Secure Conferencing User Guide for
PGP on Win95/NT and Unix

Edmund Whelan

University College London

Version 1.2a (DRAFT)

28 October 1998

© University College London, Computer Science Department

Disclaimer

UCL cannot accept any responsibility for any loss or damage resulting from the use of the material contained in this document. The information is believed to be correct, but no liability can be accepted for any inaccuracies.

Copyright note

Copyright © 1995-1998 University College London. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted, for non-commercial use only, provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
   "This product includes software developed by the Computer Science Department at University College London."
4. Neither the name of the University nor of the Department may be used to endorse or promote products derived from this software without specific prior written permission. Use of this software for commercial purposes is explicitly forbidden unless prior written permission is obtained from the authors.

THIS SOFTWARE IS PROVIDED BY THE AUTHORS AND CONTRIBUTORS "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software is derived, in part, from publicly available source code with the following copyright:

Copyright © 1991-1993 Regents of the University of California
Copyright © 1992 Stichting Mathematisch Centrum, Amsterdam
Copyright © 1991-1992 RSA Data Security, Inc
Copyright © 1992 Jutta Degener and Carsten Bormann, TU Berlin
Copyright © 1994 Paul Stewart
Copyright © 1996 Regents of the University of California

This product includes software developed by the Computer Systems Engineering Group and by the Network Research Group at Lawrence Berkeley Laboratory.

Encryption features of this software use the RSA Data Security, Inc. MD5 Message-Digest Algorithm.

Contents

1 OVERVIEW 1

2 INTRODUCTION 1

- 2.1 VIDEOCONFERENCING 1
- 2.2 SYMMETRIC CRYPTOGRAPHY 1
- 2.3 ASYMMETRIC CRYPTOGRAPHY 1

3 SOFTWARE 2

- 3.1 CONFERENCE ANNOUNCEMENT (SDR) 2
- 3.2 AUDIO (RAT) 4
- 3.3 VIDEO (VIC) 4
- 3.4 SHARED TEXT EDITOR (NTE) 5
- 3.5 SHARED WHITEBOARD 5
- 3.6 OTHER SOFTWARE 5

4 KEY MANAGEMENT 6

- 4.1 WINDOWS 95/NT PLATFORMS 6
  - *4.1.1 PGP Key Management Tool (PGPkeys)* 6
    - 4.1.1.1 Starting PGPkeys 6
    - 4.1.1.2 Generating Key Pairs 7
    - 4.1.1.3 A Typical PGPkeys Window 7
    - 4.1.1.4 Selecting Keys 7
  - *4.1.2 Eudora Light* 8
    - 4.1.2.1 Sending Secure Email 8
    - 4.1.2.2 Receiving Secure Email 8
    - 4.1.2.3 A Typical Eudora Window 9
- 4.2 UNIX PLATFORMS 9
  - *4.2.1 PGP 2.6.3i* 10
    - 4.2.1.1 PGP Commands 10
  - *4.2.2 The exmh mailtool* 11
    - 4.2.2.1 Sending Secure Email 11
    - 4.2.2.2 Receiving Secure Email 12

5 SETTING UP A SECURE CONFERENCING ENVIRONMENT 12

- 5.1 INITIAL STEPS FOR THE USER 12
- 5.2 HANDLING CERTIFICATION REQUESTS (SECURITY MANAGER ONLY) 13
- 5.3 FINAL STEPS FOR THE USER 14

6 CONFERENCE GROUPS 15

- 6.1 CREATING A NEW GROUP (CONFERENCE PARTICIPANT MANAGER ONLY) 15
- 6.2 BECOMING A MEMBER OF A GROUP 17

7 SITUATIONS WHICH MAY ARISE 18

- 7.1 NEW USER WANTS TO JOIN AN EXISTING GROUP 18
- 7.2 USER'S KEY IS COMPROMISED 19

8 CONCLUSION 21

9 CHANGES FROM PREVIOUS DRAFT 21

1 Overview

This document gives a step-by-step guide to the new user who wants to start using the secure conferencing software available from University College London. It aims to provide full details for normal users as well as users who wish to act as Conference Participant Managers (CPMs) or as the Security Manager (SM). This version of the document covers the use of PGP on both Windows 95/NT and Unix platforms and does not concern itself with the use of the Secude security toolkit, which is supported as an alternative to PGP.

2 Introduction

2.1 Videoconferencing

Multipoint videoconferencing has been available for some time but has, in general, required special equipment and facilities. In addition conferences are usually set up as a series of point-to-point connections between a multipoint control unit and each participant. This has the disadvantages that it is both expensive and does not scale to support large user groups. The Internet provides a suitable alternative for truly scaleable videoconferencing using publicly available software. One type of conferencing on the Internet uses multicast transmission rather than the point-to-point communication used by telecommunications companies. In principle this allows an unlimited number of participants to communicate with each other at the same time; it is implemented through the Multicast backbone (Mbone). This is a virtual network which makes use of the Internet, but uses a number of multicast routers (mrouters) to wrap multicast messages so that they appear as normal Internet traffic to the many normal internet routers which are unable to interpret the multicast addresses used. These wrapped packets are then passed between the multicast-aware routers. There are several parts to Internet videoconferencing: Conference Management; audio; video; shared whiteboard and; shared text editor. These are briefly discussed in later sections.

2.2 Symmetric Cryptography

Symmetric cryptography uses the same key to decrypt a message as was used to encrypt it; thus both the originator and recipient must know the key. This means that a secure way of distributing the key must be available and, as the key needs to be changed frequently for security reasons, symmetric cryptography does not scale well as the number of participants increases. Consequently, this type of encryption is not, by itself, suitable for the announcement of conferences. Nevertheless, since it is relatively fast, it is often used when large amounts of data need to be encrypted. Two of the more popular symmetric encryption algorithms are the Data Encryption Standard (DES) which uses a 56-bit key and triple-DES which uses the same algorithm as DES but encrypts the message three times using two different 56-bit keys. The multimedia audio, video and shared text editing tools currently use DES encryption when encryption is enabled.

2.3 Asymmetric Cryptography

Also known as Public Key Cryptography, this overcomes many of the problems inherent in symmetric cryptography. Each user has a pair of keys which are related mathematically in such a way that it is not feasible to determine one key even when one knows the other. Consequently, one of the keys can be made public and is referred to as the “Public Key”; the other is kept private and is known as the "Private Key". Due to the relation between the two keys, messages can be encrypted by anybody with access to the public key; they can only be decrypted by the owner who alone has access to the private key. The fact that a different, albeit related, key is used to encrypt and decrypt the message explains the term "asymmetric" cryptography. Public Key Cryptography also allows messages to be digitally signed allowing the recipient to be confident that the message originated from the owner of the private key and was not altered *en-route*. The session announcements created by SDR can be encrypted and/or signed using Public Key Cryptography. Two packages which can be used are **Pretty Good Privacy™** and **Secude™**. In general these perform the same function but only Pretty Good Privacy is discussed in this document. It is also possible to encrypt the SDR announcements using symmetric encryption (DES).

3 Software

One recommended set of conference tools is listed in the table below. This table mentions the name of the tool, the version in current use, a site from which it can be downloaded and a brief descriptor of the tool. A brief discussion of each tool is given below with much fuller documentation being available for each tool from the download site.

Software	*Version*	*Download Site*	*Notes*
SDR	2.5.8	http://www-mice.cs.ucl.ac.uk/multimedia/software/	Conference Mgt
RAT	3.0.28	http://www-mice.cs.ucl.ac.uk/multimedia/software/	Audio Tool
VIC	2.8	http://www-mice.cs.ucl.ac.uk/multimedia/software/	Video Tool
NTE	1.5.31	http://www-mice.cs.ucl.ac.uk/multimedia/software/	Text Tool
WB	1.60/1.59	http://www-mice.cs.ucl.ac.uk/multimedia/software/	Unix WB Tool
WBD	1.0	http://www-mice.cs.ucl.ac.uk/multimedia/software/	Windows WB Tool
Tcl/Tk	8.0p2	http://www.scriptics.com/	Needed for Interface

Table 1. Minimum software necessary which allows symmetric encryption to be used.

Software	*Version*	*Download Site*	*Notes*
PGP	2.6.3i	http://www.pgpi.com/	PGP used by SDR

Table 2. Security software which can be used with SDR.

Software	*Version*	*Download Site*	*Notes*
Eudora Light	3.0.5	http://eudora.qualcomm.com/	Email Tool
PGP	5.5.3I	http://www.pgpi.com/	PGP used with Eudora

Table 3. Software necessary for group and key management on Windows 95/NT.

Software	*Version*	*Download Site*	*Notes*
exmh	2.0.2	http://www.scriptics.com/applications/email	Email Tool

Table 4. Software necessary for group and key management on Unix platforms.

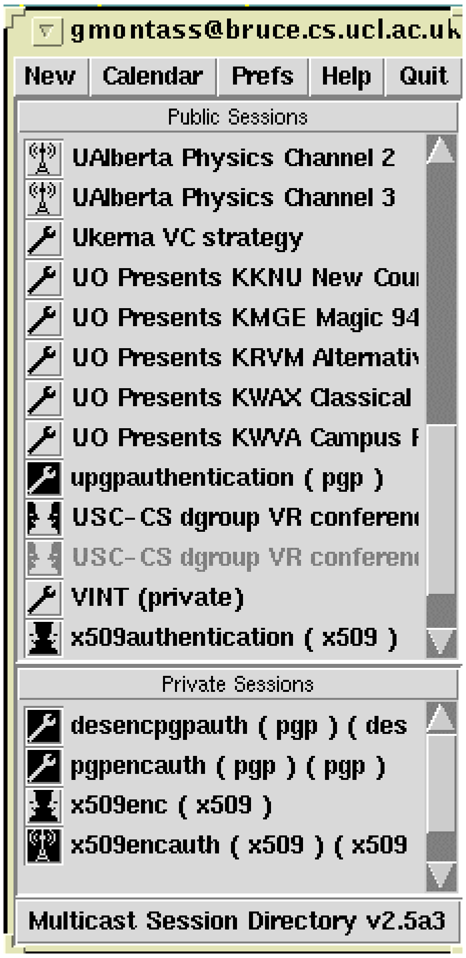
3.1 Conference Announcement (SDR)

Conference Announcement is done with the multicast session directory tool, SDR, which can be downloaded from the above site. The "*http://www-mice.cs.ucl.ac.uk/multimedia/software/*" site will be referred to as the official web-site throughout this document.

Win95/NT: Once downloaded you should double-click on the self-extracting binary and, when prompted for a directory where the program should be installed, type *"C:\Program Files\mbone"*.[1]

Unix: The downloaded file is a zipped file and should be unzipped with a command of the form "*gunzip –c sdr-2.5.8-solaris > /usr/local/bin/sdr*".[1]

SDR lists the available conferences and allows the user to join these or set up and announce their own. The main window is shown below and clicking on the conference name will bring up further details on that conference. From the detail window clicking the "Join" button will start all the multimedia tools relevant to the conference or, alternatively, each tool can be started individually by clicking on the appropriate icon. If the media details are not shown then clicking the "Media Details" button should bring them up.


gmontass@bruce.cs.ucl.ac.uk
New
Calendar
Prefs
Help
Quit
Public Sessions
UAlberta Physics Channel 2
UAlberta Physics Channel 3
Ukerna VC strategy
UO Presents KKNU New Cou
UO Presents KMGE Magic 94
UO Presents KRVM Alternati
UO Presents KWAX Classical
UO Presents KWVA Campus
upgpauthentication (pgp)
USC-CS dgroup VR conferen
USC-CS dgroup VR conferen
VINT (private)
x509authentication (x509)
Private Sessions
desencpgpauth (pgp) (des
pgpencauth (pgp) (pgp)
x509enc (x509)
x509encauth (x509) (x509
Multicast Session Directory v2.5a3

In order to create a conference click the "New" button on the top of the main SDR window which will bring up a series of windows and you should follow the instructions available either on each window or via the balloon help system. If the balloon help system is not enabled this can be changed in the "Preferences" window. One of the screens is concerned with the media tools and various options can be set including whether the media streams should be encrypted. If this option is selected a random key is generated for that stream which can be changed by overtyping if required. It should be noted that, on Windows platforms, there is no whiteboard tool available that supports encryption so care should be taken not to encrypt this stream.

---

[1] You may use any suitable directory but should be consistent and ensure it is in your PATH.

There is also a screen concerned with the security used for the announcement itself with a choice of DES, PGP or X.509 (Secude). There are two further options where the certificate is sent with PGP and X.509; in general, these options should not be necessary. At present, it is recommended that PGP be used. In order to successfully use PGP your environment will probably need a certain amount of setting up. The minimum requirement is the creation of your own public/private key pair but this must also be distributed in such a way that other people are satisfied that it is indeed your key. You may also want to have secure conferences with a group of people and this necessitates the creation and distribution of “Group Key Pairs”. This is discussed later.

If you wish simply to use DES to encrypt the announcements then you must create at least one key via the *Prefs/Security* menu. You will be prompted for a passphrase to protect this key on your disk. You must ensure that this key is distributed via secure email or out-of-band to anyone you wish to see the announcement.

It should be noted that if you choose to encrypt the media streams and do not encrypt the announcement then an eavesdropper can read the keys straight from the announcement packet and so you should not consider the conference secure. A comprehensive SDR User Guide is available from the official web site.

3.2 Audio (RAT)

The Robust-Audio Tool (RAT) can be downloaded from the official web-site.

Win95/NT: Unzip the downloaded file into the same directory as used for all the mbone tools *e.g. C:\Program Files\mbone.*

Unix: The downloaded file should be uncompressed and placed in */usr/local/bin*. A command of the form “$gunzip –c rat-3.0.28-solaris > /usr/local/bin/rat” should be executed.

When RAT is running, the main window lists the participants with the current speaker highlighted. The controls on the right of the screen control the volume of the incoming and outgoing audio. The *Options* button brings up a number of different options which can be set by the user. DES encryption is supported in RAT. A RAT user guide is available from the official web-site.

3.3 Video (VIC)

The VIC video tool, together with a user guide, can be downloaded from the above web site.

Win95/NT: If it is a zip file the instructions for RAT should be followed whereas if it is a self-extracting binary the instructions for SDR should be followed.

Unix: The downloaded file is a tarred and zipped file. Copy this file to the “*/usr/local/bin*” directory and type the following:

```
$ gunzip –c filename.tar.gz | tar xvf –
```

When running the VIC main window shows a thumbnail of each participant who is transmitting video and information on each participant is shown to the right of the relevant image. Clicking each image will enlarge it. The *Menu* button at the base of the window brings up a number of options and you can initiate transmission of your own video from this window. DES encryption is supported in VIC.

3.4 Shared Text Editor (NTE)

The shared text editor, Network Text Editor (NTE), can be downloaded from the official web-site together with a full NTE user guide.

Win95/NT: The downloaded file is a self-extracting binary and should be installed in the same way as SDR in the *C:\Program Files\mbone* directory.

Unix: The downloaded file should be uncompressed and placed in */usr/local/bin.* A command of the form “$gunzip –c nte-1.5.32-solaris.gz > /usr/local/bin/nte” should be executed.

A list of participants is shown on the right of the main screen and each participant can type, edit, move or point to text in the main workspace. DES encryption is supported in NTE.

3.5 Shared Whiteboard

Win95/NT: Download the WBD whiteboard tool from the official web-site. It is downloaded as a self-extracting binary and should be installed in the same way as NTE and SDR.

Unix: Download the WB whiteboard from the official web-site. It is a zipped and tarred file and should be moved to the */usr/local/bin* directory and the following typed:

```
$ gunzip –c filename.tar.gz | tar xvf -
```

The whiteboard tool has a full-colour display area where each participant can write, draw or type. Currently, only the Unix tool supports encryption (DES). User guides for both WB and WBD are available from the above web site.

3.6 Other Software

As well as the multimedia software some other software is required for secure conferencing and the following steps should be performed.

Win95/NT:

- Install Tcl/Tk 8.0 in a directory called “*C:\Program Files\tcl”*
  - *Download the binary tcl/tk 8.0 release*
  - *Double click on the self-extracting binary*
  - *From SDR 2.5.9 this software should be unnecessary and this step can be omitted.*
- Install Eudora Light in a directory called “*C:\Program Files\Eudora”*
  - *Double click on the self-extracting binary*
- Install PGP 5.5.3i in a directory called “*C:\Program Files\pgp\pgp553i”*

  - *Double click on the self-extracting binary*
- Install PGP 2.6.3i in a directory called “*C:\Program Files\pgp\pgp263i”*
  - *Unzip to obtain a “readme” file and a zipped file*
  - *Read the “readme” file and unzip the zipped file to the above directory*
- Open an MS-DOS window, type “edit autoexec.bat” and add the following lines:
  - set PGPPATH=C:/Program Files/pgp/pgp553i[2]
  - set HOME=C:\sdr
- Restart your computer

Unix:

- Install exmh in /usr/local/bin
  - *Download and unzip the zipped file.*
  - *Follow the instructions which come with the package*
- Install PGP 2.6.3i in /usr/local/bin
  - *Unzip to obtain a “readme” file and a zipped file*
  - *Read the “readme” file and unzip the zipped file to the above directory*
- Ensure your PATH variable includes /usr/local/bin.
- Ensure your PGPPATH variable is set to the location of your PGP keyfiles. If your keyfiles are in the ~/.pgp/ directory they should be found even if PGPPATH is not set.

It should be noted that two versions of PGP are currently required on Windows platforms. The main reason for this awkwardness is that we desire an SDR that runs both under Unix and Windows; PGP 5.5.3i does not yet run under Unix. Consequently, PGP 2.6.3i is used by SDR whereas PGP 5.5.3i is used for the key management and exchange on Windows platforms as it has a powerful user interface and plugins for common email tools such as Eudora Light. This simplifies the key management considerably. It is expected that later versions of SDR will either use PGP 5.5.3i or have the PGP functionality built directly into the software thus eliminating the need for two versions of PGP.

4 Key Management

4.1 Windows 95/NT Platforms

The easiest way to manage a set of PGP keyfiles for use with secure conferencing is by using the PGP 5.5.3i key management tool *PGPkeys* and Eudora Light. A brief overview of these tools is given here rather than repeating the necessary steps in each section.

4.1.1 PGP Key Management Tool (PGPkeys)

4.1.1.1 Starting PGPkeys

- To start *PGPkeys* click the PGP Tray icon - - which should be on the bottom right hand of your screen.

- Select “*Launch PGPkeys*” to bring up the PGP Key management window.

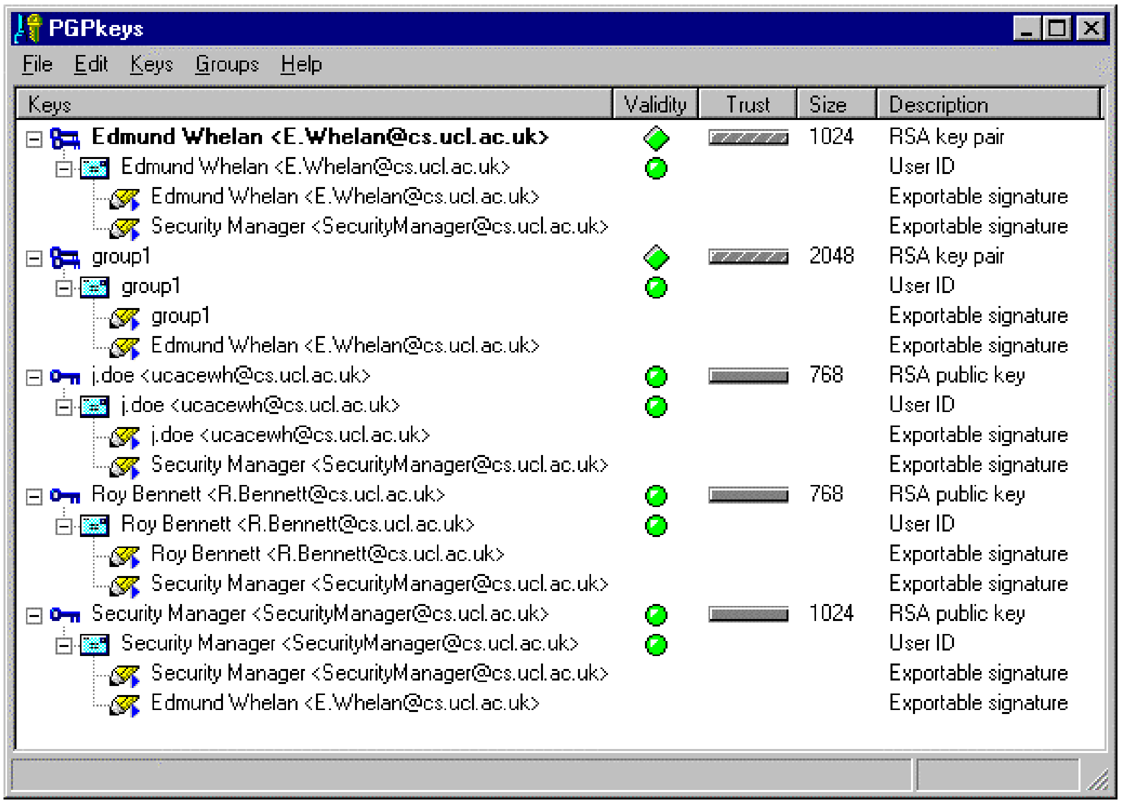
---

[2] PGPPATH specifies the location of your PGP keyfiles. Note the forward, Unix style slashes.

4.1.1.2 Generating Key Pairs

- In *PGPkeys* Click on “*Keys/New Key*” and follow the instructions. For security it is recommended that you choose a keysize of at least 1024 bits. You must select RSA as opposed to Diffie-Hellman/DSS as PGP 2.6.3i will not understand the latter.

4.1.1.3 A Typical PGPkeys Window



Keys	Validity	Trust	Size	Description
Edmund Whelan <E.Whelan@cs.ucl.ac.uk>	◆	▨	1024	RSA key pair
Edmund Whelan <E.Whelan@cs.ucl.ac.uk>	●			User ID
Edmund Whelan <E.Whelan@cs.ucl.ac.uk>				Exportable signature
Security Manager <SecurityManager@cs.ucl.ac.uk>				Exportable signature
group1	◆	▨	2048	RSA key pair
group1	●			User ID
group1				Exportable signature
Edmund Whelan <E.Whelan@cs.ucl.ac.uk>				Exportable signature
j.doe <ucacewh@cs.ucl.ac.uk>	●	▬	768	RSA public key
j.doe <ucacewh@cs.ucl.ac.uk>	●			User ID
j.doe <ucacewh@cs.ucl.ac.uk>				Exportable signature
Security Manager <SecurityManager@cs.ucl.ac.uk>				Exportable signature
Roy Bennett <R.Bennett@cs.ucl.ac.uk>	●	▬	768	RSA public key
Roy Bennett <R.Bennett@cs.ucl.ac.uk>	●			User ID
Roy Bennett <R.Bennett@cs.ucl.ac.uk>				Exportable signature
Security Manager <SecurityManager@cs.ucl.ac.uk>				Exportable signature
Security Manager <SecurityManager@cs.ucl.ac.uk>	●	▬	1024	RSA public key
Security Manager <SecurityManager@cs.ucl.ac.uk>	●			User ID
Security Manager <SecurityManager@cs.ucl.ac.uk>				Exportable signature
Edmund Whelan <E.Whelan@cs.ucl.ac.uk>				Exportable signature

4.1.1.4 Selecting Keys

- To select a key in the PGPkeys window simply click the left-hand mouse button with the cursor over the relevant key.

- Clicking the right-hand button at this stage will make a pop-up menu appear and this can be used to view the details of the key by selecting “*Key Properties*”

- If you are creating a new message in Eudora it is possible to drag keys from PGPkeys to the body of this message by highlighting the key and dragging it into the body of the message.

- If you want to select and/or drag more than one key you can highlight several keys by highlighting the first, holding down the CTRL key and highlighting any other keys you want. These can all then be dragged into the body of a Eudora mail message.

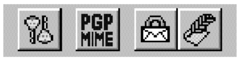
4.1.2 Eudora Light

4.1.2.1 Sending Secure Email

In order to send secure email the following steps should be taken:

- Start Eudora Light and click the *"New Message"* button

- The following toolbar should be available to you at the top of the Eudora new message window.



- If you have generated a PGP key pair for yourself you can sign any outgoing messages:

    - Click on the PGP-MIME and Sign buttons (the one with the quill). This ensures that the outgoing email is in PGP-MIME format and is signed with your private key. You will be prompted for the PGP passphrase for your private key. In general you should sign any outgoing messages so anyone with your public key can check your signature but your message is still readable if you have no secure email tool.

- If you have the recipient's public key in your PGP keyfile you can encrypt the message so only they can decrypt it.

    - Click on the PGP-MIME and Encrypt buttons (the one with the padlocked envelope). This ensures that the outgoing email is in PGP-MIME format and is encrypted with the recipient's public key. You can encrypt the message to any number of recipients as long as you have their public keys in your keyfile. This is useful if you are the Conference Participant Manager and are sending the Group key pair to a number of users.

- There may be a button to the left of those above with a box containing a red hooked arrow. This is used to select which security plugins to use. You will probably only have PGP plugins but if there are others, *e.g.* S/MIME, you should ensure that these are not selected.

4.1.2.2 Receiving Secure Email

In order to handle any signed and/or encrypted email you may receive you should do the following:

- Start Eudora Light and double click on the message you received.

- The message will be opened and you will have a line something like:

Run Plugin:"C:\Program Files\Eudora\Attach\sometitle.ems …."

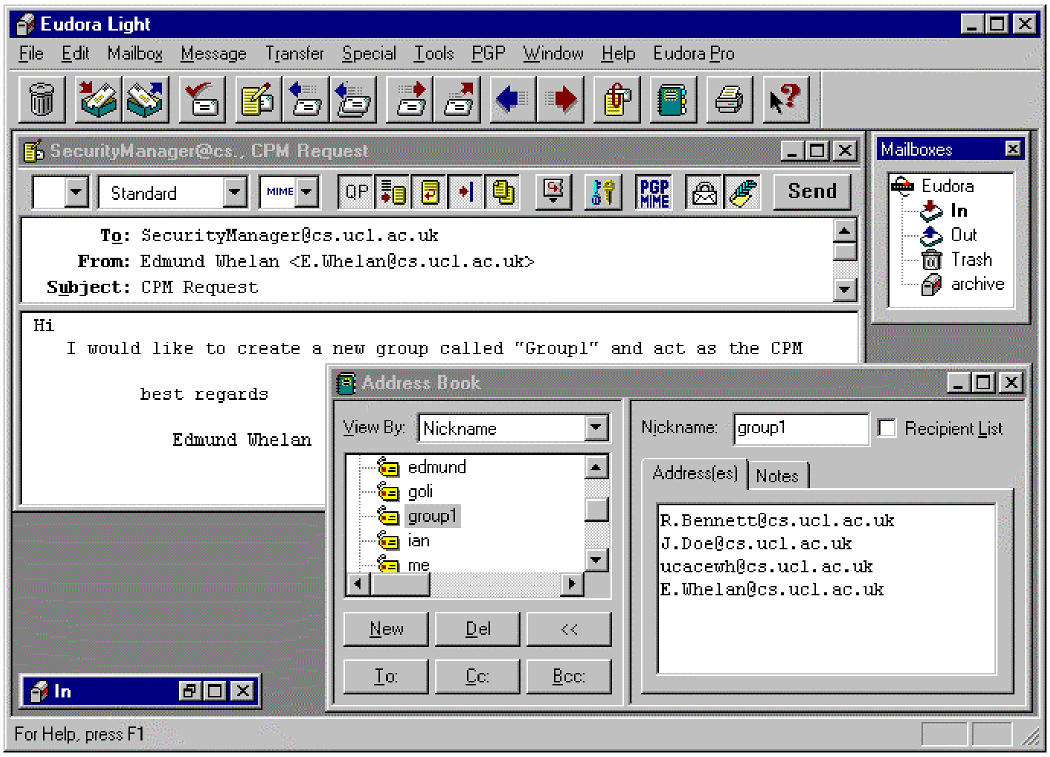
- Double click on this line. Several boxes may pop-up:

- The **PGPLog** window – if the message has been signed and you have the sender's public key in your PGP keyfile the signature will be verified. If you do not have their public key the entry "message was signed by an unknown signer" will appear. If the message "Invalid Key" appears it may be because you have the public key in your keyfile but you have not told PGP you trust it. This can be done by signing the sender's public key with your private key in PGPkeys. Once you have done this try double clicking on the message again.

- The **PGP Decryption** window will pop up if the message was encrypted and you will be asked for your PGP password. This is needed to access your private key and decrypt the message.

- The "***Key Import***" window may then appear asking you which key(s) you wish to import. This only appears when the message contains PGP public keys. Select the keys you want and click the "*Import*" button. The keys will then appear in your *PGPkeys* window. Only public keys can be imported to your keyfile in this way.

4.1.2.3 A Typical Eudora Window


Eudora Light
File Edit Mailbox Message Transfer Special Tools PGP Window Help Eudora Pro
SecurityManager@cs., CPM Request
Standard
MIME
QP
PGP MIME
Send
Mailboxes
Eudora
In
Out
Trash
archive
Address Book
New
Del
<<
To:
Cc:
Bcc:
Address(es)
Notes
In
For Help, press F1

To: SecurityManager@cs.ucl.ac.uk
From: Edmund Whelan <E.Whelan@cs.ucl.ac.uk>
Subject: CPM Request

Hi
I would like to create a new group called "Group1" and act as the CPM

best regards

Edmund Whelan

View By: Nickname
edmund
goli
group1
ian
me

Nickname: group1 ☐ Recipient List

R.Bennett@cs.ucl.ac.uk
J.Doe@cs.ucl.ac.uk
ucacewh@cs.ucl.ac.uk
E.Whelan@cs.ucl.ac.uk

4.2 Unix Platforms

The PGP Key management tool is not available on Unix platforms so PGP 2.6.3i is used. This is a command-line tool and, as such, is less user-friendly. The exmh mail tool also uses PGP 2.6.3i and is used to send and receive secure email in much the same way as Eudora on Windows platforms.

4.2.1 PGP 2.6.3i

PGP uses two keyrings, namely the public keyring (default file is ~/.pgp/pubring.pgp) where any public keys you have are stored, and the secret keyring (default file is ~/.pgp/secring.pgp) where any secret keys are stored. Each secret key is protected by a passphrase.

4.2.1.1 PGP Commands

- To generate a new key pair. Note that keysizes of at least 1024 bits should be used and, for your own key, a userid of the form "J.Doe <J.Doe@acme.org>" should be used. If you are generating a group key then the emailid field can be omitted.

```
$ pgp –kg
```

- To add a keyfile's contents to your public or secret keyring

```
$ pgp –ka keyfile [keyring]
```

- To remove a key or a userid from your public or secret keyring

```
$ pgp –kr userid [keyring]
```

- To edit your userid or passphrase

```
$ pgp –ke your_userid [keyring]
```

- To extract (copy) a key from your public or secret keyring. Using the [a] option will produce an ascii file which can safely be emailed.

```
$ pgp –kx[a] userid keyfile [keyring]
```

- To view the contents of your public or secret keyring, The [v] option will produce a verbose listing which will show all the signatures on the keys as well as the keys themselves.

```
$ pgp –kv[v]  [userid]  [keyring]
```

- To check signatures on your public or secret keyring

```
$ pgp –kc [userid] [keyring]
```

- To sign someone else's key on your keyring

```
$ pgp –ks her_userid [-u your_userid] [keyring]
```

- To remove selected signatures from a userid on a keyring

```
$ pgp –krs userid [keyring]
```

- To view general help on PGP commands

```
$ pgp –h
```

- To view help on PGP key management command

```
$ pgp –k
```

4.2.2 The exmh mailtool

4.2.2.1 Sending Secure Email

If you are using a version of exmh other than 2.0.2 then the precise labelling of buttons may differ. However, the steps you should take are the same. If you want to send secure email using exmh, click the "*Comp*" button to bring up the message composition window. Fill in the "To:", "cc:" and "Subject:" fields as normal and type your message. When ready to send the message click on the "*PGP…*" button at the top of the window and this will pull-down a menu. From this menu select either: "*PGP sign clear*" which just signs the message and sends it unencrypted; "*PGP encrypt only*" or; "*PGP encrypt and sign*". A window may pop up asking you to select the key for either encrypting or signing and, if signing, you will be prompted for the passphrase to unlock your secret key.

When sending mail:

- If encrypting a message the emailid of the recipient must be exactly the same as in the angled brackets of their PGP key.
- The PGP exmh preferences should be:
  - Always choose the sign key: ON
  - Cache map from email to public-key: persistent
- PGP may try to use the environment variable LOCALHOST to complete the email addresses. If this is set to the name of your local machine this may cause problems. If it does you should add a line similar to "setenv LOCALHOST cs.ucl.ac.uk" to your login script. Alternatively set "Cache map from email to public-key" to NONE.

If you want to send your public key to, say, the Security Manager, open the message composition window, click the "*More/Attachment/Attach PGP Keys*.." button and select the key you want to send. If the key you want is on your public keyring and it is not shown then click the "*List*" button at the top of the "*Choose Key*" window. If you want to send several keys you should select the first key from the "*Choose Key*" window and click OK and then follow the same procedure for subsequent keys. If a large number of keys is to be sent it may be more efficient to create a single PGP file outside exmh by writing a script to do the following:

```
$ pgp –kx "user1" keyfile.pgp"        (this extracts user1's key into keyfile.pgp)
$ pgp –kx "user2" keyfile.pgp"        (this extracts user2's key into keyfile.pgp)
$ pgp –kx "user3" keyfile.pgp"        (this extracts user3's key into keyfile.pgp)
$ pgp –a keyfile.pgp"                 (this creates an armored "keyfile.asc" file)
```

However, this is probably only useful if you are acting as either the Security Manager or the Conference Participant Manager.

4.2.2.2 Receiving Secure Email

If you receive a message which has been signed but not encrypted, you will be able to read the message and a button will appear which you can click to check the signature.

If the message has been encrypted a box will appear labelled "*Show with PGP*". Clicking this box will invoke PGP to handle the message. You will be prompted for the passphrase needed to unlock your secret key in order to decrypt the message.

Note that you should ensure that the option "*Keep PGP password*" in the PGP preferences window should be set to "off" as this has been known to cause problems.

If you receive someone else's public key in an email message you should click the right hand mouse button whilst the cursor is over the relevant MIME body part and enable "*Show content with PGP*" if this is not enabled. This will let you see details of the keys you have received. You should then save the keys to a file by clicking the right hand mouse button, highlighting the "*Save keys…*" option and then releasing the button.

To add someone's public key to your public keyring type the following, where *keys.asc* is the name of the file in which you saved the public key(s) from within exmh:

```
$ pgp  –ka  keys.asc  ~/.pgp/pubring.pgp
```

5 Setting Up A Secure Conferencing Environment

5.1 Initial Steps for the User

Assuming you have never used PGP before and so have no previous keys you should:

1. Generate a PGP Private/Public keypair for yourself using either PGPkeys on Windows platforms or the command "pgp –kg" on Unix platforms.

2. Send a signed email to the Security Manager with your public key in the body of the message. The subject should be "Public Key for *John Doe*" using your own name.

3. In order that the Security Manager can be assured of the validity of your key you should send the fingerprint, length and ID of your key to the Security Manager. This should be signed with your normal signature and be on headed paper from your institution and should be sent via fax or surface mail. The Security Manager details[3] are as follows:

    Email: SecurityManager@cs.ucl.ac.uk
    Phone : +44 171 419 3688
    Fax: +44 171 387 1397

---

[3] You may have your own Security Manager in which case the details will differ.

Address: Security Manager
c/o Dr Edmund Whelan
Department of Computer Science
University College London
Gower Street
London, WC1E 6BT
England

The PGP Key details for the Security Manager are:

Length: 1024 bits
Key ID: 0x53739D53
Fingerprint: CA70 9F58 125E 5036 4639 8444 2BE6 D405

5.2 Handling Certification Requests (Security Manager Only)

This section details the steps you should take, as Security Manager, upon receipt of a PGP public key from a user who wishes to be certified.

1. On Windows platforms start Eudora and double click on the message you received. On Unix platforms, start exmh, click on the message and click “Check Signature”.

2. The signer will be unknown as you do not yet have the new user’s public key in your keyfile.

Win95/NT: Import the new user’s public key into your PGP keyfile. Check the fingerprint, length and ID of the key with the details you have received out-of-band from the new user. If all is satisfactory you should then sign the user’s key by highlighting their key, clicking the right-hand mouse button and selecting “*sign*”**. You should click the checkbox allowing the signature to be exported**. You should then send a signed and encrypted email to the user with both your own public key (as Security Manager) and their public key, which has now been signed by you, in the message body.

Unix: Save the key to a file as described in Section 4.2.2 and type “pgp –ka filename” in order to start adding the user’s public key to your public keyring. Check the fingerprint, length and ID of the key with the details you received out-of-band from the new user. If all is satisfactory you should then sign the user’s key. Note that if you have more than one secret key on your keyring PGP may automatically select the wrong one. This can be avoided by using the command “pgp –ka filename –u myuserid” where the “-u” option specifies which secret key to use for signing. You should then send a signed and encrypted email to the user with both your own public key (as Security Manager) and their public key, which has now been signed by the Security Manager, in the message body. This procedure has been detailed in Section 4.2.2.1.

3. Add the user’s public key, signed by yourself, to the official web page at:

http://www.cs.ucl.ac.uk/research/ice-tel/pgpkeys

5.3 Final Steps for the User

You will now, assuming that the Security Manager is convinced of the validity of your key, receive an email from him that will contain your public key which he will have signed. This email will also contain the Security Manager's public key and will have been encrypted with your public key so that only you can decrypt it. You should perform the following steps:

- On Windows platforms start Eudora and double click on the message you received. With Unix select the relevant message in exmh and click "Show with PGP".

- The signer will be unknown, as you do not yet have the Security Manager's public key in your keyfile.

Win95/NT:

- Decrypt the message and import your own public key (now signed by the Security Manager) and the Security Manager's public key into your PGP keyfile.

- In the *PGPkeys* window your key should now have been signed by the Security Manager and the Security Manager's key should also be present. You should bring up the "*Key Properties*" window for the Security Manager's key and confirm the fingerprint, length and ID of the key with those in this document and/or on the official website.

- Once satisfied as to the validity of the Security Manager's key you should sign it with your own private key and set the trust to be "**trusted"** in the *"Key Properties*" window. If you wish you can select the checkbox allowing the signature to be exported but this is not necessary. The Security Manager's key is basic to the trust model currently used for the Secure Conferencing, as his signature will determine the validity of other people's keys.

Unix:

- Save your key, signed by the Security Manager, and the Security Manager's key to files. Then type "pgp –ka filename" where filename is the name of the file containing, firstly, the Security Manager's key and, secondly, your own key. This will add both keys to your public keyring.

- Start to sign the Security Manager's key by typing "*pgp –ks "Security Manager" –u myuserid*", where myuserid is the key you wish to use for signing, and follow the instructions. Check the fingerprint, length and ID of the Security Manager's key with those in this document and, once satisfied, complete the signing process. Note that the "-u" option is only necessary if you have more than one secret key in your secret keyfile.

- You should now set the trust of the Security Manager's key to be completely trusted by typing "pgp –ke "Security Manager"" and setting the trust level to "4". The Security Manager's key is basic to the trust model currently used for the Secure Conferencing, as his signature will determine the validity of other people's keys.

Your environment is now set up to take part in secure conferences. The steps needed to set-up and/or join groups and make full use of the secure conferencing software are detailed in the following sections.

6 Conference Groups

6.1 Creating a New Group (Conference Participant Manager Only)

In order to create a new conference group the following steps should be taken:

1. Send a signed and encrypted email to the Security Manager with the Subject "CPM Request". The body of the message should include the name of the group you wish to use.

2. The Security Manager will decrypt the message, verify your signature and confirm that you are allowed to become a Conference Participant Manager. Once satisfied he will send a signed and encrypted email to you containing the public keys of every user. These will all have been signed by the Security Manager.

3. Alternatively, these keys can all be obtained from the official website the details of which are given above. Verify that the message was signed by the Security Manager and import the necessary keys into your PGP keyfile.

4. The Security Manager needs to keep an email list of all Conference Participant Managers. This is in case a user's key is compromised as each group, which the user was a member of, has also to be assumed to have been compromised. Consequently, if such a situation arises, the Security Manager needs to be able to send out a signed and encrypted email to every Conference Participant Manager containing the user's details and, if possible, a replacement key for them.

5. Create a new PGP key pair for the group, it is probably a good idea to leave the emailid field blank.

Win95/NT:

6. Highlight the new key and click the right hand mouse button. From the menu which appears select "*Export*". **Make sure you click the checkbox to export the private key as well as the public key**. Save this key to a file.
7. The management of the group is handled via the Eudora address book. There is some group functionality within PGP 5.5.3i but this does not interface with Eudora easily. Set up a group as follows:

    - Open the Eudora address book (click on the button with a book on it)
    - Click *New* and type in the name of the group *e.g.* Group1
    - In the Addresses field type in the email addresses of any users you want to include in the group. Each should be on a new line and the email address must be exactly the same as in the angled brackets of their PGP key.

- A typical Eudora window showing the address book for a conference group is shown earlier in this document.

8. Create a new message in Eudora with the following fields:

    - Subject: “New Key for Group1”[4]
    - To: Group1

9. Click on the “*Attachment*” button (the one with a big paperclip) and select the file you exported the group key pair to.

10. Send the group key pair to all the members of the group in the following way:

    - Type the password *e.g.* “Group1 password is “this is the password”” in the body of the mail message.
    - Drag the public keys of all members of the group from the PGPkeys window to the message body window. **Remember to include your own public key.**
    - Send the message making sure that it is sent **encrypted and signed**.

Unix:

6. Extract the secret key to an ascii file by typing:

```
$ pgp –kxa “Group1” keyfile.asc .pgp/secring.pgp
```

7. The management of the group is handled via the exmh mh aliases list. Set up a group as follows:

    - Open the exmh mh alias list by clicking the “*Address/MH Aliases*” button
    - Type in a name for the group on the left *e.g.* group1
    - In the emailid field on the right type in the email addresses of any users you want to include in the group clicking the insert key after each one. The email address must be exactly the same as in the angled brackets of their PGP key.
    - Note that the PGP exmh preferences should be:
        - Always choose the sign key: ON
        - Cache map from email to public-key: persistent
    - PGP may try to use the environment variable LOCALHOST to complete the email addresses even if you have entered them fully. If this is set to the name of your local machine this may cause problems. If it does you should add a line similar to “setenv LOCALHOST cs.ucl.ac.uk” to your login script. Alternatively set “Cache map from email to public-key” to NONE.

8. Create a new message in exmh with the following fields:

    - Subject: “New Key for Group1”

---

[4] Insert the name of the Group here

- To: group1

9. Click on the "More/*Attachment/Attach File"* button and select the file you exported the private group key to.

10. Click on the "More/*Attachment/Attach PGP Keys"* button and select the public part of the group key pair.

11. Send the group key pair, together with all the members' public keys, to the members of the group in the following way:

    - Type the password *e.g.* "Group1 password is "this is the password"" in the body of the mail message.
    - Create an ascii pgp key file containing the keys of all members of the group as described in Section 4.2.2.1 and click on the "More/*Attachment/Attach File"* button and select this ascii keyfile. **Remember to include your own public key.**
    - Send the message making sure that it is sent **encrypted** and **signed.**

6.2 Becoming a member of a group

If you are being invited to become a member of a group you will be sent an encrypted email message containing the public keys of all other users who have been invited to join the group as well as the group private/public key pair. You should perform the following steps:

- On Windows start Eudora and double click on the message you received. On Unix start exmh and select the message you received.

- The signer will probably be unknown as you do not yet have the Conference Participant Manager's public key in your keyfile.

Win95/NT:

- Decrypt the message and you should have the option of importing a number of public keys including all the other members of the group as well as the group public key. Import all these keys to your keyfile.

- The email message will now have a line saying something like:
  Attachment Converted: "C:\Program Files\Eudora\Attach\group1.asc"

- In the *PGPkeys* window you should now see all the keys you have just imported. Note that the group key is not a key pair but simply the public part. In order to import the private part of the group key pair you should:

  - In *PGPkeys* click on "*Keys/Import*" and select the file from above
    i.e. *"C:\Program Files\Eudora\Attach\group1.asc"*
  - A box will pop up warning you that, as some of the keys are private, you will have to set the trust manually. Click "*OK*"
  - The "*Key Import*" box opens and you should import the group key pair.

- In the *PGPkeys* window you should check the details of the group key pair and, if satisfied, sign it and set the trust level to "*trusted*".
- Change the passphrase for the group private key to be the same as that of your own private key – this makes things easier for SDR.

A typical *PGPkeys* window for a user (Edmund Whelan) is shown earlier. Note that there are two key pairs – his own and one for Group1. Also note the public keys of several other users, some of whom will be in Group 1, and that all have been signed by the Security Manager's private key. The Security Manager's public key is present and has been checked and then signed by the user.

Unix:

- Decrypt the message and save the various keys to files. Import these keys into your pgp keyrings using "*pgp –ka filename keyring*". Take care to import the private group key to your secret keyring and the public group key to your public keyring.

- Use "pgp –ke group1" to edit the properties of the secret group key. You should set the level of trust to "4" and also change the password, which should have been included in the email message, to be the same as that of your own private key as this makes things easier for SDR.

7 Situations Which May Arise

It is assumed that you have set up a conference group called *Group1* and distributed the group public/private key pair.

7.1 New User Wants to Join An Existing Group

If a user wishes to join an existing group they should send a signed email to the Conference Participant Manager asking to be added to the group membership. Upon receipt of this email the Conference Participant Manager should:

1. Send a signed and encrypted email to the Security Manager requesting the new user's public key. The Security Manager will then email you a copy of the user's key signed with the Security Manager's private key allowing you to verify it. He will send this in an encrypted and signed email. This step should be done even if the user himself sends you a copy of his public key signed by the Security Manager's private key as the Security Manager may no longer consider the user's key to be valid. Import the user's key into your PGP keyring.

2. Alternatively you can download the user's key, again including the Security Manager's signature, from the official website.

3. Verify the message the user sent asking to be added to the group – this can only be done at this stage as you only now have a valid copy of the user's key signed by the Security Manager.

4. Add the user to the Group list in your Eudora Address book (on Win95/NT) or exmh alias list (Unix).

5. Email the existing group public/private key pair to the user remembering to include the passphrase in the body of the email. This email should be signed with your private key and encrypted with the public key of the new user. If all your secret keys are protected by the same passphrase you should change the passphrase associated with the group secret key either with the command “pgp –ke” on Unix platforms, or via PGPkeys on Windows, prior to extracting it to a file for sending. This will ensure that the security of your other private keys is not compromised.

6. You should also include the public keys of all members of the group, including yourself, in order to allow the new user to verify session announcements from any member of the group.

7. You should send the new user’s public key to all existing members of the group in order to allow them to verify any session announcements the new user may make. The “Subject” field should be something like “New member for Group1”.

7.2 User’s Key is Compromised

If a user’s private key is compromised then this also compromises any group keys they have access to. The following steps should be taken:

1. The user should take steps to fix the security breach and ensure it cannot occur again.

2. The user should generate a new key pair for him/herself.

3. The user should send a signed email to the Security Manager including his/her new public key as well as his/her old public key which is to be revoked.

4. The user should also send the fingerprint, ID and length of their new and old keys to the Security Manager out-of-band by fax or letter

5. The Security Manager will then remove the user’s old key from the website and email all Conference Participant Manager’s with the details of the old key which is no longer valid and include the new public key for the user signed by the Security Manager. This email should be signed and encrypted.

6. The Conference Participant Managers should check the membership of all the groups they manage and, if the compromised user is found to be a member, they should take the following steps:

   - Edit the group membership in your Eudora address book (on Win95/NT) or the exmh alias list (on Unix) and remove the relevant user.

   - Remove the existing group key pair from your PGP keyfile.

   - Create a new group key pair ensuring that the password is different to the old one.

Win95/NT:

- Export the new group key pair to a file. **Make sure you click the checkbox to export the private key as well as the public key**.

- Create a new message in Eudora with the following fields:

  - Subject: “Replacement Key for Group1”
  - To: Group1
  - In the body put a message saying the previous group1 key has been revoked and users should replace it with the one in this message together with the passphrase for the new group private.

- Click on the “*Attachment”* button (the one with a big paperclip) and select the file you exported the group key pair to.

- Send the group key pair to all the members of the group in an encrypted and signed message.

Unix:

- Export the private part of the new group key pair to a file.

- Create a new message in exmh with the following fields:

  - Subject: “Replacement Key for Group1”
  - To: Group1
  - In the body put a message saying the previous group1 key has been revoked and users should replace it with the one in this message together with the passphrase for the new group private.

- Click on the “*More/Attachment/Attach File”* button and select the file you exported the private group key to.

- Click on the “*More/Attachment/Attach PGP Keys*” button and select the new public group key.

- Send the group key pair to all the members of the group in an encrypted and signed message.

7. If you are an existing member of a group and receive such a message you should verify the message is genuine and then delete the revoked group key pair from your keyfile. Then follow the steps in Section 6.2 to become part of the “new” conference group.

All or some of the above steps may also be necessary for other reasons *e.g.* if a user leaves a company or it may simply no longer be suitable for a particular user to remain a member of a group. The initial point of contact should always be the Security Manager as he is the person who keeps details of all the keys and ensures they are valid. He is also in the best position to contact all the Conference Participant Managers.

8 Conclusion

This document should contain all the necessary information for users to set up and make use of secure videoconferencing on both Win95/NT and Unix platforms. However, the secure conferencing system is under continual development and you should ensure that you have the latest version of this document. It is hoped that secure key depositories will soon be available, using secure DNS and/or PGP keyservers, and changes such as this will be reflected in this document.

9 Changes from Previous Draft

- 1.1 Original draft
- 1.2 Added first draft of instructions for Unix platforms in addition to Win95/NT.
- 1.2a Added copyright notice and title page. Some clarifications and modifications. Background to Unix and Win95/NT changed to be different.