK4ipSwBBOQCeJx56tFmn49IsUkbAvIV4X5zRHzuJAEYEEBECAAYF
Ajky1xIACgkQiQFQUr3wPGgXqACcDMGgsOA5gEU/cWj3FxE+AUe9T2UAoPHTtwXB
3osnFOYt2a5iJfKI9LK4tCVKYW11cyBDdXJyYwxsIDxqZXBjMWVAdWRjzi5nbGEU
```

```
YWMudWs+iQBLBBARAgALBQI5MpblBAsDAgEACgkQKlhSJKEeYHAjzgcEmV9OaMvN
EKwq1YNGdXSnYo+rVA4AnjUGhBGmPbkEhHoJBuEfVdXczmI1iQBGBBARAgAGBQI5
MpczAAoJEIkBUFK98DxogvkAniLl4ovUAzw4Ken15bITc2Cx8TLWAJ0S40dk+S1p
c2JNnKOFYBP2qxUJmbkBDQQ2uXxjEAQA/owFjNyaKHEUCMr0zMt47+AOR1VDAZXN
ZT7rvbbgIwlg6BQVX0e/B/D36B46m4CEs8iAIwk85ulcVJAjCjFq9S4awZRP2RCr
LGk7CSQzPzrVjLCSWUc56Lwalm3jG1IjIoKNfUNh6S60NtP/nqfT16OCilHKgsS7
3GnyRuCrS9sAAgIEAIkULatZpthN6vQ4wZUYI76mcX8MSEmhGkNHYDBuWRokdiwA
JcSjDENY9gM2uqA3Bv389+uPxKtBd3xgUU9SSsKNfXZrWU1/DnYX2dqiehQgpU8Y
GF2jWNMF9hQs6gu05YAQkXBMhjbHD4If/ZWLPhKAXGh9Yp/yLnm1mmV2cUKsiQBG
BBgRagAGBQI2uXxjAAoJECpYUiSnmBwvZ0An1veWFpi9DaXmBNH2Gg8ZOMNr6El
AKDTa7PPjmiPVVZasBEkmKptMoShcg===eZdj
```

-----END PGP PUBLIC KEY BLOCK-----

## 5.2 The X.509 Model

With X.509, the trust model is hierarchical, with a CA at the top which can sign keys lower down which in turn can sign keys further down and so on. The CA may be established within an institution for its own purposes or the institution may decide to make use of a 'trusted third party' CA such as VeriSign.

VeriSign (partnered with BT Trustwise in the UK) have the biggest share of the certificate market. To obtain a certificate, you go to the CA site, prove your identity to them and pay for the certificate. You generate your Private and Public Key pair locally and send the Public Key to the CA. The CA will then add your information (e.g. name, company) to your Public Key and sign it with their Private Key. In this way anyone using for example a common web-based mailer or web browser can verify your Public Key as most web browsers have VeriSign and other common CA Public Key certificates built in.

Certificate Authorities issue different levels or types of certificate, usually classes 1-3, and these need to be renewed annually. The CA goes through certain procedures to establish the identity of the certificate holder. These may or may not be very rigorous. The amount of identity checking that the CA carries out and the information contained in the certificate depends on the class of certificate issued. Class 1 certificates are for personal use. Little identity checking is carried out before these certificates are issued. They usually just check that the e-mail address supplied can receive e-mail. Class 3 certificates are used to authenticate the identity of a web site to visiting browsers and the CAs require a rather higher standard of proof before issuing such a certificate.

## 6 Private Keys and Passphrases

As has been shown, the Private Key belonging to an individual is central to Public Key Encryption and digital signatures. It has to be available only to its owner and must not be shared with others. Firstly it needs to be kept (like a bank card) where others cannot get access to it and secondly it needs to be protected by a passphrase (serving a similar function to the PIN used with a bank card). A pass phrase is similar to a password, but is longer and may include a mixture of upper and lower case characters, punctuation, spaces and numbers. Most importantly a passphrase should be something which its owner can remember easily, but others cannot guess. After three wrong guesses at a bank card PIN, the card is confiscated by the machine. However if someone got hold of your Private Key, they could set a computer to try every word in several dictionaries until it found the right one. It is for this reason that Private Keys are protected by a longer passphrase than conventional passwords or PINs.

## 7 Uses of Encryption and Digital Signature

The feasibility of using the techniques discussed in this paper to streamline digital processing within a University, depends on how many (and how diverse a range of people) need to have PGP and to have their own Private Keys. Each person who has a Private Key needs to understand fully the implications of having it, using it and keeping it and its passphrase in such a way that no-one else can use it. No-one should give his or her passphrase to someone else to use on their behalf (a secretary for example). It is also more difficult to manage encryption and digital signatures if the people are not all within one institution, particularly if they are not already known to each other. The main issue is: 'should you trust the Public Key offered as really belonging to the person who claims to own it?'.  
The following sections identify some areas of our activities and their suitability for use with digital signatures.

### 7.1 Feasible

- Incoming job references or applications could be encrypted (only one Private Key is required in the personnel department and the personnel department's Public Key could be made widely available).
- Discussion of examination questions among question setters could be encrypted and signed (small group who all know each other and could exchange Public Keys - external examiners might be a problem). (Chadwick, Tassabehji and Young, 2000 [2])
- Sending examination questions or results to the Registry encrypted and signed (possibly too many Private Keys if all examiners needed them but could adopt a scheme similar to the one adopted at the Crichton campus of the University of Glasgow in Dumfries, where they are signed on behalf of the examiners, by an approved person as proxy) (Currall, Blair and Aiton, 2000) [3].

### 7.2 Possible (some difficulties)

- Approval forms used across an institution could be signed (e.g. Head of Department, Personnel, Finance would all need Private Keys to add their signatures and exchange Public Keys for verification).
- Medical certificates. The actual certificate could go straight to the University Registry who could then send a signed e-mail notification to departments and/or Advisers of Studies to say that they have seen the certificate. (A fairly wide distribution of Public Keys would be necessary, the Registry may not want to handle all the certificates and departments might need copies).

### 7.3 Not Feasible at Present

- Purchase orders signed by budget holder and purchase officer (potentially too many Private Keys distributed across an institution).
- Monthly financial reports sent to heads of departments (encryption using many different Public Keys, though possible, is more likely to create difficulties).
- Booking forms for resources, such as vehicles, rooms, etc., signed by users (potentially everyone who uses the resource would need Private Keys).
- Internal processing of grant applications and other internal forms processing which are signed by various people (too many people would need Private Keys).
- Signed applications and/or forms from outside (difficult to verify external Public Keys as being genuine without a central CA for HE/FE).
- Forms originating from a wide variety of individuals, such as expense claims, signed by the individual and possibly a budget holder (too many people would need Private Keys).

## 8 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, Blair, E and Aiton, A (2000), "Case studies in the use of PGP".  
<http://www.gla.ac.uk/projects/scotmid/gendocs/pkicase-smp.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 University of Glasgow. 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 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\\_ds\\_technology.pdf](http://www.ja.net/documents/gn_ds_technology.pdf)



© The JNT Association 2001

**Joint Information  
Systems Committee**

