



IPND Manager

Integrated Public Number Database (IPND)

IPND Data Users and Data Providers Access to Internet Interface Service (IIS)

Date: January 2018

Approved by: Tony Parker

Title: IPND Manager

Author(s): Logical Technologies Pty Ltd
Telephone: (03) 8643-6444
Fax: (03) 9670-9904
Application: Integrated Public Number Database

This publication has been prepared and written by Logical Technologies for Telstra Corporation Limited (CAN 051 775 556), and is copyright. Other than for the purposes of and subject to the conditions prescribed under the Copyright Act, no part of it may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission from the document controller. Product or company names are trademarks or registered trademarks of their respective holders.

Note for non-Telstra readers: The contents of this publication are subject to change without notice. All efforts have been made to ensure the accuracy of this publication. Notwithstanding, Telstra Corporation Limited does not assume responsibility for any errors nor for any consequences arising from any errors in this publication.

CONTENTS

Integrated Public Number Database (IPND)	1
1. Overview	4
Assumptions	4
Information provisioned by LogicalTech	4
Element	4
Purpose	4
Section(s) referred	4
Information to be provided to LogicalTech	5
Element	5
Purpose	5
Section(s) referred	5
2. VPN	6
Overview	6
Downloading VPN Configuration	6
Establishing a Tunnel	9
Checking the Tunnel	9
3. Authentication	12
Overview	12
Generating an SSH Key-Pair	12
Public Key	14
Using SSH Agent	14
SSH Access Configuration	15
4. Connecting	17
Overview	17
VPN	17
Environments	17
SSH Connection	17
SFTP (Linux Examples)	17
SCP (Linux Examples)	18
SCP and SFTP (Windows Environment)	18
Directories	21
5. File Encryption	23
Overview	23
GnuPG Key Pairs	23

Generating a gpg Key Pair	23
Using GNU Privacy Assistant	25
Managing your gpg key ring	26
Load the IPND Public key.....	26
Encrypting and Decrypting Files	28
6. Batch Processing.....	30
7. Messages.....	31
Error	31
Reason.....	31
8. References	32
9. Glossary	33
10. Appendix 1	34

1. OVERVIEW

This document describes how to establish a connection to the IPND Internet Interface Service (IIS). It details the technology required.

In order to ensure the confidentiality of the data uploaded and downloaded from the IPND the following measures will be deployed as part of the IIS:

- 1) VPN (SSL) tunnels
- 2) SSH Based file transfer tool with PKI for authentication.
- 3) Encryption of files using GnuPG (open source) tools also using PKI.

It is assumed that the user has applied and been authorised to become an IPND User by the IPND Manager according to defined processes. Refer to <https://www.telstra.com.au/consumer-advice/ipnd>

Assumptions

It has been assumed that Linux users will use command line options and Windows users will use GUIs (although command line options are available)

Filezilla and WinScp have been tested as transfer utilities.

GPG for Windows was used for GPG encryption and decryption.

The solution assumes that the use of OpenVPN will be allowed. In some cases it may be necessary to work with corporate network personnel to allow access.

Information provisioned by LogicalTech

The following table lists the information which will be provided to you for deployment purposes

Element	Purpose	Section(s) referred
OpenVPN Username and Password	Access to OpenVPN gateway	2 VPN
Comment details	Input into gpg-key pair	5 Generating a gpg Key Pair
IPND Public Key	Used to encrypt data sent to the IPND	5 Load the IPND Public key

Information to be provided to LogicalTech

The following table lists the information which you will send to LogicalTech for deployment purposes. You will need to send details to ipnd-support@logicaltech.com.au.

Element	Purpose	Section(s) referred
SSH Public Key	Enable SFTP and SCP access	3 Authentication
GPG Public Key	Enable encryption of files received from the IPND	5 Generating a gpg Key Pair

Overview

In order to reduce the risk profile associated with making sensitive data privately available over the internet access to the IIS will be enabled through TLS VPNs.

This section will describe how to download the configuration files needed to establish a tunnel to the IIS, how to establish a tunnel and how to check that the tunnel has been established.

Downloading VPN Configuration

Subsequent to being granted access to the IPND via the IIS the IPND support team will have provided an OpenVPN Username and Password. These will enable you to download the IIS VPN application and configuration files that are available from **gw1.ipnd.com.au**

Login with the OpenVPN Username and Password provided to you by the IPND Support Team, in the image below the label “user1” is used. Substitute your own credentials for this label.

When connecting initially use the login option as shown below:

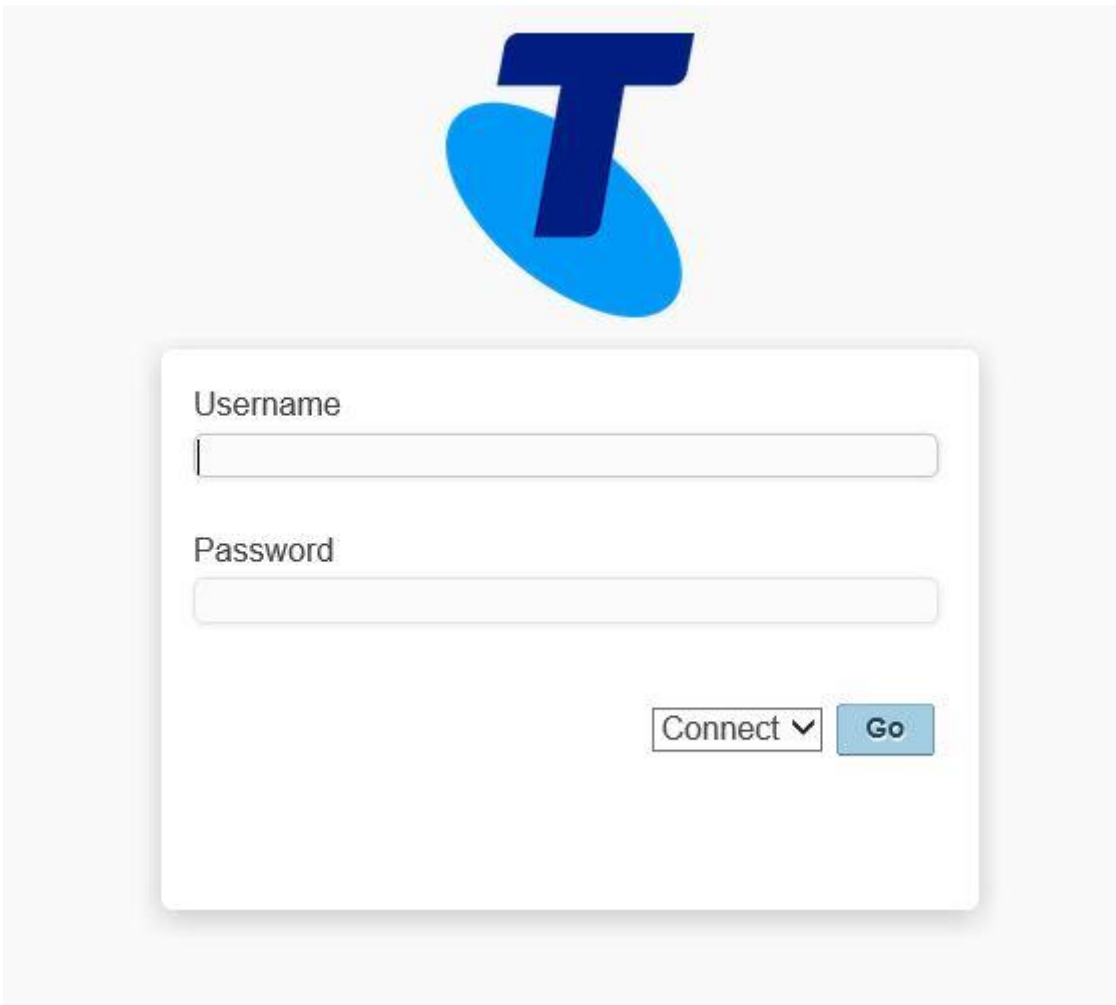


Image 1 - VPN Login Screen

After successfully logging in you will be presented with the following screen:



Image 2 VPN Download Screen

The links for downloading the OpenVPN Connect app will direct you to the appropriate download location for the client suited to your environment.

The Windows and OS X links will download a file (.msi or .dmg)

The Android and IOS links will take you the appropriate app stores. The Linux link will take you to additional instructions on how to deploy a Linux distribution OpenVPN client app.

The connection profiles section will enable you to download a `client.ovpn` configuration file that can be imported into pre deployed SSL clients.

The user-locked profile will require authentication with the password provided. The autologin profile allows the tunnel to be established without a password being entered to establish the tunnel.

Establishing a Tunnel

Invoke the SSL VPN Client as appropriate for your operating system.

An option to connect to gw.ipnd.com.au will be available. Select that option and establish a connection.

Linux Example

```
sudo openvpn --config client.ovpn
```

Windows Example

The Windows Installation of the OpenVPN client will install an icon in the tray or notification area.

To connect:

Right Click on the OpenVPN icon and select **gw.ipnd.com.au**

Then select **connect as <user1>** (where <user1> is the OpenVPN Username and Password assigned to you by the LogicalTech team)

Checking the Tunnel

The VPN tunnel will have been created in the form of a network interface. For examples see the screen shots below:

Linux Example

```
Ifconfig -a
```

```
tun0  Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
inet addr:10.10.120.6 P-t-P:10.10.120.6 Mask:255.255.255.0
inet6 addr: fe80::384c:ef9:668b:8cce/64 Scope:Link
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:0 (0.0 B) TX bytes:242 (242.0 B)
```

The above information shows that a virtual networks interface labelled tun0 that has been created by the TLS VPN software. It shows that the local IP address assigned to the interface is 10.10.120.6.

To ensure that data intended for the IIS is routed accordingly a routing table similar to the one displayed in the screen shot below should exist in your system.

```

netstat -nr
Kernel IP routing table
Destination  Gateway      Genmask      Flags MSS Window  irtt Iface
0.0.0.0      192.168.30.254 0.0.0.0      UG    0 0    0 enp0s25
10.10.110.9  10.10.120.1   255.255.255.255 UGH   0 0    0 tun0
10.10.110.17 10.10.120.1   255.255.255.255 UGH   0 0    0 tun0
10.10.110.18 10.10.120.1   255.255.255.255 UGH   0 0    0 tun0
10.10.110.26 10.10.120.1   255.255.255.255 UGH   0 0    0 tun0
10.10.120.0  0.0.0.0       255.255.255.0 U     0 0    0 tun0
10.10.120.0  10.10.120.1   255.255.254.0 UG    0 0    0 tun0
160.206.232.120 192.168.30.254 255.255.255.255 UGH   0 0    0 enp0s25
169.254.0.0  0.0.0.0       255.255.0.0  U     0 0    0 enp0s25
192.168.30.0 0.0.0.0       255.255.255.0 U     0 0    0 enp0s25

```

Windows Example

From a command window run the following command:

```
ipconfig /all
```

```

Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix . : 
Description . . . . . : TAP Adapter OAS NDIS 6.0
Physical Address. . . . . : 00-FF-FB-D5-BC-A1
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::2877:bd9:97af:f725%22(Preferred)
IPv4 Address. . . . . : 10.10.120.7(Preferred)
Subnet Mask . . . . . : 255.255.252.0
Default Gateway . . . . . : 10.10.120.1
DHCPv6 Iaid . . . . . : 369164283
DHCPv6 Client DUID. . . . . : 00-01-00-01-19-83-7D-79-00-15-5D-97-14-12
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                       fec0:0:0:ffff::2%1
                       fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled

```

Image 3 - VPN Tunnel Windows Example

The above information shows that a virtual networks interface labelled TAP Adapter has been created by the TLS VPN software. It shows that the local IP address assigned to the interface is 10.10.120.7

Check routing by running the following command from a command window:

```
netstat -rn
```

```

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.151.195  192.168.151.176  261
0.0.0.0                    0.0.0.0          10.10.120.1     10.10.120.7     121
10.10.110.8                255.255.255.255  10.10.120.1     10.10.120.7     121
10.10.119.0                255.255.255.0    10.10.120.1     10.10.120.7     121
10.10.120.0                255.255.252.0    On-link         10.10.120.7     276
10.10.120.7                255.255.255.255  On-link         10.10.120.7     276
10.10.123.255              255.255.255.255  On-link         10.10.120.7     276
127.0.0.0                  255.0.0.0        On-link         127.0.0.1       286

```

Image 4 - Routing Information - Windows Example

3. AUTHENTICATION

Overview

This section describes the steps required to gain access to the IIS File Transfer Service (FTS) using the SSH based scp and sftp applications. In order to minimise risk associated with password management SSH authentication is based on PKI using SSH key pairs.

SSH Key Pairs

SSH Keys are a means of identifying yourself to an SSH server using public-key cryptography.

Public-key cryptography, also known as asymmetric cryptography, is a class of cryptographic algorithms which requires two separate keys, one of which is secret (or private) and one of which is public. Together they are known as a key-pair.

Your Public Key must be provided to LogicalTech once generated. This will be used to register Data User or Data Provider access on the server.

Generating an SSH Key-Pair

Linux Example

To generate a SSH key pair you will need to use the following command:

```
cd ~/.ssh  
ssh-keygen -b 4048 -t ed25519 -f <user> -C <Organisation Name>
```

You will be prompted to provide a secure passphrase.

Note that unattended SSH sessions may be initiated without the need to authenticate each connection through the use of the ssh-agent utility. It is preferred that you use this approach. If you do not secure your secret key with a passphrase your access to the IPND may be compromised

The above command will generate a two key pair files as follows:

```
<user>.pub  
<user>
```

-t ed25519 specifies the key type. This is the preferred type of the options that are presented.

Note that key types RSA 1024 bits and DSA are no longer considered secure.

Your private and private keys should be deployed in the <user>/ssh directory in the user account you may be using.

Windows Example

In order to generate an SSH key pair you will need to download a tool such as PuTTYgen.



Run the PuTTYgen application by clicking on the icon

You will see a screen similar to this:

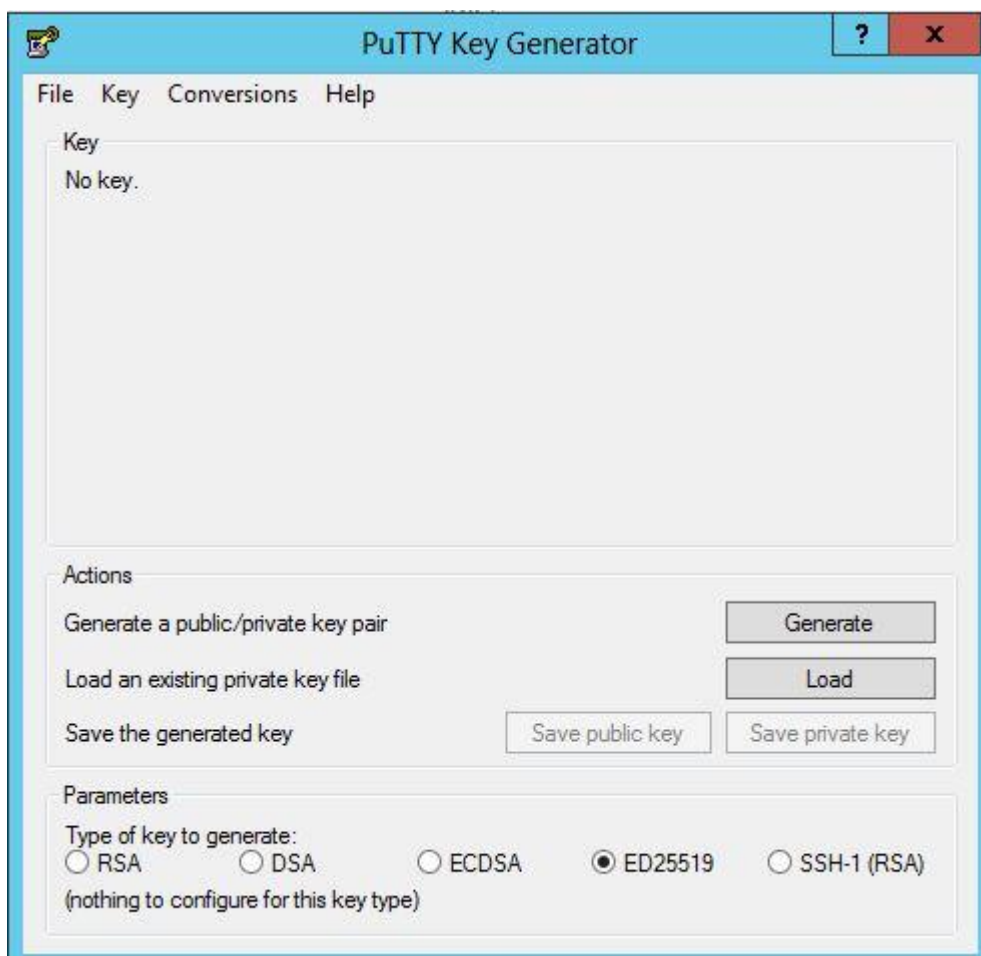


Image 5 - SSH Key Pair - Windows Example

You will need to select ED25519 as the key type – then click **Generate**

Save the public and private keys in a known location.

Public Key

Once you have your keys provide your public key (<user>.pub) to ipnd-support@logicaltech.com.au. You will be contacted to validate the key signature before it is deployed.

Using SSH Agent

In order to be able to access the IPND sftp/scp service you will need to authenticate using the private key that you generated in the above step.

This will require that you enter the passphrase associated with your private key. For an unattended batch system this could present a problem and it is therefore advised that the ssh-agent component be used to load the private key so that unattended batch transfers can take place.

ssh-agent acts like a trusted repository into which your private key can be loaded.

Linux Example

Run the program ssh-agent. You may need to do this as root.

This will produce output such as :

```
SSH_AUTH_SOCK=/var/folders/86/7kj3s11j57qgp72g9lcg_rb80000gn/T//ssh-APQFoXMiSuk/agent.53227; export SSH_AUTH_SOCK;  
SSH_AGENT_PID=53228; export SSH_AGENT_PID;  
echo Agent pid 53228;
```

Note - invoking ssh-agent with a “-t nnnn “ argument will set the default life time of the loaded key to nnnn. The omission of this parameter ensures that the key is loaded indefinitely.

This parameter can be overridden with a specific value for a specific key.

This information will provide the ssh-agent details that your process will require to connect to use the keys. The environment details will need to be made available in any environment that the scp/sftp connections are being used from.

Adding a key requires the invocation of the “ssh-add” command as follows:

```
ssh-add -t 300 .ssh/<testkey>
```

Will load the private key .ssh/<testkey> into ssh-agent for a duration of 300 seconds. You will be required to enter the passphrase to be able to load the key.

Windows Example

You will need to start the putty agent. The Pageant daemon will have been installed with your installation of PuTTYGen.

Start this up (right click) and add your ssh key.

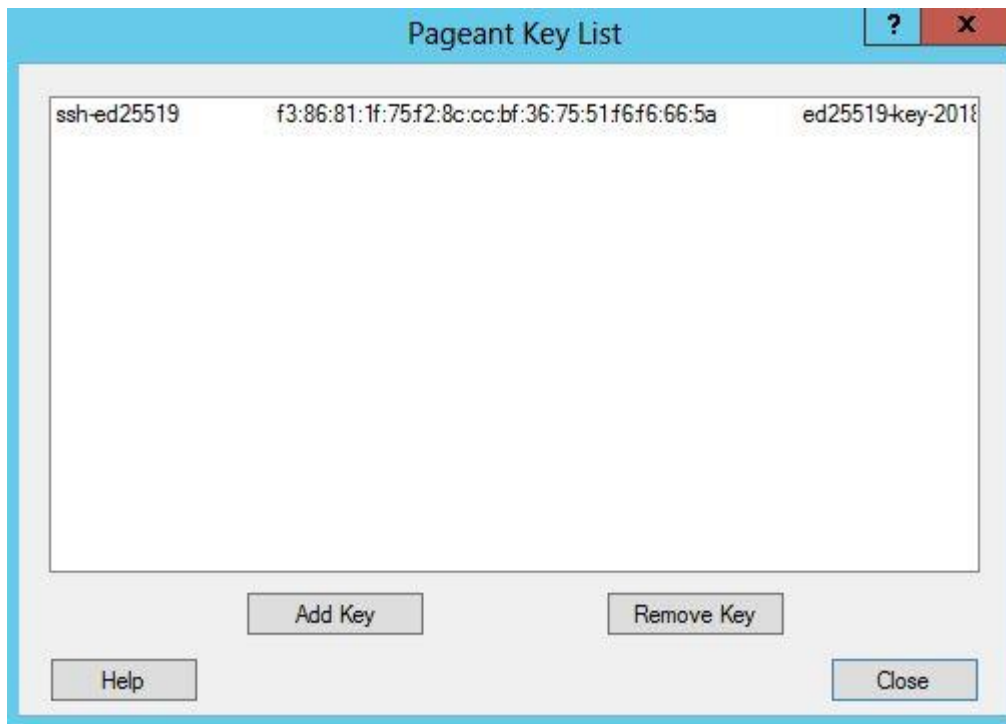


Image 6 - Puttygen - SSH Agent

SSH Access Configuration

Linux Example

In order to ensure that your connection to the IPND services are as seamless as possible ensure that your configuration details are specified in the `.ssh/config` file associated with the account from which you are transferring files to and from the IPND.

The format of the config file is as follows:

Production Service Example

```
host ipndfts-p
hostname 10.10.110.8
port 22
IdentityFile .ssh/<user_priv_key>
user <prod-user>
```

User Test Service Example

```
host ipndfts-t
hostname 10.10.110.8
```

```
port 22
IdentityFile .ssh/<user_priv_key>
user <test-user>
```

Windows Example

The configuration files for Windows' GUIs are stored as part of the Site details in the GUI setup.

4. CONNECTING

Overview

This section provides some background on, and describes how to connect to the IIS FTS.

VPN

Once you have established a VPN connection as described in the VPN section the tunnel may be left on. If dropped because of network interruptions you will need to re-connect to the IPND server.

Environments

The IIS provides FTS access to the core IPND Production and User Test environments. Refer to Appendix 1 for details of IP addresses etc.

SSH Connection

You will have the option of using two tools to connect to the IPND file transfer service. These are sftp and scp.

SFTP (Linux Examples)

When you invoke sftp you will have a similar interface to standard ftp, such as put, get etc.

Note SFTP is a better option to use when testing or connecting to the FTS interactively.

Note that you will not be allowed to upload files where the filename does not match the IPND file sources that have been associated with your user account.

For instance if you are an IPND Data Provider with a user account specified as “gentelco” that has been assigned the file source “gente” then it will only be possible to upload files that have the following format: IPNDUPGENTE.nnnnnn.asc

If you are an IPND Data User then you would be able to upload User Query Files (UQF) that would have the following format: IPNDQUIGENTE.yyyymmddhhmiss.asc

Note the “.asc” extension is created by the gnupg tools that will encrypt the data for transmission. Refer to the File Encryption section for the data encryption process. Files that have not been encrypted will not be accepted by the FTS.

SCP (Linux Examples)

scp provides an alternative mechanism to send and retrieve files from the IPND FTS services.

Note SCP is a better option to use in conjunction with automated batch process.

Assuming that the `.ssh/config` file has been set up as appropriate the syntax for uploading a file using scp as follows:

```
scp IPNDUPGENTE.0000001.asc ipndfts-p:
```

Where a file is being uploaded to the FTS production environment and the SSH configuration has been setup as described in the SSH Configuration section of this document.

The syntax for downloading a file using scp would be:

```
scp ipndfts-p:download/IPNDUPGENTE.0000001.err.asc
```

Note that this tool does not provide the same level of real time filename validation but nevertheless files that do not comply to the standards outlined above will be placed in a rejected Directory.

If the `.ssh/config` file has not been specified then the syntax would be as follows:

```
scp -i .ssh/<user_priv_key> IPNDUPGENTE.0000001.asc gentelco@ipndfts-p:
```

And for downloading a file would be:

```
scp i .ssh/<user_priv_key> gentelco@ipndfts-p:download/IPNDUPGENTE.0000001.err.asc
```

SCP and SFTP (Windows Environment)

You will need to install software that will allow SCP or SFTP connection.

WinSCP or Filezilla are example clients.

WinSCP configuration

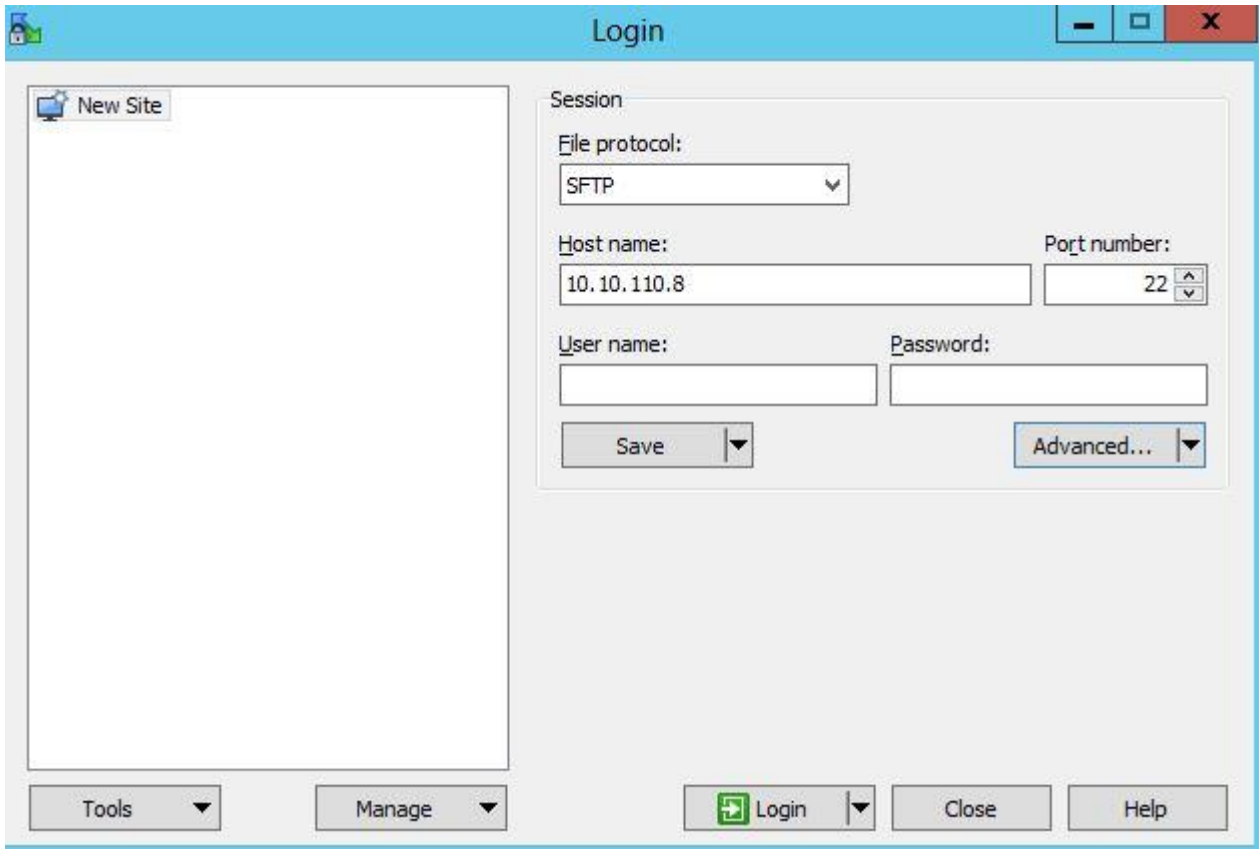


Image 7 WinSCP Configuration

Select the **Advanced** button

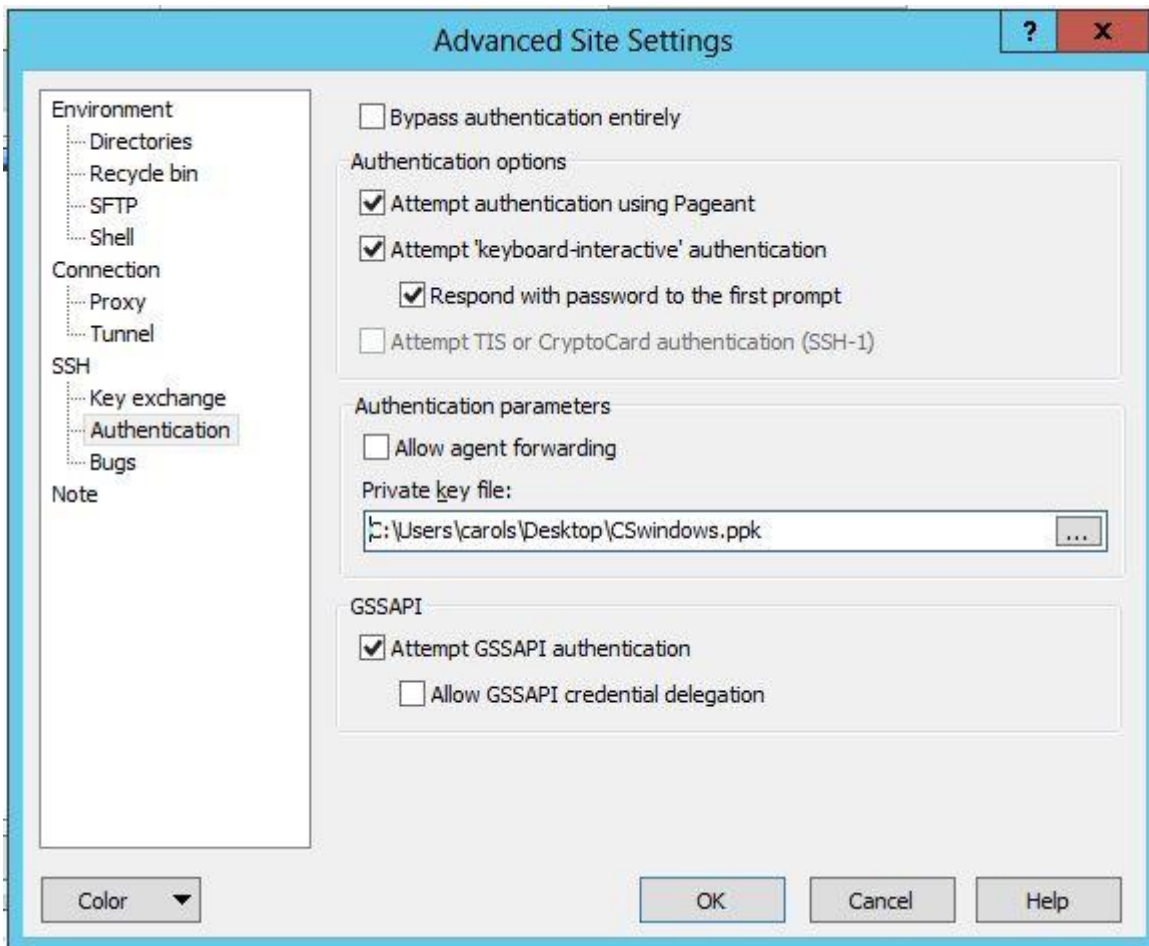


Image 8 - WinSCP - Site Settings

In the SSH Authentication section, select the private key you generated previously.

You can save the login for your organisation in the User name: input box.

Save the configuration as a name you will use again.

Click **Login** to log into the server.

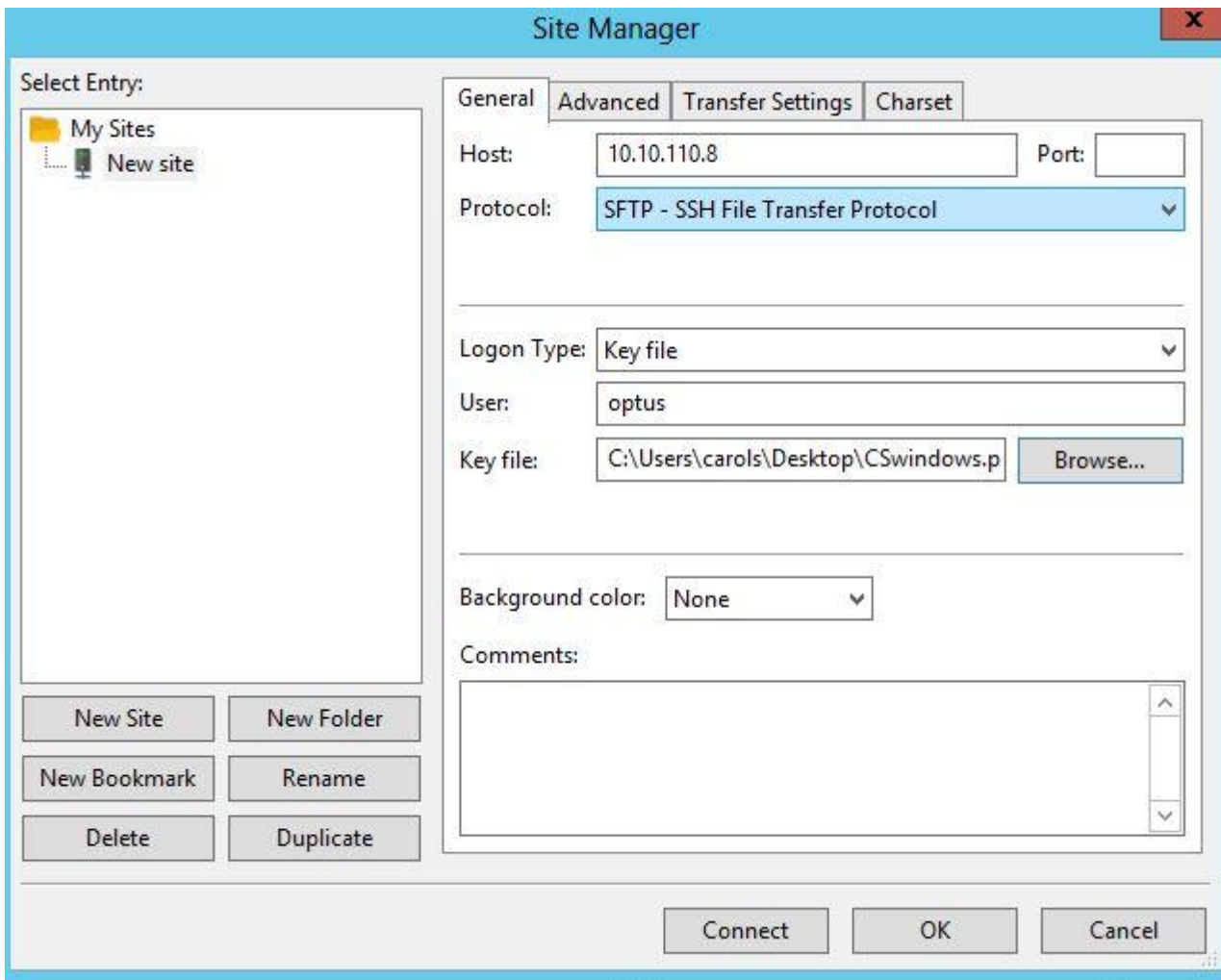


Image 9 - Filezilla Configuration

Create a new site.

Specify the IP Address

Specify the username provided for your organisation

Select **SFTP** as the Protocol

Select **Key File** in Logon Type.

In the Key File box, browse to the file that contains your SSH private key and add it.

Directories

There are three directories in each FTS environment, these are:

- archived
- download
- rejected

archived

This directory will contain those IPND files that are older than 30 days.

download

This directory will contain those IPND files that you may download.

rejected

This directory will contain any IPND files that are not valid because either:

- the filename does not comply with the specified valid filename associated with the user account,
- the file has not been encrypted.

Note: files can be uploaded to the user's home directory.

5. FILE ENCRYPTION

Overview

All files that are provided to and from the IPND via the IIS FTS will be encrypted using GnuPG

This section provides an overview on how to use the programs and utilities associated with this software.

GnuPG Key Pairs

GnuPG uses public-key cryptography so that users may communicate securely. In a public-key system, each user has a pair of keys consisting of a private key and a public key. A user's private key is kept secret; it need never be revealed. The public key may be given to anyone with whom the user wants to communicate. GnuPG uses a somewhat more sophisticated scheme in which a user has a primary keypair and then zero or more additional subordinate keypairs. The primary and subordinate keypairs are bundled to facilitate key management and the bundle can often be considered simply as one keypair

Generating a gpg Key Pair

This section describes how to generate a gpg key pair so that IPND files can be encrypted and decrypted.

Note: these should be created in the same environment in which IPND files are going to be sent/received from the IPND.

Your Public Key must be provided to LogicalTech once generated. This will be used to encrypt files you receive from the IPND. Please send the key to IPND-support@logicaltech.com.au.

Linux Example

To generate a gpg key pair run the following command on the CLI.

```
gpg --full-generate-key
```

This will result in the following be displayed:

```
Please select what kind of key you want:
(1) RSA and RSA (default)
(2) DSA and Elgamal
(3) DSA (sign only)
(4) RSA (sign only)
Your selection? 1
```

Select 1 as shown above. You will then be asked about keysize.

What keysize do you want? (2048) 4096

Select 2048 or 4096. You will then be asked about the lifetime or duration of the key.

Please specify how long the key should be valid.

0 = key does not expire

<n> = key expires in n days

<n>w = key expires in n weeks

<n>m = key expires in n months

<n>y = key expires in n years

Key is valid for? (0)

Select 0 to ensure that you do not need to renew the key.

You will then be asked to input your name, email address and Comment and to confirm that the information is ok.

Real name: Test User

Email address: test-user@org.com.au

Comment: Org

You will be provided with the information that needs to be added to the Comment field.

You will be requested to input a passphrase to protect your key - it is imperative that you specify a strong password or passphrase. After your passphrase has been typed in the keys will be created and stored in your key chain.

To check that your keys are loaded run the following command and check that the keys are displayed.

```
gpg --list-keys
```

Windows Example

You will need to install software that will allow you to generate GPG keys. You can review options at <https://www.gnupg.org/download/>

Using GNU Privacy Assistant

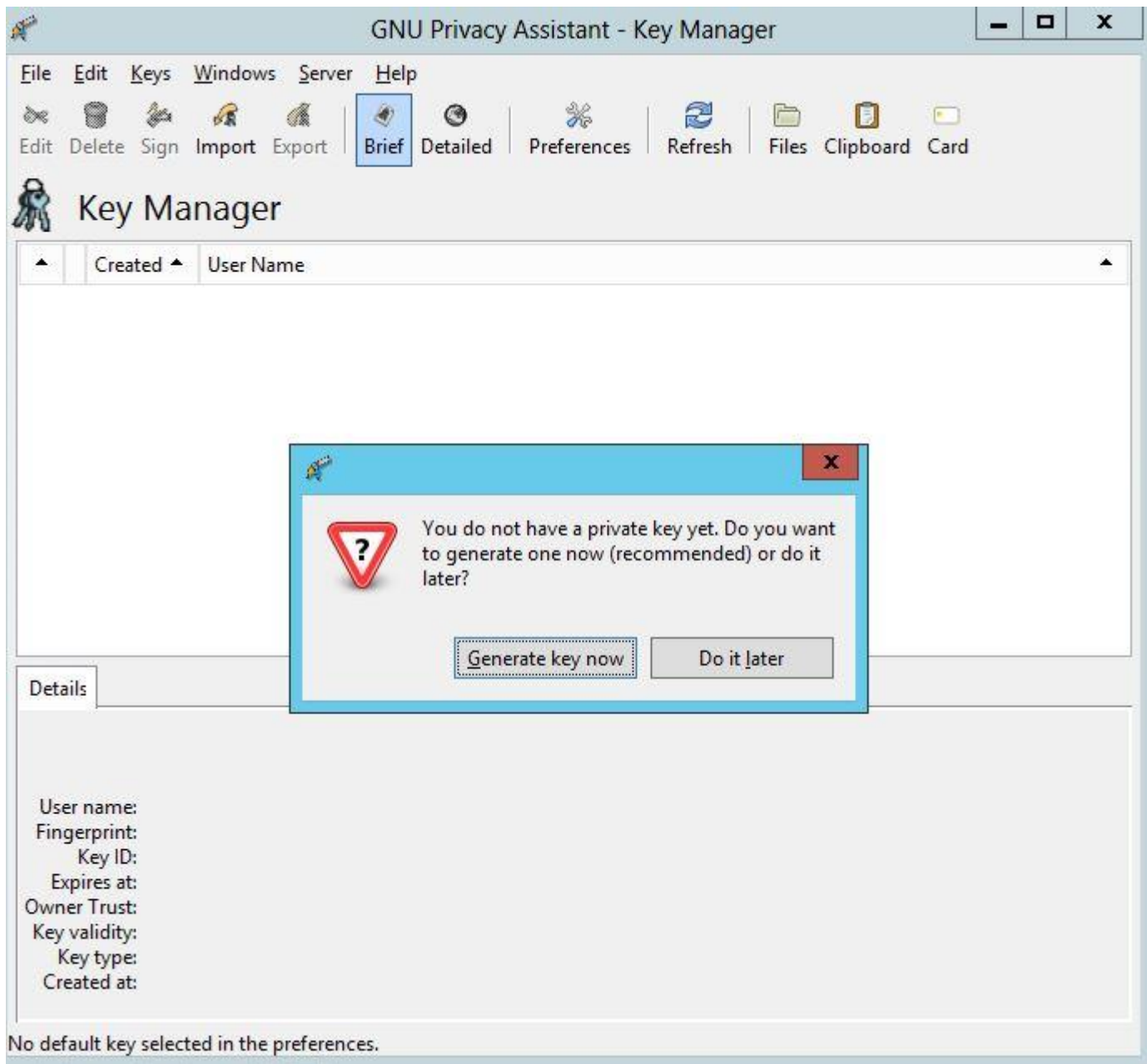


Image 10 - GNU Privacy Assistant - Generate Keys

You will be asked to input your name and email address.

You must enter the Comment provided by LogicalTech in the Comment field

You will also have the option to generate a passphrase.

Save a backup of the key.

Managing your gpg key ring

There are 3 main keys that you will need to manage:

- 1) Your secret key generated in the Generating a gpg Key Pair section outlined above.
- 2) Your public key also generated in the Generating a gpg Key Pair section outlined above (together 1 and 2 constitute a key-pair)
- 3) The IPND public key.

Your key pair will be stored in a gpg key ring.

Linux Environment

The keys created by you will have been added to your key ring when you created the key pair. You can verify this by running one of the following commands.

```
gpg --list-keys
gpg --list-secret-keys
gpg --list-public-keys
```

Load the IPND Public key

This key will have been provided to you by the IPND Support Team. To import into your key ring run the following command (it assumes the IPND Public key is named IPND-IIS-public.key)

Linux Environment

```
gpg --import IPND-IIS-public.key
```

Verify the fingerprint of the IPND IIS Public key.

```
gpg --fingerprint ipnd-operations@logicaltech.com.au
pub  rsa2048 2012-10-17 [SC]
    DFBA FA74 E2AB 64D6 C696 F24A 42CE 16EF 9281 E7B1
uid      [ full ] LT IPND <ipnd-operations@logicaltech.com.au>
sub  rsa2048 2012-10-17 [E]
```

Confirm with the LogicalTech team that the fingerprint is correct.

Set the trust of the IPND IIS Public key.

gpg —edit-key ipnd-operations@logicaltech.com.au

Type in “trust” in the CLI that is invoked and then select option 5 and then exit.

```
trust
 1 = I don't know or won't say
 2 = I do NOT trust
 3 = I trust marginally
 4 = I trust fully
 5 = I trust ultimately
 m = back to the main menu
```

Windows Environment

You will need to import the IPND Public Key provided to you by the IPND Support Team.

You can verify that the keys are loaded by using the GPA application gui.

To do this click on **keyring** in the main menu. The following screen will be displayed.

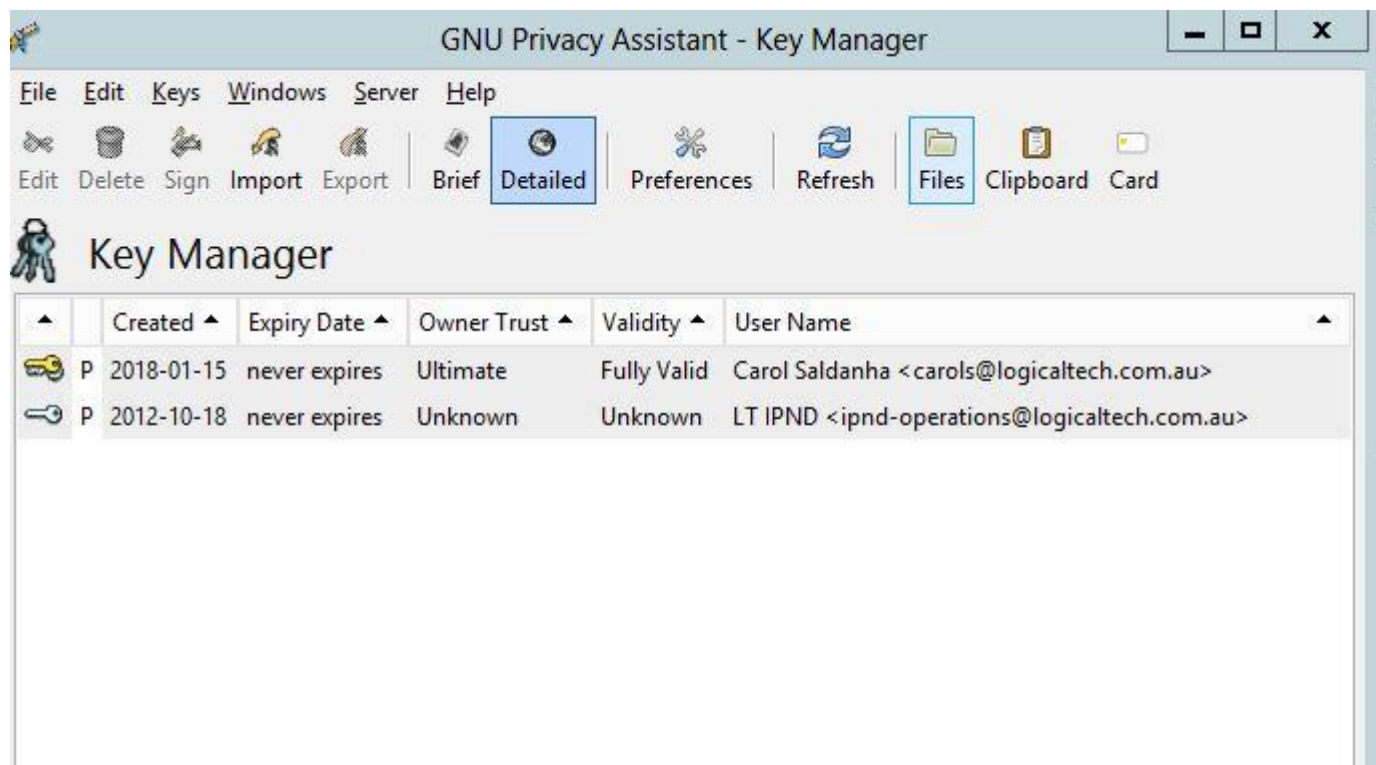


Image 11 - Importing Keys into Keyring

You will need to “trust” the IPND Public key. All files you receive will be “signed” with the IPND private key to prove it was generated by the IPND.

Trusting the IPND public key will allow the signature to be unencrypted.

Right click on the IPND key and click on “**Set Owner Trust**”

Encrypting and Decrypting Files

Linux Environment

Encrypting

Files that you upload to the IPND IIS will need to be encrypted using the IPND public key.

The command is:

```
gpg --batch --sign --encrypt --armor --recipient ipnd-operations@logicaltech.com.au  
IPNDUPGENTE.0000001
```

This will produce a file named IPNDUPGENTE.0000001.asc which will have been encrypted with the IPND IIS public key. The `--sign` option will also have signed the file with your private key.

Note: All files uploaded to the IPND IIS will need to be encrypted as described here.

Decrypting

All files that you download from the IPND IIS will have been encrypted using YOUR public key and will need to be decrypted using YOUR secret key.

To decrypt a file the command is:

```
gpg --batch --decrypt IPNDUPGENTE.0000001.001.err.asc
```

After running this command the file will be decrypted using your secret key and a plain text file called IPNDUPGENTE.0000001.001.err will have been created.

Windows Environment

Encrypting

Click on the **Files** menu option in the GNU Privacy Assistant GUI.

Select the file you want to encrypt e.g IPNDUPGENTE.0000001

Select the **Encrypt** menu option.

You will be presented with the options of which public keys to use to encrypt the file. Select the IPND public key.

You must also check the “armor” checkbox

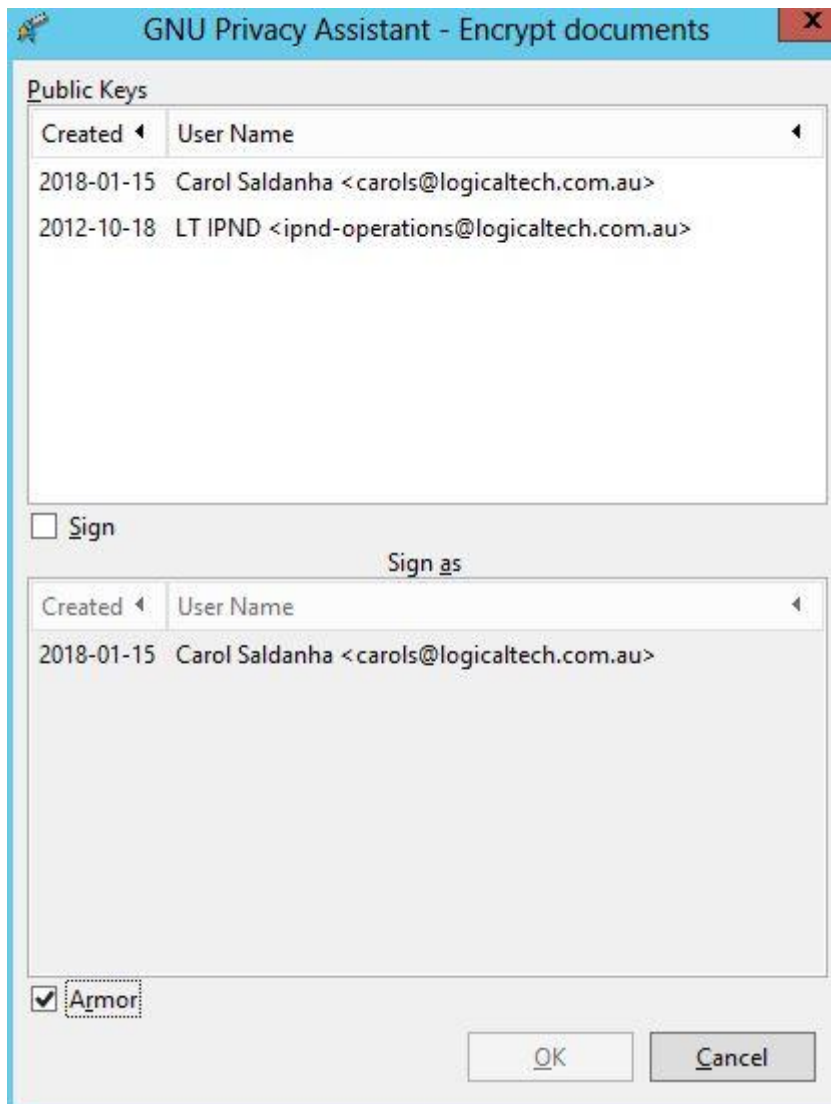


Image 12 - Encrypting Files

The resulting file will be called IPNDUPGENTE.0000001.asc

NOTE: the IPND will expect to receive an encrypted file with a “asc” extension. You must therefore select the “armor” option..

Decrypting

Click on the Files menu option in the GNU Privacy Assistant GUI.

Select the file you want to decrypt e.g IPNDUPGENTE.0000001.err.asc

Select the **decrypt** menu option.

Your private key should be used to decrypt the file you have downloaded.

6. BATCH PROCESSING

This section provides a brief overview of how to setup your environment to use gpg in a batch mode. This is an involved area and this information is provided as an initial aid.

Depending on your operating environment your secret key will be cached up by a gpg agent and you should only need to specify your secret key passphrase the first time.

It is possible to cache your secret key for a specified duration so that any batch processing can occur without requiring user input.

7. MESSAGES

Error Files will report success or failure of uploads as documented in the Data Users and Data Providers Technical Requirements document.

Files that are immediately rejected i.e not sent to the legacy IPND system, will be moved to the “rejected” directory with an error suffix. The error suffix will represent the first reason found for rejecting the file.

The table below documents rejected file errors:

Error	Reason
R001	File does not match valid file pattern
R002	File not valid for user type
R003	For IPNDUP/QU files, the FILESOURCE must be valid for user
R010	File must be encrypted
R020	File decryption failed
R100	Empty File
R200	File too large

8. REFERENCES

For detailed information on how to use the gnupg set of tools refer to:

<https://www.gnupg.org/documentation/manuals/gnupg.pdf>

9. GLOSSARY

Term	Description
IIS	Internet Interface Service
IPND	Integrated Public Number database
VPN	Virtual Private Network
SSH	Secure Shell
PKI	Public Key Infrastructure
TLS	Transport Layer Security
FTS	File Transfer Service
CLI	Command Line Interface
GPG	GNU Privacy Guard

10. APPENDIX 1

This page provides a summary of all the relevant information required.

FTS Production IP address	10.10.110.8
FTS User Test IP Address	10.10.110.8
FTS Production Username	"p_<user>"
FTS User Test Username	"t_<user>"