FUJ00232520

Document Title: **Customer Service Operational Change Procedure**

Document Type: Procedural

Release: N/A

Abstract: This document describes the procedure for Operational Changes where the changes are made to the live operation, only change the documented baseline when pre-authorised by CP, do not change the counter and are not covered by other processes e.g. the ICL Pathway Release Process.

Document Status: DRAFT

Author & Dept: Paul Curley, Customer Service

Contributors: Steve Parker

Reviewed By: Mik Peach
Steve Parker
John Simpkins
Mike Stewart

Comments By: 24th May 2000

Comments To: Document Controller & Author

Distribution: ICL Pathway Library, people who require approved versions only

FUJ00232520

0.0 Document Control

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/PinICL No.
0.1	20/8/99	First draft	

0.2 Approval Authorities

Name	Position	Signature	Date
M.Riddell	CS Operations Mgr		

0.3 Associated Documents

	Reference	Version	Date	Title	Source
1	ICL/PW/SM/PRO/003	1-Draft	5/8/99	ICL OSD – Pathway Operations Procedures	ICL OSD Service Mgt
2	TBA			CS Duty Manager procedures for OCP/Rs	ICL Pathway
3	CS/PRD/067	0.2	03/5/99	Operational Change Process	Customer Service

0.4 Abbreviations/Definitions

Abbreviation	Definition
CM	ICL Pathway Configuration Management
CP	ICL Pathway Change Proposal
CS	ICL Pathway Customer Service
OBC	Operational Business Change
OCP	Operational Change Proposal
OCR	Operational Corrections Request
OSD	ICL Pathway Operational Service Division
SSC	ICL Pathway System Service Centre (3rd line support)

FUJ00232520

0.5 Changes in this Version

Version	Changes
0.1	None this is the first draft

0.6 Changes Expected

Changes
•

FUJ00232520

0.7 Table of Contents

FUJ00232520

1 Introduction

This document describes the set up and use of PGP electronic signing keys. The document shows the user that has PGP software installed how to set up a key, define a key ring of other "signers" and how the signing operation will work within Customer Service.

2 PGP and Public Key Cryptography (Overview)

With PGP™, you can protect the privacy of your email messages and files by encrypting them so that only the intended recipients can read them. You can also digitally sign messages and files, which ensures their authenticity. A signed message verifies that the information within it has not been tampered with in any way.

PGP is based on a widely accepted encryption technology known as public key cryptography in which two complementary keys—a key pair—are used to maintain secure communications. To send someone a private email message, you use a copy of that person's public key to encrypt the information, which only they can decipher by using their private key. Conversely, when someone wants to send you encrypted mail, they use a copy of your public key to encrypt the data, which only you can decipher by using a copy of your private key.

You also use your private key to sign the email you send to others. The recipients can then use their copy of your public key to determine if you really sent the email and whether it has been altered while in transit. When someone sends you email with their digital signature, you use a copy of their public key to check the digital signature and to make sure that no one has tampered with the contents.

To use PGP, you must first create a key pair.

FUJ00232520

3 Getting started

You will need to have your email address handy as well as a “pass phrase”. This is just like a password only longer! Your pass phrase should contain multiple words and may include spaces, numbers, and punctuation characters. Choose something you can remember easily but that others won't be able to guess. **MAKE SURE THAT YOU REMEMBER THE PASSPHRASE – IF YOU DO NOT YOU HAVE TO GENERATE A NEW KEY FROM SCRATCH.**

You will also need to find somewhere to store a backup copy of your “keys” below is a **suggestion** for where they can be stored but you may wish to store somewhere more secure.

Select Windows NT explorer and set up a folder on your “M” drive called “keys”

To do this press “Start” bottom left hand corner of your screen

Select “programmes” from the first box

Select “Windows NT explorer” from the second box

Click on your “M” drive

From menu select “file” and the “new”

From next box select “folder” this creates a folder on your drive called “new folder” type “keys” to rename this folder.

4 Generating the key

The following process enables you to generate the key pair. The process is managed by a “key wizard” that walks you through each stage so just follow the screens.

Right click on the PGP icon (padlock) in the task bar (bottom right of your screen) to show the PGP menu.

Select the entry "**Launch PGPKeys**" and the key wizard will take you through the key generation screens, answer the questions as follows:

1. Read this screen, it contains some important information. Then press the NEXT button
2. Enter you name and email address as requested then press NEXT
3. Ensure the "Diffie-Hellman/DSS" key pair type box is selected and press NEXT
4. Ensure that “2048 bits (the default value)” is selected and press NEXT
5. Ensure "Key pair never expires" is selected and press NEXT
6. The Corporate Signing Key should read “PathwaySSC” just press NEXT
7. The Designated Revocation Key is also set up for “PathwaySSC” just press NEXT to proceed
8. Enter your Pass Phrase twice and press NEXT (remember this is case sensitive and is minimum 12 chars)

The wizard will now generate your key pair. Wait patiently for **“Complete”** to appear at the bottom of the box then press **NEXT**

FUJ00232520

The next page gives you the opportunity to send your new key to the keyserver. DO NOT send your key yet, it needs to be signed first (more of this later). Ensure that the "Send my key to the root server now" box is not checked and then press **NEXT**.

The key generation phase is now complete and you have your first key. Press **FINISH** and the PGP keys window will be displayed.

4.1 Taking a backup copy of your keys

Once you have generated a key pair, it is wise to put a copy of them in a safe place in case something happens to the originals.

Your private keys and your public keys are stored in separate keyring files, which you can copy just like any other files to another location on your hard drive or to a floppy disk. By default, the private keyring (secring.skr) and the public keyring (pubring.pkr) are stored along with the other program files on your hard disc in the folder **C:\Program Files\Network Associates\Pgp60\PGP Keyrings**, but you can save your backups in any location you like

PGP prompts you to save a backup copy when you close the PGPkeys application after creating a new key pair:

Select the new location into the box and press **SAVE**

As another security precaution, consider assigning a different name to your private keyring file and then storing it somewhere other than in the default PGP folder where it will not be so easy to locate. You use the Files pane of the PGPkeys Preferences dialog box to specify a name and location for your private and public keyring files.

FUJ00232520

5 Preparing the keys for use

Before you can use your key to sign documents, it must be countersigned by one of the trusted introducers within Pathway. This counter signature verifies that the PGP signature actually belongs to you. Once your signature has been verified, the trusted introducer will send your key onto the Pathway certificate server so that it is available to everybody within Pathway.

In order for a key to be held by the Pathway SSC certificate server, it MUST be signed as being valid by one of the trusted introducers, PGP is integrated with Microsoft outlook to make using its facilities easier.

If a key is sent to the certificate server without one of these signatures, it will be rejected.

To become registered simple send you public key to Steve Parker in the SSC.

5.1 Sending your key to another PGP user

Log into email and select open a "**NEW MAIL MESSAGE**"

Address the message to Steve Parker and entitle the email "**Your-name attached is my PGP key for signing**" and put a short message into the text box asking Steve to introduce your PGP key.

From the menu select "**PGP**" and then from the drop down menu, select "**Launch PGPkeys**

This display's the PGP keys screen, from this screen left click on your key eg paul.curley GRO and drag this into the message dialog text box this automatically attaches the key as a .asc file.

Open the PGP menu within outlook and select "**Sign now**".

Enter the **passphrase** for your key. PGP will then sign the mail item.

You will see the signature header at the beginning of your mail item and the actual signature value at the end. Once a mail item has been signed you should make NO more changes to the mail item.

Once the signature is present, simply **send** the mail item.

Whenever you send someone your public key, be sure to sign the email. That way, the recipient can verify your signature and be sure that no one has tampered with the information along the way.

When the Steve Parker receives your mail item he will: validate the signature, sign your signature and send it to the certificate server. Once this is complete Steve will return your email message and your keys have now been set up ready for use.

FUJ00232520

5.2 Enabling your key for use

Once you have set up your key you need to identify other people who are involved in the sign off process and register them on your key ring.

Therefore the next step is to set up your "key ring" to include the other people included in your sign off loop. The people on the CS Key Ring are listed below:

Janet Reynolds
Jean Woolley
Mik Peach
Steve Parker
John Simpkins
Mike Stewart
Mike Woolgar
Tony Wicks
Paul Curley
Dave Wilcox
John Wright
Dave Fletcher
Richard Brunskill
Deirdre Conniss

5.3 Finding keys for your key ring

To set these people of your key ring use the following process:

Click on the "padlock" icon in the taskbar and select **"LaunchPGPKeys**"

From the taskbar in the dialog box select "**Server"**

From drop down box select "**Search"**

This opens a further dialog box entitled "PGPKeys search window"

Tab down to the detail box next to the "contains" detail box and type in the surname of the first person on the above list "**Reynolds**" this will then search the server and return an entry for Janet Reynolds. Move the cursor down to Janet's name and "**right click"** your mouse **once** to select the entry.

The entry will then be highlighted "**left click"** the mouse and from the menu shown select "**Import to local Key ring**"

This then copies Janet's entry onto your key ring.

FUJ00232520

Repeat this process for all the names on the above list. (if any are missing and the sever fails to find the name - just ignore this and move onto the next name on the list. It means that they aren't registered yet).

6 Automatically getting keys

Once you have set up your initial list you can set the system to automatically update you if you receive a sign document with a key that is not known to your key ring. The following process explains how to set this up.

From the "**PGPKeys search window**" box and from the PGP keys window select "**Edit**" from the drop down box shown select "**Preferences…**"

This displays a preferences screen from the top tab select "Servers"

This displays the certification server – you need to tick the boxes marked "**Encrypting to unknown keys**" & " **Verification**" the press "**Ok**"

You are now ready to begin signing documents and emails and passing them onto the next signer.

7 Electronic signing process

Electronic signing will be used to "sign off" OCPs that are sent into Customer Service from OSD Service management. At this stage Customer Server authorisers will be asked to view the OCP document and electronically sign the mail item (Not the OCP) as authorisation.

An OCP is sent to the "**CSPathwayCP"** mailbox. The admin staff will annotate the email with the designated duty manager and "sign" the email the pass onto SSC.

The SCC manager will technically vet the OCP request and either reject and return to admin with the rejection reasons or approve and "sign" the email then pass onto the designated duty manager.

The designated duty manager will then assess the OCP operational and scheduling impact then either reject and return to admin or assess who else within Customer Service needs to approve the OCP and amend the email with the list of people requiring to approve the OCP. The designated duty manager will then approve and "sign" the email passing the email onto the next person for approval.

If the duty manager decides that no further approval is needed he will send the signed OCP back to admin and then OSD.

The approval (or rejection) process will then be continued by all the named people on the email list and then be returned to admin.

Admin will then return the approved OCP back to OSD Service Management.

FUJ00232520

The flow of OCP 's around Customer Service will always follow the same route. All OCP requests will initially be sent to admin who will then pass all OCPs onto SSC who will send to Duty Manager, The Duty Manager will send onto the Optional groups in order. Each group will send onto the next, the last one on the list will send back to Admin.

1. Admin (M)
2. SSC (M)
3. Duty Manager (M)
4. Operations (O)
5. Networks (O)
6. Business continuity (O)
7. Infrastructure (O)
8. Reference data (O)
9. Release management (O)
10. Reconciliation (O)
11. Admin (M)

M = Mandatory O = Optional

Admin will always be the first and the last to see the OCP, SSC and duty management must see ALL OCPs. any of the other Optional user groups may be asked to authorise an OCP depending on the nature and impact of OCP. The Duty Manager will decide which Optional group needs to see the OCP and annotate the email accordingly.

8 OCP turnaround target times

The following turnaround times are set as targets and include all the signatories involved.

Urgent – 2 hours

Routine – 8 hours

Janet and Jean will chase the OCP to ensure sign off but it is down to the individual to ensure that sign of is within the required timescale. Mandatory signers must regularly monitor their email for OCP's, Optional signatories will be told about the sign off by the Duty Manager.