Integrated Public Number Database (IPND)

IPND Data Users, Data Providers & CSP Access to Internet Interface Service (IIS)

Date: Oct 2025

Vers: 2.03

Approved by: Penny Waite

Title: IPND Manager

Author(s):   LogicalTech Pty Ltd

Application: Integrated Public Number Database

Document Control

Version	Release Date	Written By	Reviewed By	Notes
1.9	30/11/2023	LogicalTech		IIS updates
2.0	29/01/2024	LogicalTech (The IPND Support team)		Document revised to integrate both command-line interface (CLI) and graphical user interface (GUI) functionalities within key sections. Additional trouble shooting added to relevant sections.
2.01	4/06/2024	LogicalTech		Include CLI GPG public key export example
2.02	May 2025	LogicalTech & IPND Manager		Consolidated DP, DU with CSP IIS Docs Updated OpenVPN sections to cater to Access Management changes
2.03	Oct 2025	LogicalTech & IPND Manager		Consolidated DP, DU with CSP IIS Docs Updated OpenVPN sections to cater to Access Management changes

Document Updates and Corrections

If you have identified any additional errors or have suggestions for improvement, we encourage you to share them with us. Your feedback is invaluable in helping us maintain the accuracy and quality of our documents.

To submit corrections or provide feedback, please email us at: IPND-Support@logicaltech.com.au

with the subject line "Document Errata - [Document Title] - [Version Number]." Include the page number, a brief description of the error, and the corrected information.

Thank you for your understanding and collaboration.

Table of Contents

General

General

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:

- VPN Secure Sockets Layer (SSL) tunnels
- SSH Based file transfer tool with Public Key Infrastructure (PKI) for authentication.
- Encryption of files using GnuPG (open source) tools also using PKI.

1.1. Assumptions

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

Linux/WSL Users predominantly utilize command-line options.

Windows Users predominantly utilise Graphic User Interfaces (GUIs).

Both Linux/WSL and Windows platforms support command-line options.

All CLI commands quoted in this document have been tested in both Windows CLI (PowerShell/CommandPrompt) and Linux/WSL, with differences highlighted where they occur to ensure compatibility.

FileZilla and WinSCP have been tested as file transfer utilities to ensure compatibility.

Windows Users utilise Kleopatra for GPG encryption and decryption tasks.

The IIS solution assumes the utilisation of OpenVPN Client.

Users may require the assistance of / coordination with their organisations IT / network personnel to enable User access or trouble shoot connection issues.

Important reminder: Maintaining / regular updating client utilities is the responsibility of all IPND Users.

Screenshots included in this document are indicative and appearance may change as client versions of Windows and Linux applications are updated.

1.1.1. User Toolsets

There are <u>three</u> essential toolsets for **Data Providers and Data Users (DPs / DUs)**:

    (1)   **OpenVPN Client:** For managing VPN connections.
    (2)   **SSH (Secure Shell) Suite:** For secure remote access and file transfer.
    (3)   **GPG (GNU Privacy Guard):** For encryption, decryption of files.

There are <u>two</u> essential toolsets for **Carriage Service Providers (CSPs)**:

    (1)   **OpenVPN Client:** For managing VPN connections.
    (2)   **GPG (GNU Privacy Guard):** For encryption, decryption of files.

The below is an overview of required toolsets for two environments:

- Command Line Interface (CLI), and
- Graphical User Interface (GUI).

The options include:

a) Linux/WSL for CLI,
b) Windows: PowerShell (PoSh) or CommandPrompt (CMD) for CLI, and
c) Windows Desktop for GUI.

Choose the environment suitable for your organisation from the options presented in the table, which includes details for CLI and Windows GUI.

Environment (CLI/GUI)	*Command Line Interface (CLI)*		*Graphical User Interface (GUI)*
Tools (1-3)	*a) Linux/Windows Subsystem for Linux (WSL)*	*b) Windows: PowerShell or CommandPrompt (CMD)*	*c) Windows Desktop*
(1) VPN Client **(Data Provider + Data User + CSP)**	openvpn	Not available (Must use GUI client)	OpenVPN Connect, OpenVPN GUI
(2) SSH (Secure Shell suite) **(Data Provider + Data User)**	ssh, scp, sftp, ssh-keygen, ssh-agent*, ssh-add*	ssh, scp, sftp, ssh-keygen, ssh-agent*, ssh-add*	PuTTY, WinSCP, FileZilla
(3) GPG (GNU Privacy Guard) **(Data Provider + Data User + CSP)**	gpg	gpg	Kleopatra

1.1.2. Installing the Toolsets in the user operating environment

The User is responsible for installation of their preferred operating environment.

1.1.2.1. CLI: LINUX, WSL

For Debian based systems:

```
Ubuntu 20.04.6 LTS. Installing (1) ssh, (2) gpg, (3) VPN client

sudo apt-get install openssh-client gnupg2 openvpn -y
```

For Red Hat based systems:

```
Red Hat Enterprise Linux release 8.5 (Ootpa). Installing (1) ssh, (2) gpg, (3) VPN client

sudo yum install openssh-clients gnupg2 openvpn -y
```

CLI: PowerShell, CommandPrompt:

    1.   VPN Client: Not Available, Use the Windows (GUI) option

2. Windows OpenSSH Suite: Open PowerShell as an administrator, then run:

As administrator: Windows PowerShell
Add-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0

3. GPG: Users will need to download (https://www.gpg4win.de/index.html) and run the GPG4Win installer. Deselect all selectable components (Okular, Kleopatra, GpgOL, GpgEX, Browser integration) leaving only the CLI GnuPG component.
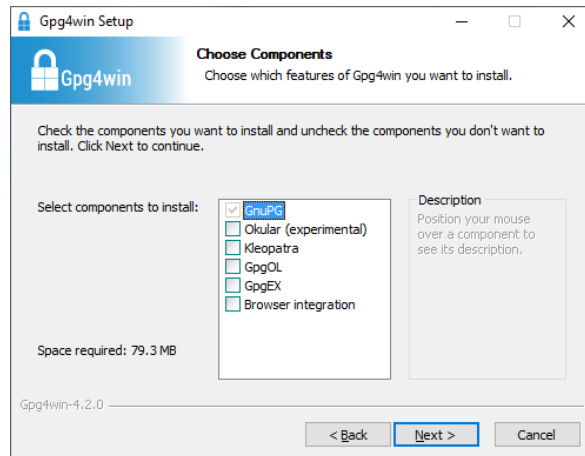
GPG4Win installer screen

1.1.2.2.   GUI: WINDOWS

1. OpenVPN Client: Download the either 1 of the 2 available Windows OpenVPN clients by following Section 3.3 or visit

   a)   https://openvpn.net/client/client-connect-vpn-for-windows/ (OpenVPN Connect)

   or

   b)   https://openvpn.net/community-downloads/ (OpenVPN GUI).

> Note: This guide refers to using OpenVPN Connect.
> OpenVPN Connect supports a single VPN connection at a time.
> OpenVPN GUI allows Users the ability to initiate multiple concurrent VPN connections to **different** servers using multiple profiles. Please note that concurrent logins with your IPND VPN configuration are forbidden. This restriction should be taken into account when planning **Disaster Recovery (DR)** or **High Availability (HA)** architectures.

2. SSH Suite: For the complete PuTTY suite, download MSI ('Windows Installer') from the putty developer's official web site below, or select the individual components required for download:

   putty.exe (the SSH and Telnet client itself)

   pscp.exe (an SCP client, i.e. command-line secure file copy)

   psftp.exe (an SFTP client, i.e. general file transfer sessions much like FTP)

   puttytel.exe (a Telnet-only client)

   plink.exe (a command-line interface to the PuTTY back ends)

   pageant.exe (an SSH authentication agent for PuTTY, PSCP, PSFTP, and Plink)

puttygen.exe (an RSA and DSA key generation utility)

pterm.exe (a PuTTY-style wrapper for Windows command prompts)

https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

⚠ Other download sites have been known to plant RATs (Remote Access Tools) into putty packages.

3. GPG: Download (https://www.gpg4win.de/index.html) and run the GPG4Win installer.
Install the default selectable components as shown below.
When the Installer completes it will launch Kleopatra.
Exit Kleopatra.

Note: Older versions of GPG4Win will also install GNU Privacy Assistant (GPA) which is an alternative program for managing certificates. The use of GNU Privacy Assistant (GPA) is no longer required and has been deprecated in this document.
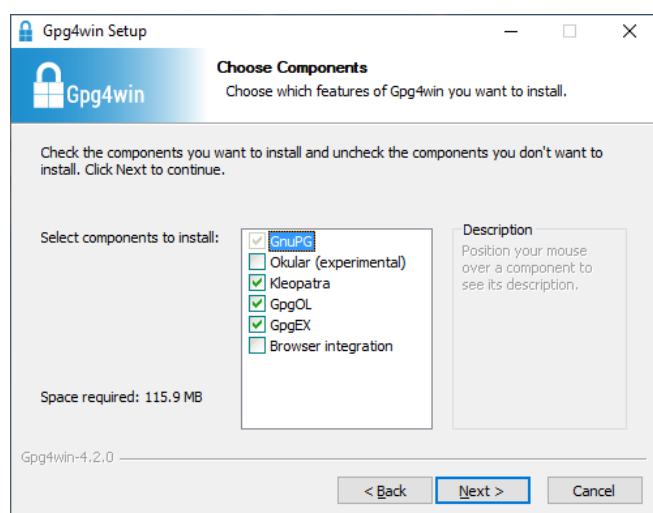
GPG4Win installer screen

1.1.3.   Updating Toolsets

It is the User's responsibility to ensure that the chosen tools are kept up to date (with the current version) to mitigate security risks and benefit from performance improvements.

1.2.   Information provided to Users by the IPND Support team

The following table includes the information provided to Users for User Setup:

Element	Purpose	Section(s) referred
OpenVPN Profile	Access to OpenVPN gateway	2.3 Downloading VPN Profile and OpenVPN Client
IPND Public Key	Encrypt data sent to the IPND	4.4 Import, Fingerprint and trust the IPND Public GPG key
Comment details (optional)	Input into GPG-key pair	4.3 Creating a GPG key pair, Finger Printing, Exporting

1.3.   Information Users must provide the IPND Support team

The following table includes the information Users are required to send to the IPND Support team for User Setup, via email:

General

Element	Purpose	Section(s) referred
SSH Public Key	Enable SFTP access	3-SSH KEY PAIRS
GPG Public Key	Enable encryption of files received from the IPND	4-GPG KEY PAIRS

1.4.   Additional Information

The following table includes additional information that will need to be verified.

This **must not** be done via email. Users will be contacted by the IPND Support team to verbally verify fingerprints.

Element	Purpose	Section(s) referred
Key Fingerprints	Key fingerprints will need to be **verbally** verified.	Appendix 1 – Fingerprints

2.VPN: (ALL USERS) DATA PROVIDER + DATA USER + CSP

2.1. Overview

To mitigate the risks linked to exposing sensitive data over the internet, access to the IIS will be granted exclusively through VPNs.

This section provides Users the steps required to:

- Download User VPN Profile;
- Establish a VPN tunnel;
- Check that the VPN tunnel has been established successfully.

Note: The VPN Profile includes the Fully Qualified Domain Name (FQDN) URI necessary for establishing the VPN tunnel.

Organizations enforcing firewall restrictions or access controls must use this FQDN instead of a fixed IP address.

The correct DNS resolution for this URI is critical for the IPND VPN server's high-availability setup. In the event of a failover to a new instance, the IP address will change.

Any User who has hard coded the IP address will be unable to connect to the new instance post-failover.

Please also be aware that **future VPN configuration files may use a different URI/FQDN** as part of ongoing improvements or infrastructure changes. Ensure your systems and firewall rules are flexible enough to accommodate such updates.

2.2. VPN Settings

VPN Settings are included in the VPN Profile download as explained in the following section.

More information is included in APPENDIX 2: OPENVPN CONFIGURATION FILE EXAMPLE.

2.3. Downloading VPN Profile and OpenVPN Client(s)

2.3.1. Obtaining and downloading User IPND OpenVPN Profile

When Users are granted access to the IPND by the IPND Manager, they receive an email from the IPND with further instructions.

The email contains a link to an IPND Provisioning page along with instructions for download and installation of the OpenVPN Client.

To access the IPND Provisioning page, Users must click on the link in the email, or copy the Request ID from the email and access the IPND Provisioning page: https://provisioning.ipnd.com.au

If the User details on the IPND Provisioning page are correct, the User confirms by clicking on the 'Send Verification Code' button.

If the User details on the IPND Provisioning page are incorrect, please contact the IPND Manager immediately: IPND.Manager@team.telstra.com

Once the User clicks on 'Send Verification Code', two things will occur:

1. The User will receive an SMS to their nominated mobile number containing a Verification Code;
2. The IPND Provisioning page will expand to include a field for the User to enter the Verification Code received from the sms.

IPND - VPN Provisioning

OpenVPN Profile Download

Use the form below to request a verification code to your registered phone number. Contact the IPND Manager if any of the listed details are incorrect

VPN Username

telco

Verification Phone Number

+61xxxxxx123

Organisation

Telco Australia

Send Verification Code

Documentation

IPND Data Users and Data Providers Access to IIS

IPND Manager

IPND.Manager@team.telstra.com

Once the correct Verification Code is entered the 'Download' button will become available for the User to Download the OpenVPN Profile.

The download button will remain inactive until the correct Verification Code is entered.

IPND - VPN Provisioning

OpenVPN Profile Download

Contact the IPND Manager if any of the details listed below are incorrect

VPN Username

telco

Verification Phone Number

+61xxxxxx123

Organisation

Telco Australia

Enter the verification code that was sent to +61xxxxxx123 . The download will begin immediately

Verification Code

Verification Code

Download

Please note:
- The Download link is valid for **7 days**.
- The VPN Profile can be downloaded **only once**.

IPND - VPN Provisioning

ⓘ Download Success

Your download with begin automatically

OpenVPN Profile Download

VPN Username

> telco

Verification Phone Number

> +61xxxxxx123

Organisation

> Telco Australia

2.3.2. Downloading a VPN Client Application

The email includes links to versions of the **OpenVPN client** for Windows, macOS, and Linux that have been **tested and verified** to work with the current IPND VPN server.

Please note: while newer versions of the OpenVPN client may be available, we recommend using the provided versions to ensure compatibility with the current release of the IPND VPN setup.

2.4. Establishing a VPN Tunnel

2.4.1. Pre VPN Client Installation DNS resolution check

It is recommended that Users confirm that the DNS resolution of the VPN Profile URI is working. APPENDIX 2: OPENVPN CONFIGURATION FILE EXAMPLE

Do NOT edit your VPN Profile to use a fixed IP address.

2.4.2. CLI: Linux, WSL, PowerShell, CommandPrompt

To test local DNS resolution run:

```
Linux terminal, Windows PowerShell or Windows CommandPrompt Pre start VPN
checks

## Test your default DNS resolution

    nslookup gw1.ipnd.com.au
    # You will get something like the following back

    Server:         <Your DNS Server Name>
    Address:        <Your DNS Server IP>
    Non-authoritative answer:
    Name: gw1.ipnd.com.au
    Address: <Current IP of gw1 server>
```

If local DNS resolution fails, then test external resolution by running:

```
Linux terminal, Windows PowerShell or Windows CommandPrompt Pre start VPN
checks

## Test external server DNS resolution via Google's Public DNS (8.8.8.8)
```

```
nslookup gw1.ipnd.com.au 8.8.8.8
# You will get something like the following back


Server:        8.8.8.8
Address:       8.8.8.8#53
Non-authoritative answer:
Name: gw1.ipnd.com.au
Address: <Current IP of gw1 server>
```

Please consult your Network Support Team to resolve any DNS resolution issues.

2.4.3.   GUI: Windows

A GUI check is not available. Users must use the CLI option(s) above.

2.4.4.   Starting the VPN Client

2.4.4.1.   CLI: Linux, WSL example

```
Linux/WSL Initial VPN Tunnel Test

## This initial Test will only exit if there is a problem or when you press ^C
sudo openvpn -- config client.ovpn
## You should see something like the following ##
Tue Jan 23 21:07:45 2024 OpenVPN 2.4.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4]
[EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Apr 28 2021
Tue Jan 23 21:07:45 2024 library versions: OpenSSL 1.1.1d  10 Sep 2019, LZO 2.10
..
Tue Jan 23 21:07:57 2024 /sbin/ip route add 54.79.164.151/32 via 192.168.4.1
Tue Jan 23 21:07:57 2024 /sbin/ip route add 10.10.110.8/32 metric 101 via 10.10.xxx.1
Tue Jan 23 21:07:57 2024 /sbin/ip route add 10.10.110.31/32 metric 101 via 10.10.xxx.1
Tue Jan 23 21:07:57 2024 /sbin/ip route add 10.11.50.12/32 metric 101 via 10.10.xxx.1
Tue Jan 23 21:07:57 2024 /sbin/ip route add 10.11.110.8/32 metric 101 via 10.10.xxx.1
Tue Jan 23 21:07:57 2024 /sbin/ip route add 10.10.119.0/24 metric 101 via 10.10.xxx.1
Tue Jan 23 21:07:57 2024 Initialization Sequence Completed
^C
Tue Jan 23 21:13:39 2024 event_wait : Interrupted system call (code=4)
Tue Jan 23 21:13:39 2024 SIGTERM received, sending exit notification to peer
Tue Jan 23 21:13:40 2024 /sbin/ip route del 10.10.110.8/32 metric 101
Tue Jan 23 21:13:40 2024 /sbin/ip route del 10.10.110.31/32 metric 101
Tue Jan 23 21:13:40 2024 /sbin/ip route del 10.11.50.12/32 metric 101
Tue Jan 23 21:13:40 2024 /sbin/ip route del 10.11.110.8/32 metric 101
Tue Jan 23 21:13:40 2024 /sbin/ip route del 10.10.119.0/24 metric 101
Tue Jan 23 21:13:40 2024 /sbin/ip route del 54.79.164.151/32
Tue Jan 23 21:13:40 2024 Closing TUN/TAP interface
Tue Jan 23 21:13:40 2024 /sbin/ip addr del dev tun0 10.10.xxx.yyy/22
Tue Jan 23 21:13:40 2024 SIGTERM[soft,exit-with-notification] received, process exiting
```

2.4.4.2.   GUI: OpenVPN GUI/Connect

Upon completion of installation of the OpenVPN client, Users will see a desktop icon and an app icon in their notification area.

1.   To import the OpenVPN Profile, right click on the OpenVPN Connect icon and select: Import Profile
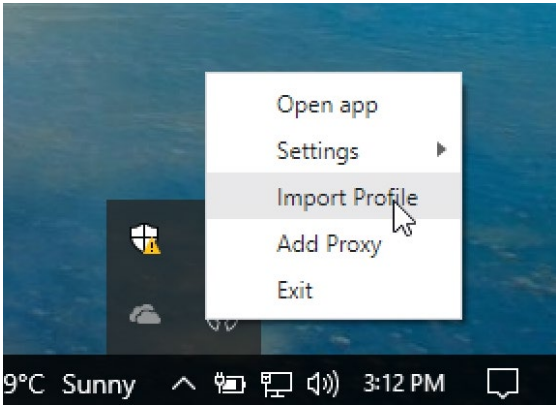
Users will be prompted to BROWSE and select their OpenVPN Profile by clicking Open:
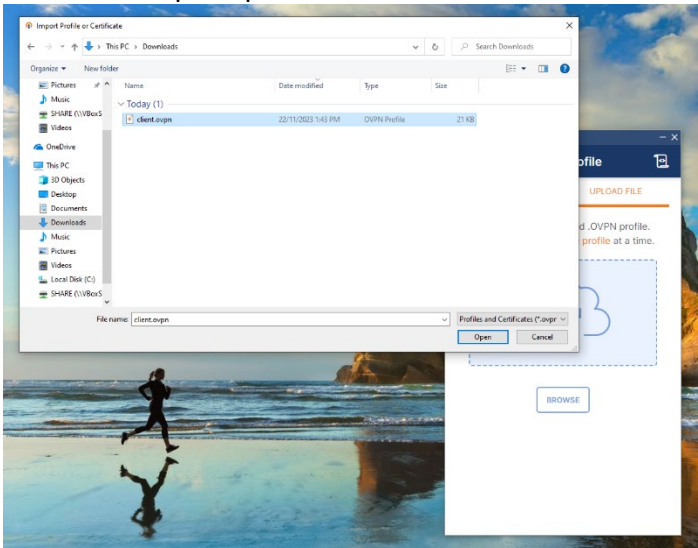
Once the OpenVPN Profile is imported, the User must click on either 'PROFILES' (to save and return to main app page) or 'CONNECT' to save the OpenVPN Profile. Clicking the back arrow causes the OpenVPN Profile to be un-saved.
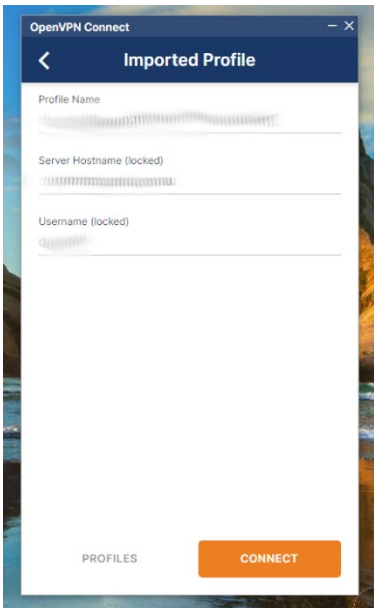
2.   To connect

When back on the main app page simple click on button near the top left to connect.
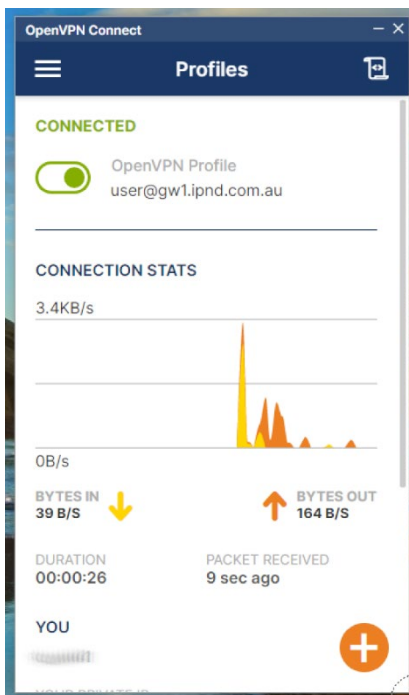
OpenVPN Client – Connected

General

2.5. Checking the Tunnel

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

2.5.1. CLI: Linux, WSL

```
Linux/WSL daemon test / checking tun device

sudo openvpn -- config client.ovpn --daemon
## The command should return to your shell prompt with no error messages


## Check the Network VPN tun device
ifconfig -a
## or
ip a s
..

..

<n>: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
UNKNOWN group default qlen 100
    link/none
    inet 10.10.xxx.yyy/22 brd 10.10.123.255 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::f178:9f76:d8c4:db75/64 scope link stable-privacy
       valid_lft forever preferred_lft forever


## Checking Routing
netstat -nr
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         <yourgatewayip> 0.0.0.0         UG        0 0          0 enp0s25
10.10.110.9     10.10.xxx.1     255.255.255.255 UGH       0 0          0 tun0
10.10.110.17    10.10.xxx.1     255.255.255.255 UGH       0 0          0 tun0
10.10.110.18    10.10.xxx.1     255.255.255.255 UGH       0 0          0 tun0
10.10.110.26    10.10.xxx.1     255.255.255.255 UGH       0 0          0 tun0
10.10.xxx.0     0.0.0.0         255.255.255.0   U         0 0          0 tun0
10.10.xxx.0     10.10.xxx.1     255.255.254.0   UG        0 0          0 tun0

..
```

The above information shows that a virtual networks interface labelled tun0 has been created by the 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 Users should have a routing table like the one displayed above.

2.5.2. CLI: PowerShell

Open a Windows PowerShell as a standard User.

- Check VPN network interface:

```
Windows PowerShell - Checking VPN tun/tap device

## Run the following command

Get-NetAdapter | Where-Object { $_.InterfaceDescription -like "*TAP*" -or $_.InterfaceDescription
-like "*TUN*" } | Format-Table -AutoSize


## You should see something like


## If you have installed OpenVPN Connect
Name                     InterfaceDescription                     ifIndex Status   MacAddress         LinkSpeed
----                     --------------------                     ------- ------   ----------         ---------
..
Local Area Connection TAP-Windows Adapter V9 for OpenVPN Connect    18 Up          00-FF-D8-1A-97-1E   1 Gbps
..


## If you have installed OpenVPN GUI

Name                     InterfaceDescription                     ifIndex Status   MacAddress         LinkSpeed
----                     --------------------                     ------- ------   ----------         ---------
..
OpenVPN TAP-Windows6  TAP-Windows Adapter V9                          4 Up          00-FF-0D-53-86-19   1 Gbps
..
```

- Check VPN Network details:

Windows PowerShell - Checking VPN network details

If you have installed OpenVPN Connect
Ensure you copy/use the **InterfaceDescription** from the previous command in the "" quotes

```
Get-NetAdapter | Where-Object { $_.InterfaceDescription -eq "TAP-Windows Adapter V9 for OpenVPN Connect" } | Get-
NetIPAddress

IPAddress          : fe80::5112:910d:d77c:e26a%18
InterfaceIndex     : 18
InterfaceAlias     : Local Area Connection
AddressFamily      : IPv6
Type               : Unicast
PrefixLength       : 64
PrefixOrigin       : WellKnown
SuffixOrigin       : Link
AddressState       : Preferred
ValidLifetime      : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime  : Infinite ([TimeSpan]::MaxValue)
SkipAsSource       : False
PolicyStore        : ActiveStore

IPAddress          : 10.10.xxx.yyy
InterfaceIndex     : 18
InterfaceAlias     : Local Area Connection
AddressFamily      : IPv4
Type               : Unicast
PrefixLength       : 22
PrefixOrigin       : Manual
SuffixOrigin       : Manual
AddressState       : Preferred
ValidLifetime      : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime  : Infinite ([TimeSpan]::MaxValue)
SkipAsSource       : False
PolicyStore        : ActiveStore
```

If you have installed OpenVPN GUI
Ensure you copy/use the **InterfaceDescription** from the previous command in the "" quotes

```
Get-NetAdapter | Where-Object { $_.InterfaceDescription -eq "TAP-Windows Adapter V9" } | Get-NetIPAddress

IPAddress          : fe80::cc4a:f658:6a3f:8c61%4
InterfaceIndex     : 4
InterfaceAlias     : OpenVPN TAP-Windows6
AddressFamily      : IPv6
Type               : Unicast
PrefixLength       : 64
PrefixOrigin       : WellKnown
SuffixOrigin       : Link
AddressState       : Preferred
ValidLifetime      : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime  : Infinite ([TimeSpan]::MaxValue)
SkipAsSource       : False
PolicyStore        : ActiveStore

IPAddress          : 10.10.xxx.yyy
InterfaceIndex     : 4
InterfaceAlias     : OpenVPN TAP-Windows6
AddressFamily      : IPv4
Type               : Unicast
PrefixLength       : 22
PrefixOrigin       : Dhcp
SuffixOrigin       : Dhcp
AddressState       : Preferred
ValidLifetime      : 364.23:57:00
PreferredLifetime  : 364.23:57:00
SkipAsSource       : False
PolicyStore        : ActiveStore
```

- Check routing by running the following command from a PowerShell or CommandPrompt:

Windows PowerShell - Checking VPN network routing

```
## Run the following to check network routing

Netstat -nr

..


IPv4 Route Table

===========================================================================

Active Routes:

Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0       10.0.2.2       10.0.2.15     25
         10.0.2.0    255.255.255.0       On-link        10.0.2.15    281
        10.0.2.15  255.255.255.255       On-link        10.0.2.15    281
       10.0.2.255  255.255.255.255       On-link        10.0.2.15    281
      10.10.110.8  255.255.255.255     10.10.120.1   10.10.xxx.yyy    126
     10.10.110.31  255.255.255.255     10.10.120.1   10.10.xxx.yyy    126
      10.10.119.0    255.255.255.0     10.10.120.1   10.10.xxx.yyy    126
      10.10.120.0    255.255.252.0       On-link    10.10.xxx.yyy    281
    10.10.xxx.yyy  255.255.255.255       On-link    10.10.xxx.yyy    281
    10.10.123.255  255.255.255.255       On-link    10.10.xxx.yyy    281
      54.66.2.26  255.255.255.255       10.0.2.2       10.0.2.15    281
        127.0.0.0        255.0.0.0       On-link        127.0.0.1    331
        127.0.0.1  255.255.255.255       On-link        127.0.0.1    331
  127.255.255.255  255.255.255.255       On-link        127.0.0.1    331
        224.0.0.0        240.0.0.0       On-link        127.0.0.1    331
        224.0.0.0        240.0.0.0       On-link        10.0.2.15    281
        224.0.0.0        240.0.0.0       On-link    10.10.xxx.yyy    281
  255.255.255.255  255.255.255.255       On-link        127.0.0.1    331
  255.255.255.255  255.255.255.255       On-link        10.0.2.15    281
  255.255.255.255  255.255.255.255       On-link    10.10.xxx.yyy    281

..
```

General

3. SSH KEY PAIRS: DATA PROVIDER + DATA USER (NA CSPs)

3.1. Overview

This section provides an overview of SSH Key Pair management. It covers the generation of Key Pairs, offering examples for both Linux/WSL and Windows. The content also addresses fingerprinting and sharing Public Keys. Additionally, this section explains the utilization of SSH Agent, including examples for both Linux and Windows. The section concludes by offering guidance on SSH access configuration, with a focus on CLI (Linux, WSL, Windows - PowerShell and CommandPrompt) examples.

SSH Keys provide a secure method for authenticating with the IPND IIS-File Transfer Server (FTS) through public-key cryptography. This cryptographic technique involves a pair of keys: a Private (secret) Key and a Public Key.

Users are required to generate an SSH Key Pair and provide the generated Public Key to the IPND Support team.

The Public SSH Key will be used to give a User authenticated access to their account on the IIS-FTS.

3.2. Generate an SSH Key-Pair

The following examples show how to create an SSH key-pair for the IPND User account <user>.

3.2.1. CLI: Linux, WSL, PowerShell, CommandPrompt

SSH key pair creation

It is highly recommended that the User is in their home directory (referred to from this point forward as `<TheCurrentDirectory>`) to run the below command:

As a standard user <user>: Linux, WSL, Windows – PowerShell or CommandPrompt

GENERATE A SSH KEY-PAIR
NB: It Is recommended that you copy the generated location where the keys are being saved (shown in orange) and change the id part of the file name to a short (without spaces) version of your company name, and paste this as 'file in which to save the key'.

```
ssh-keygen -t ed25519 -C "<LongCompanyName>"
        Generating public/private ed25519 key pair.
        Enter file in which to save the key (<TheCurrentDirectory>/.ssh/id_ed25519):
        <TheCurrentDirectory>/.ssh/<ShortCompanyName>_ed25519
        Created directory '<TheCurrentDirectory>/.ssh'  ## Not Displayed if directory already exists
        Enter passphrase (empty for no passphrase):
        Enter same passphrase again:
        Your identification has been saved in <TheCurrentDirectory>/.ssh/<ShortCompanyName>_ed25519.
        Your public key has been saved in <TheCurrentDirectory>/.ssh/<ShortCompanyName>_ed25519.pub.
        The key fingerprint is:

        SHA256:V0+1gTGVBrxTxEwHPo+e5dChLgdagjpAGCBQR7dtBV8 <LongCompanyName>

        The key's randomart image is:

        +--[ED25519 256]--+
        |=. .E*+oo=..     |
        |+.o.=Booo.+      |
        |*.=o+o*.+.       |
        |.B.+ o =         |
        |... o o S        |
        |   . o o o       |
        |    . B o .      |
        |     = .         |
        |                 |
        +----[SHA256]-----+
```

Important: Take note of the SSH key's fingerprint (Shown above)

⚠ Linux/WSL places greater emphasis on SSH Key Pair files and directory permissions in comparison to Windows.

It is recommended that Users inspect the permissions of the existing directory and those of the generated key-pair files after key-pair generation in the event that the "Created directory" message didn't appear.

As a standard user <user>: **Linux only**

```
## Setting/Correcting file permissions
        chmod 700 <TheCurrentDirectory>/.ssh
        chmod 600 <TheCurrentDirectory>/.ssh/<ShortCompanyName>_ed25519

        chmod 644 <TheCurrentDirectory>/.ssh/<ShortCompanyName>_ed25519.pub
```

3.2.2.　　GUI: Windows Putty

Run the PuTTygen application

Users will be navigated to a screen similar to the below:
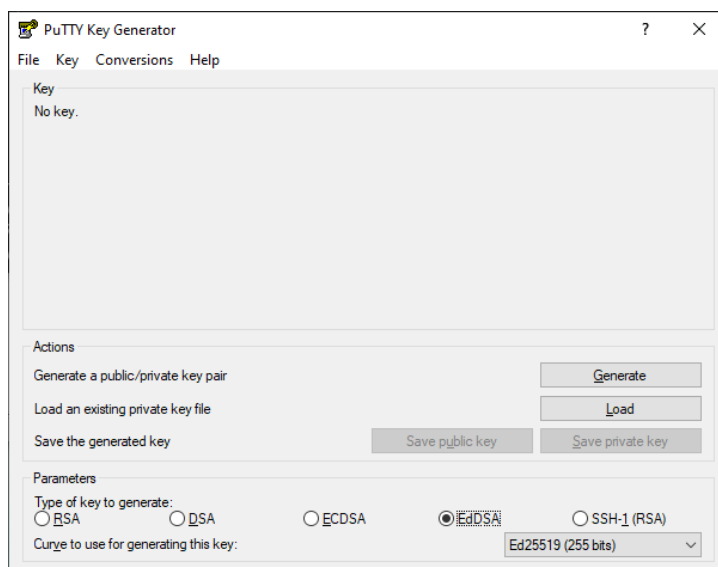
SSH Key Pair creation - Windows Example

Select **EdDAS** and **ED25519(255 bits)** in the dropdown as the key type.

Click "Generate".
Once the key has been generated the following screen will appear:
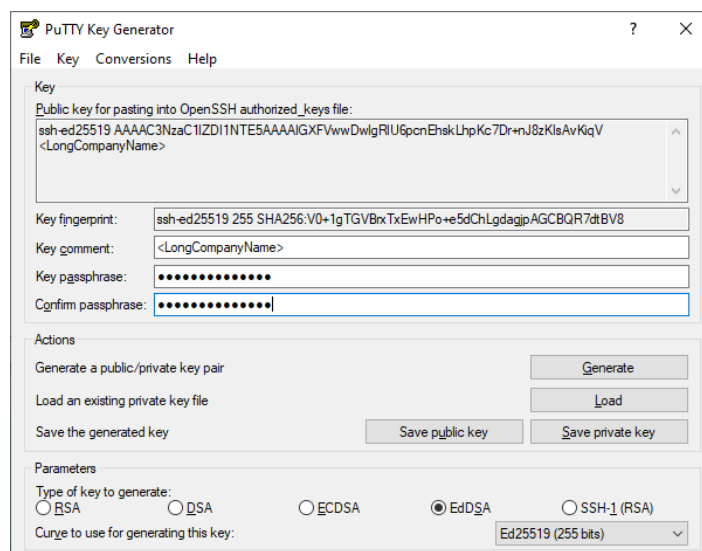
SSH Key Pair creation – PuTTY Key Generator

Users must perform the following when presented the above screen:

- Take note of the Key Fingerprint.
- Enter the User's Organisation / Business name in the Key comment field.
- Enter a secure passphrase.
- Save the Public Key in a known location with the Organisation / Business short form(spaceless) name as the key filename with a file extension **.pub**. Do NOT save the file in the default - C:\Program Files\PuTTY folder.
- Save the Private Key in a known location the same name as the Public Key filename without a file extension. It is given the file extension of **.ppk** by the application. Do NOT save the file in the default - C:\Program Files\PuTTY folder.

3.3. Fingerprinting and sharing the Public SSH Key

Upon successfully generating the keys, Users are required to send the **SSH Public key** (<user>.pub) to the IPND Support team via email: ipnd-support@logicaltech.com.au

Upon receipt of the Public Key, the IPND Support team will be in contact to verbally validate the key fingerprint before it is deployed.

> Important Notes:
> Do not send key fingerprints via email.
> The IPND Support team will be in contact to verbally verify key fingerprints.
> Do not email the Private Key. Private Keys must be protected by passphrase and stored in a secure location.

The following section details how to obtain / regenerate fingerprints for SSH and GPG Keys for verbal verification with the IPND Support team.

3.3.1. CLI: Linux, WSL, PowerShell, CommandPrompt

If the SSH Key-Pair was generated using ssh-keygen via CLI: Linux, WSL, Windows - PowerShell

> As a standard user <user>: Linux, WSL, Windows – PowerShell or CommandPrompt

```
## FINGERPRINT AN EXISTING SSH PUBLIC KEY
ssh-keygen  -l -f '<TheCurrentDirectory>/.ssh/<ShortCompanyName>_ed25519.pub'
        256 SHA256:V0+1gTGVBrxTxEwHPo+e5dChLgdagjpAGCBQR7dtBV8 <LongCompanyName> (ED25519)
```

3.3.2.   GUI: Windows PuTTY

If the Key-Pair was generated via PuTTYgen, open the PuTTYgen application and click on load and browse to locate the saved private (.ppk) file. The passphrase is required to load the key.
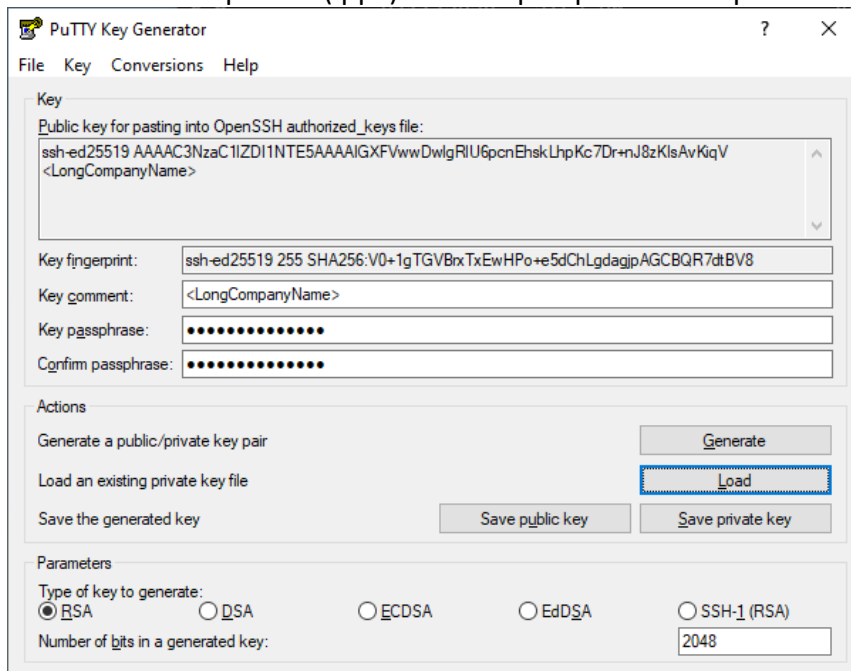
SSH Key Pair creation – PuTTY Key Generator

3.4.   Using an SSH passphrase storage agent: ssh-agent, pagaent

Authentication is required to access the IPND SFTP/SCP service using the SSH Private Key generated in previous sections of this document.

To authenticate, the User is required to enter the passphrase associated with the SSH Private Key. Automated / unattended batch systems are required to perform authentication for each session. It is recommended that automated / unattended batch transfer solutions utilise a ssh-agent component to load the Private Key for authentication.

A ssh-agent is a trusted repository into which the Private Key can be loaded.

3.4.1.   CLI: Linux, WSL, PowerShell, CommandPrompt: Setting up ssh-agent

For CLI environments, it is recommended that a ssh-agent is utilised to manage SSH Keys for authentication. The ssh-agent securely stores the passphrase protected Private Key for each session, eliminating the need for the User to enter the passphrase for each SSH connection. The ssh-agent temporarily stores the passphrase protected Private Key in memory, providing the User a seamless and secure way to manage SSH connections without compromising the security provided by the passphrase. To use ssh-agent, follow these steps:

As a standard user <user>: Linux, WSL, Windows – PowerShell or CommandPrompt

```
## Start ssh-agent run the following:
# For Linux/WSL only

eval "$(ssh-agent -s)"

# For PowerShell/CommandPrompt only

ssh-agent

## Load a private key into the agent, You will be prompted for the key's passphrase
# For Linux/WSL or PowerShell/CommandPrompt

ssh-add -t <lifetime> <TheCurrentDirectory>/.ssh/<ShortCompanyName>_ed25519
```

Note: <lifetime> e.g. -t 3600s for 3600 seconds, -t 60m for 60 minutes, -t 2h for 2 hours, -t 1d for 1 day).

3.4.2.   CLI: Linux, WSL, PowerShell, CommandPrompt Using ssh-agent

The ssh-agent is designed to be used with SSH and its suite of programs. SSH programs will use ssh-agent if it is running. If ssh-agent is not running, the User will be prompted for their SSH Key's passphrase.

3.4.3.   GUI: Windows Setting up Pageant

In the Windows environment, **Pageant** serves a similar purpose as the **ssh-agent** in CLI (Linux/WSL, Windows-PowerShell or CommandPrompt). Pageant is part of the PuTTY suite of tools and acts as an SSH authentication agent. Pageant allows Users to load their Private SSH Keys into memory, and other PuTTY-related tools (eg: PuTTY itself or Plink) for authentication without prompting Users for the passphrase each time.

The below details the process for loading and accessing the Keys in Pageant:

1.   Start Pageant:

 Start Pageant by running the pageant.exe executable.
 It will run in the background and appear as an icon in the system tray.

2.   Load Keys into Pageant:

 Right-click on the Pageant icon in the system tray.
 Choose "Add Key" and select your Private SSH Key file.
 Enter the passphrase for the key if it's protected by one.

3.   Agent Process:

 Pageant is now running as an SSH agent in the background.
 It holds the Private Keys in memory and provides them to applications upon request.

4.   Key Access:

 The use of **PuTTY**, **Plink**, or other PuTTY-related tools to connect to an SSH server, enables these tools to communicate with Pageant to access the Private Keys loaded into it.

 Users will not be prompted to enter the passphrase as long as Pageant is running, and the keys are loaded.

5.   To view loaded keys:

Locate the Pageant Icon: Pageant will run in the background and can be found in the system tray of the Windows taskbar.

Right-Click on Pageant Icon: Select "View Keys": A window like the one below will open, displaying the list of currently loaded keys.
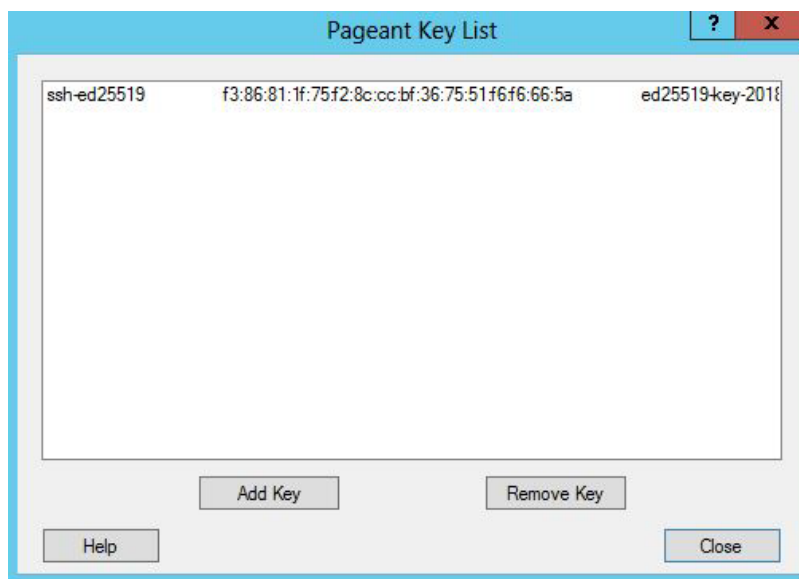
Puttygen - SSH Agent

3.4.4.   CLI: Windows Using Pageant with PowerShell or CommandPrompt

Pageant is designed to be used with PuTTY and its suite of programs. The use of Pageant with CLI: PowerShell/CommandPrompt (Windows) OpenSSH is not covered in this document.
Pageant does not work with Linux/WSL.

3.4.5.   GUI: Windows Using Pageant with WinSCP or FileZilla

WinSCP will use Pageant if it is running. If Pageant is not running, Users will be prompted for their SSH Key passphrase.

FileZilla will use Pageant if it is running. If Pageant is not running, Users will be prompted for their SSH Key passphrase, where FileZilla will by default remember the passphrase until it is closed.

3.5.   SSH Access Configuration

3.5.1.   CLI: Linux, WSL, PowerShell, CommandPrompt

To ensure that Users' connection to the IPND services is as seamless as possible, the Users configuration details must be specified in the same directory location as the SSH Key-Pair files:
`<TheCurrentDirectory>/.ssh/`**config** file associated with the account from which Users transfer files to and from the IPND. The format of the config file is as follows:

 #Production Service Example

```
host pfts
hostname pfts.ipnd.com.au
port 22
IdentityFile ~/.ssh/<prod_user_priv_key>
user <prod-user>
```

#User Test Service Example

```
host ufts
hostname ufts.ipnd.com.au
port 22
IdentityFile ~/.ssh/<test_user_priv_key>
user <test-user>
```

3.5.2. GUI: Windows WinSCP or FileZilla

Not applicable as this is internally managed by the application.

4. GPG KEY PAIRS: (ALL USERS) DATA PROVIDER + DATA USER + CSP

4.1. 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.

4.2. 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.

4.3. Creating a GPG key pair, Finger Printing, Exporting

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.

The GPG Public Key must be provided to the IPND Support team once generated via email to: IPND-support@logicaltech.com.au. The generated GPG Public Key will be used to encrypt files transferred / downloaded from the IPND.

4.3.1. CLI: Linux, WSL, PowerShell, CommandPrompt

Users will be provided with the information to be added to the Comment field (optional).

Users will be prompted to provide a passphrase to protect their GPG Key. It is imperative that a strong password or passphrase is specified. After the passphrase is entered the GPG Keys will be created and stored in the key chain.

To generate a GPG Key Pair run the following:

```
As a standard user <user>: Linux, WSL, Windows – PowerShell, CommandPrompt

## GENERATING your gpg key pair

gpg --expert --full-generate-key

        gpg (GnuPG) 2.4.3; Copyright (C) 2023 g10 Code GmbH
        This is free software: you are free to change and redistribute it.
        There is NO WARRANTY, to the extent permitted by law.
        Please select what kind of key you want:
           (1) RSA and RSA
           (2) DSA and Elgamal
           (3) DSA (sign only)
           (4) RSA (sign only)
           (7) DSA (set your own capabilities)
           (8) RSA (set your own capabilities)
           (9) ECC (sign and encrypt) *default*
          (10) ECC (sign only)
          (11) ECC (set your own capabilities)
          (13) Existing key
          (14) Existing key from card
        Your selection? 9
        Please select which elliptic curve you want:
           (1) Curve 25519 *default*
           (2) Curve 448
           (3) NIST P-256
           (4) NIST P-384
           (5) NIST P-521
```

```
        (6) Brainpool P-256
        (7) Brainpool P-384
        (8) Brainpool P-512
        (9) secp256k1
    Your selection? 1
    Please specify how long the key should be valid.
            0 = key does not expire ## Recommended by LogicalTech ##
        <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) 0
    Key does not expire at all
    Is this correct? (y/N) y
    GnuPG needs to construct a user ID to identify your key.
    Real name: YourCompanyName
    Email address: CompanyEmailAddress@xxx.yyy.zzz
    Comment: Company
    You selected this USER-ID:
        "YourCompanyName (Company) <CompanyEmailAddress@xxx.yyy.zzz>"

    Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
    We need to generate a lot of random bytes. It is a good idea to perform
    ..
    public and secret key created and signed.
    pub   ed25519 2024-01-24 [SC]
          0EE4B570D5894794B328D4E83143C8B76468C1C0
    uid                  YourCompanyName (Company) <CompanyEmailAddress@xxx.yyy.zzz>
    sub   cv25519 2024-01-24 [E]
```

LIST the public key(s)

```
gpg -k   or   gpg --list-keys

    pub   ed25519 2024-01-24 [SC]
          0EE4B570D5894794B328D4E83143C8B76468C1C0
    uid           [ultimate] YourCompanyName (Company) <CompanyEmailAddress@xxx.yyy.zzz>
    sub   cv25519 2024-01-24 [E]
```

FINGERPRINT (Shown in green) your key identified by `CompanyEmailAddress@xxx.yyy.zzz`

```
    gpg --fingerprint CompanyEmailAddress@xxx.yyy.zzz

    pub   ed25519 2024-01-24 [SC]
          0EE4 B570 D589 4794 B328  D4E8 3143 C8B7 6468 C1C0
    uid           [ultimate] YourCompanyName (Company) <CompanyEmailAddress@xxx.yyy.zzz>
    sub   cv25519 2024-01-24 [E]
```

EXPORT PUBLIC KEY (To a file, shown in green). Send this file via email to the IPND Support team to: IPND-support@logicaltech.com.au, for verbal validation.

```
    gpg --armor --export CompanyEmailAddress@xxx.yyy.zzz > MyPublicKey.asc
```

4.3.2. GUI: Windows Kleopatra

Launch Kleopatra and click 'New Key Pair'.

If there are no (0) keys (created or imported) Users will be presented with the screen below when Kleopatra is launched.

If keys are present, upon launching Kleopatra Users will be presented with the Certificates page containing previously created/imported keys.

To create a new keypair click on the 'New Key Pair' icon in the centre of the screen or select 'New OpenPGP Key Pair' from the 'File menu'
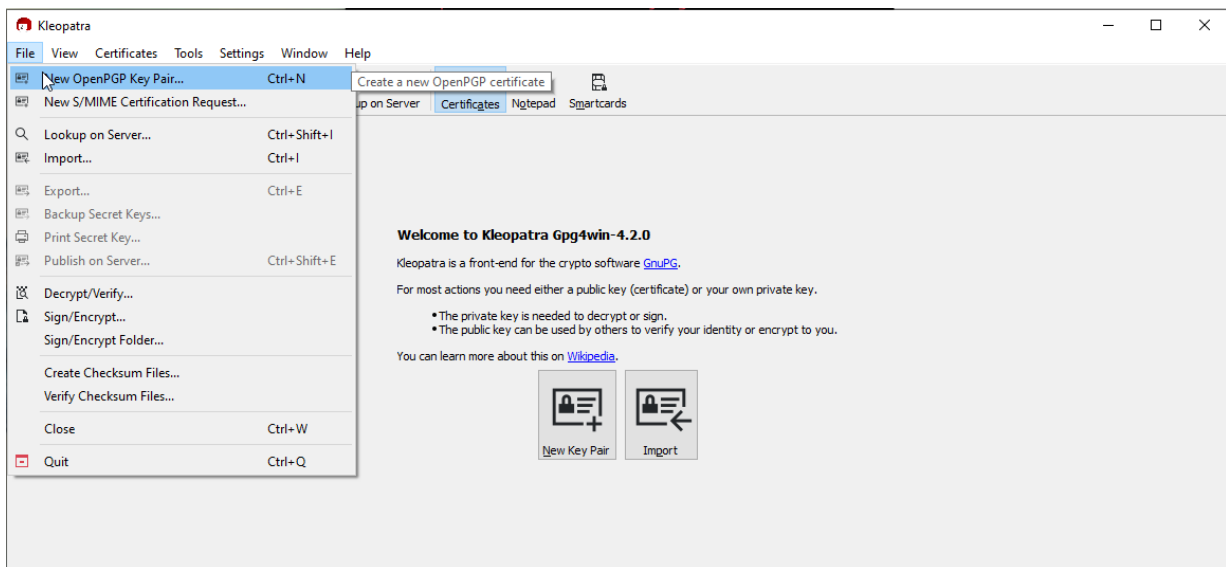
Kleopatra – 0 GPG keys present

Users will be prompted to provide their Name and email address. Users must tick the 'Protect the generated key with a passphrase' box and click on the 'Advanced Settings…' button.

On the Advanced Settings page select ECDSA/EdDSA with the value ed25519.
Tick the +ECDH box and select cv25519.
Unselect the 'Valid until:' checkbox.
Click OK to return the Create OpenPGP Page, after which hitting OK Users will be prompted to provide a passphrase.
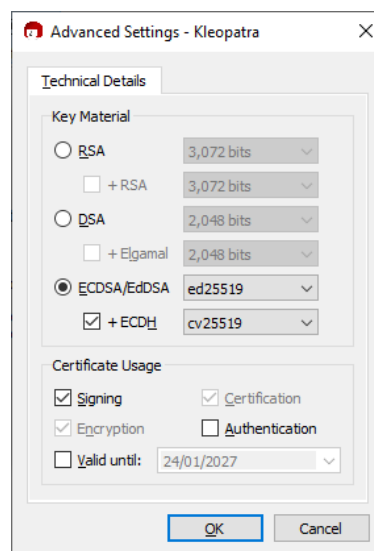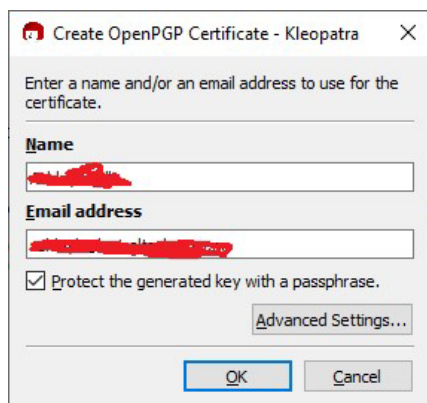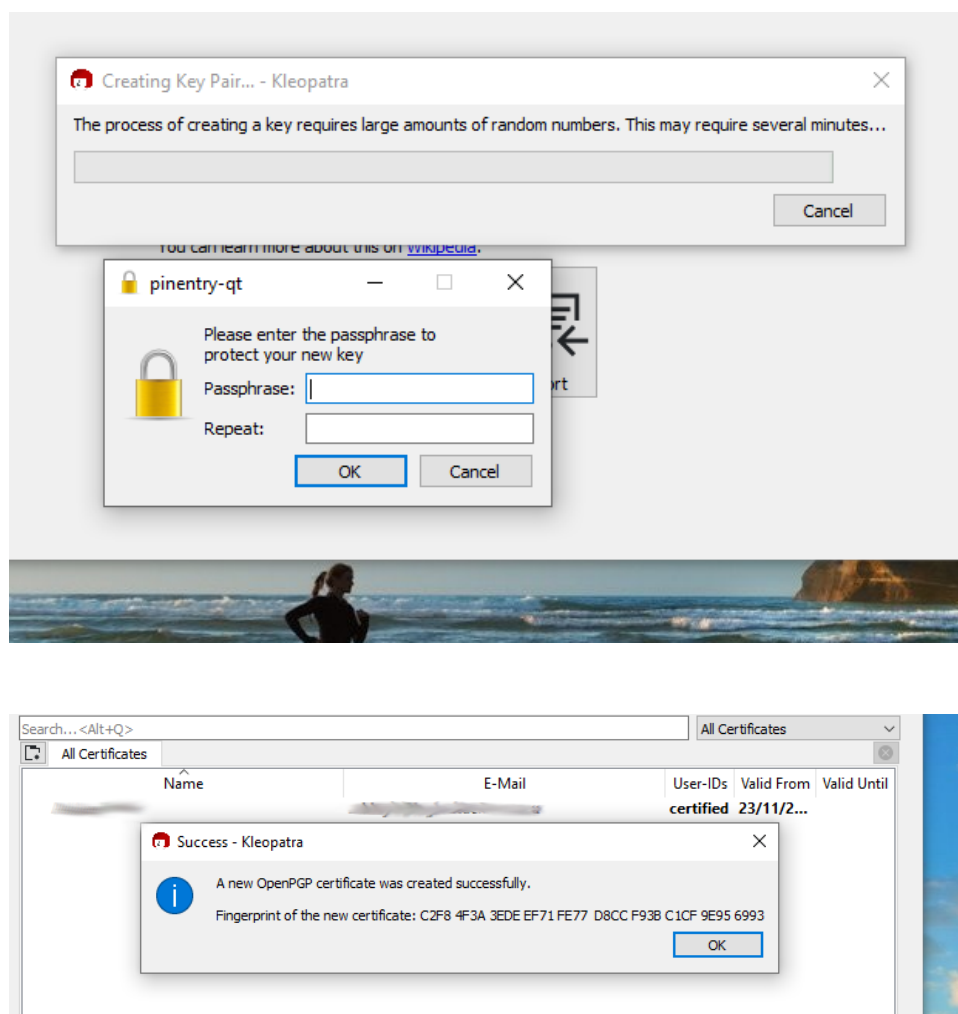
Take note of the fingerprint for verbal validation by the IPND Support team.

To export the Public Key, highlight the GPG Key on the Certificates page and right click.

Select Export and Save the Public GPG Key and send the Key via email to the IPND Support team to: IPND-support@logicaltech.com.au, for verbal validation.
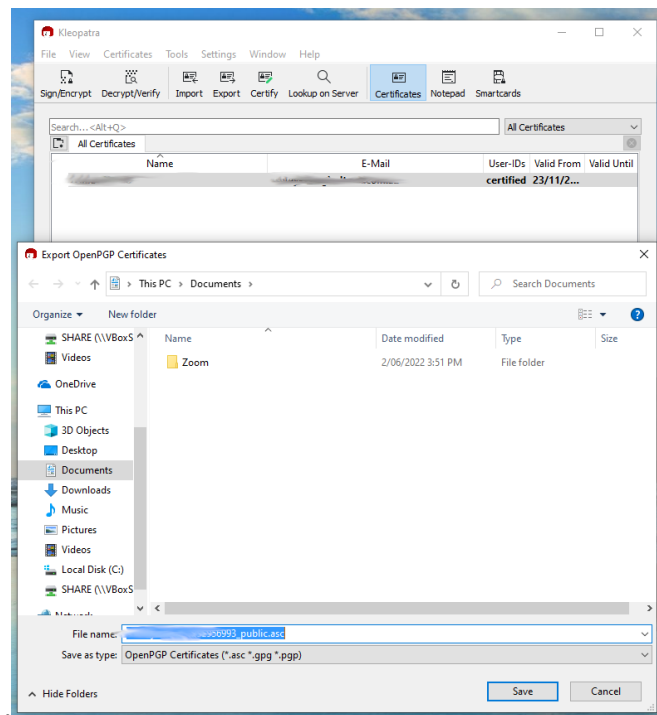
4.4. Import, Fingerprint and trust the IPND Public GPG key

The following instructions assume the User has already created their GPG Key.

The instructions on importing the IPND Public GPG Key also assumes that the IPND Public Key has been saved/named IPND-IIS-publickey.gpg

The IPND Public GPG Key file will have been provided to Users by the IPND Support Team.

This key is a simple text file that looks like:

IPND-IIS public gpg key (ASCII-armored format)

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQENBFpny9QBCADb1u+tXTD2VwrFdPfX3eJlmnnz9MGD8i0oGCQEZT2KJ/yf42qM
f/dR38JCCcbbnE1/N5TkaxeSrk9WqataVEY6r75himzhJP5IHBcl1JtSu67hz2WU
P+2K6tzBV+NntuTGyVsqZiNgGr3O8gC2mYBZ+hcBVID0y29kQgHD952N4jmpsq65
/l4KV/Uto7p6b1Yd3WLjl6Uk6PaCypuxDrqy2ftPeQ5BmZv1qLytt3zx8MeSkadL
+y4qmL+8dVB0jtzP7n1drZzHovCa7BE1KqrnKEFjvIw95UiBY7jCmT8LxsxVUBhh
5q98kdfjgx/wF/YQlcI3NYaAe2in1pJzIl5VABEBAAG0SGlwbmQtaWlzIChJUE5E
IE1JUyBmaWxlIHRyYW5zZmVyIGVuY3J5cHRpb24ga2V5LikgPGlwbmQtaWlzQGlw
bmQuY29tLmF1PokBOQQTAQgAIwUCWmfL1AIbAwcLCQgHAwIBBhUIAgkKCwQWAgMB
Ah4BAheAAAoJEEYPjXxbxZg1oKwH/2iJlx4Y/LYRfdFRwY27YT1yxAPRUL5hg019
ByZHjJh7dyajHKbq4bNL++5jiRCbbOAXk1SGouAZkGBStkmXUoxPjuohJeuJIOUx
n8rxLmjMi01nma/y8Tyav/bGnjzGa0U0f9yfG/FhJozCinEtbtmhlLlGSkLTaYhk
8mzREEzd5s4+LZ+P8ClSmrXYGNGP8+uLwem3Y+sgkA8IeKhGE26So+llOld687sE
DklpQJMHfpmAhW7jJW1gyLQl/iULW6oF1SqxNEN/4aLk2K9OmoPwQpO4eHsSmQfE
q8aY9YPpGUEUb8zzFjcb2nbgZpS9pgnLygYrQN7dLrL7Qye+f365AQ0EWmfL1AEI
ANO+L4kW1WLJBGiuorlkTCGYyCf2j8i83nJCYoJWBzg7+csv6VefG7bIaLgNPs5k
7dszG7Ztfr/bLf5M8pigvHcfcJhx68tYzD6hW5PONr5rdy2rH8k/H6ZNkkGZKkJq
puTO2uDtQg0ONQ1o0AOo6kRvm2uO2UCG0n3nb+detfsOuHtVGSKo/g2nM3a9mLhK
mjd1QMeBI8cpqw/R4KERTNNbTwYxQnZsVXOyzuJHQBynCyAtvDMhO5Ch4y4WQp2A
PdiXLYN7pqFudjsuTm02uRBjDrjzRndQQWNbVWS1SPepz86hd6/Euj2atxnVsWU/
/gWHqvyX3+PxBOhIQNfMCGsAEQEAAYkBHwQYAQgACQUCWmfL1AIbDAAKCRBGD418
W8WYNVmAB/9H+Tgx5wWcXW7GkvlNXR2vqOwlBG4RE5EWjj7qTP2+JUZslEDve8GD
z00bmEfon+XwQVHU9U6xvXdpPYQfL+hHYtT+UusBhKwm7Ov/RHNO+6JlfoEvjo2I
t522sed0XnLSWpF9xogqaRAXN+4W03Vmlswbw24aQUgfLCNa5qA2tnusHk8wjgrm
8aVUCoaCbQGE18K57S2o2xTCNTLt8J7ysGiTSLwJMoEtHqzqUwCtyEzAYHY9cpVZ
/HcjKb6KkV5djqzmOjH0df69tZu+newoF6HNRCgbVtsKK5CexabG+ggAV171SQkk
tDdhSb6UPVV7cozE/nqBCpBfkr8NCVUC
=fixq
-----END PGP PUBLIC KEY BLOCK-----
```

Save the IPND Public Key and check its md5sum

As a standard user <user>: Linux, WSL

```
## Use the cd command to change to the directory where you saved the IPND public key file

cd <Directory Where File was saved>


md5sum IPND-IIS-publicley.gpg

        afe982d3fc99e636efb0d7ed4d6b6e8a  IPND-IIS-publicley.gpg
```

As a standard user <user>: Windows – PowerShell or CommandPrompt

```
## Use the cd command to change to the directory where you saved the IPND public key file

cd <Directory Where File was saved>


Get-FileHash -Algorithm MD5 -Path ".\IPND-IIS-publicley.gpg"

        Algorithm       Hash                             Path
        ---------       ----                             ----
        MD5      AFE982D3FC99E636EFB0D7ED4D6B6E8A        C:\Users\UserName\IPND-IIS-pub...
```

4.4.1. CLI: Linux, WSL, PowerShell, CommandPrompt

Users **MUST** import, fingerprint and **trust** the IPND-IIS Public Key.

As a standard user <user>: Linux, WSL, Windows – PowerShell or CommandPrompt

```
## Use the cd command to change to the directory where you saved the key file
cd <Directory Where File was saved>
## IMPORT the public gpg key
gpg --import IPND-IIS-publickey.gpg

        gpg: keybox '/home/<user>/.gnupg/pubring.kbx' created ##Extra Line shown in Linux/WSL

        gpg: /home/<user>/.gnupg/trustdb.gpg: trustdb created ##Extra Line shown in Linux/WSL

        gpg: key 460F8D7C5BC59835: public key "ipnd-iis (IPND IIS file transfer encryption key.) <ipnd-
        iis@ipnd.com.au>" imported

        gpg:               imported: 1


## LIST the public key(s). You should see the key you created earlier and the imported IPND key

gpg -k

        ---------
        pub   ed25519 2024-01-24 [SC]
              0EE4B570D5894794B328D4E83143C8B76468C1C0
        uid           [ultimate] YourCompanyName (Company) <CompanyEmailAddress@xxx.yyy.zzz>
        sub   cv25519 2024-01-24 [E]

        pub   rsa2048 2018-01-23 [SC]
              CD4C04C9630DAD81B192A1BC460F8D7C5BC59835
        uid           [ unknown] ipnd-iis (IPND IIS file transfer encryption key.) <ipnd-iis@ipnd.com.au>
        sub   rsa2048 2018-01-23 [E]


## FINGERPRINT (Shown in orange) the ipnd-iis key identified by ipnd-iis@ipnd.com.au

gpg --fingerprint ipnd-iis@ipnd.com.au

        pub   rsa2048 2018-01-23 [SC]
              CD4C 04C9 630D AD81 B192  A1BC 460F 8D7C 5BC5 9835
        uid           [ unknown] ipnd-iis (IPND IIS file transfer encryption key.) <ipnd-iis@ipnd.com.au>
        sub   rsa2048 2018-01-23 [E]


## TRUST the ipnd-iis public key (Trust Level Must be >= 4)

gpg --edit-key ipnd-iis@ipnd.com.au

        gpg (GnuPG) 2.4.3; Copyright (C) 2023 g10 Code GmbH
        This is free software: you are free to change and redistribute it.
        There is NO WARRANTY, to the extent permitted by law.
        pub  rsa2048/460F8D7C5BC59835
             created: 2018-01-23  expires: never       usage: SC
             trust: unknown       validity: unknown
        sub  rsa2048/B239EE64FBFA9B6E
             created: 2018-01-23  expires: never       usage: E
        [ unknown] (1). ipnd-iis (IPND IIS file transfer encryption key.) <ipnd-iis@ipnd.com.au>
        gpg> trust
        pub  rsa2048/460F8D7C5BC59835
             created: 2018-01-23  expires: never       usage: SC
             trust: unknown       validity: unknown
        sub  rsa2048/B239EE64FBFA9B6E
             created: 2018-01-23  expires: never       usage: E
        [ unknown] (1). ipnd-iis (IPND IIS file transfer encryption key.) <ipnd-iis@ipnd.com.au>
        Please decide how far you trust this user to correctly verify other users' keys
        (by looking at passports, checking fingerprints from different sources, etc.)
          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
        Your decision? 5
        Do you really want to set this key to ultimate trust? (y/N) y
        pub  rsa2048/460F8D7C5BC59835
             created: 2018-01-23  expires: never       usage: SC
             trust: ultimate      validity: unknown
        sub  rsa2048/B239EE64FBFA9B6E
             created: 2018-01-23  expires: never       usage: E
        [ unknown] (1). ipnd-iis (IPND IIS file transfer encryption key.) <ipnd-iis@ipnd.com.au>
        Please note that the shown key validity is not necessarily correct
        unless you restart the program.
```

```
        gpg> quit


## Confirm TRUST Level (shown in orange) as ultimate
gpg --fingerprint ipnd-iis@ipnd.com.au
        pub   rsa2048 2018-01-23 [SC]
              CD4C 04C9 630D AD81 B192  A1BC 460F 8D7C 5BC5 9835
        uid           [ultimate] ipnd-iis (IPND IIS file transfer encryption key.) <ipnd-iis@ipnd.com.au>
        sub   rsa2048 2018-01-23 [E]
```

The IPND Support team will validate verbally that the fingerprint is correct.

> Note: Please DO NOT send key fingerprints via email. They must be verified verbally by the IPND Support team.

4.4.2.   GUI: Windows Kleopatra

Users are required to import the IPND Public Key provided to them by the IPND Support team using the Kleopatra application.
By default, keys created/imported by Windows - PowerShell or CommandPrompt will be visible to Kleopatra (if it is installed).

Note: A different process applies for Linux/WSL.

4.4.2.1.   GUI: WINDOWS IMPORTING THE IPND GPG KEY

Launch Kleopatra.

If there are no (0) keys (created or imported) Users will be presented with the screen below when Kleopatra is launched. If this is the case, the User must repeat the steps in Section 4.3 Creating a GPG key pair, Finger Printing, Exporting.

If keys are present, upon launching Kleopatra Users will be presented with the Certificates page containing previously created/imported keys.
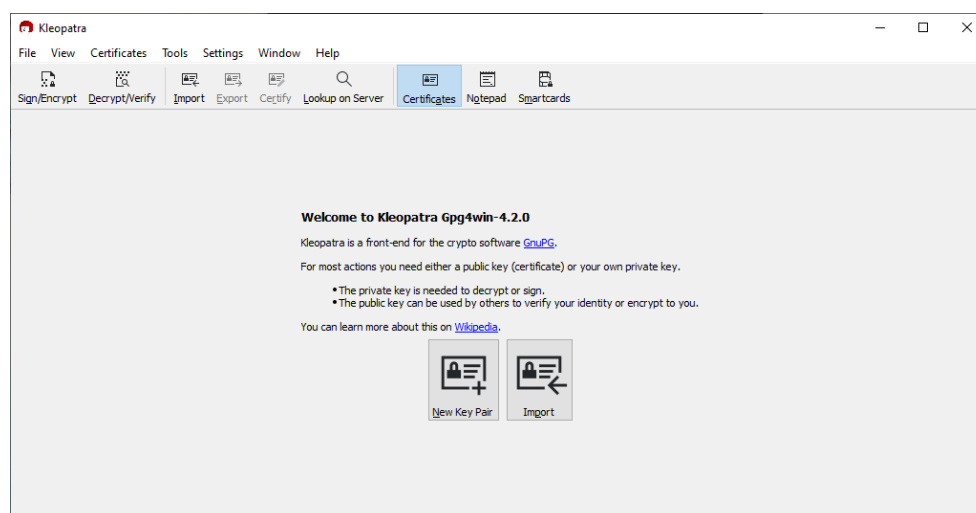
Kleopatra: 0 GPG keys present
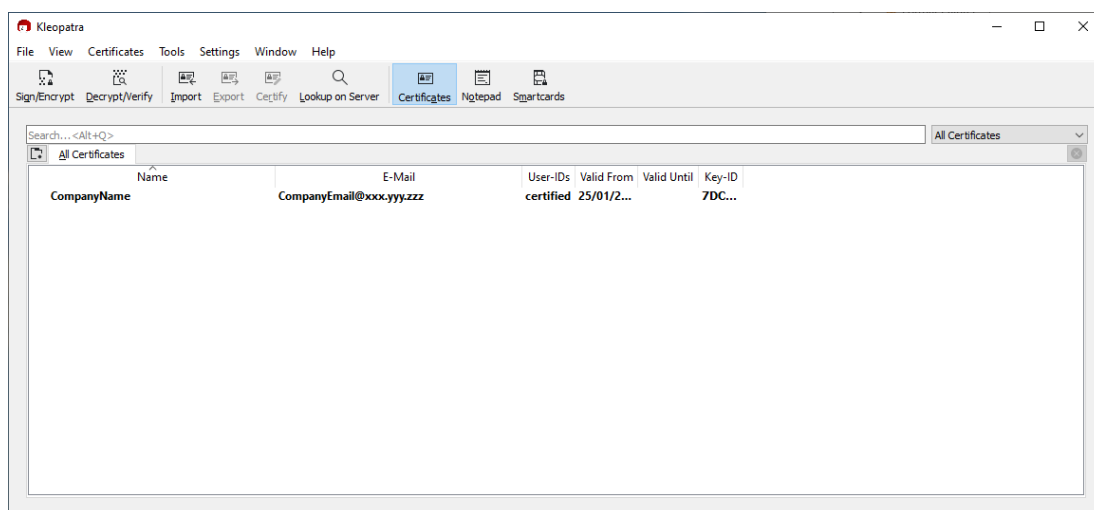
Kleopatra: 1 GPG key present

Click on 'File' and select 'Import'.

If the IPND Public Key was not saved with the recommended name, select 'Any files (*)' and then browse to the location of the saved IPND-IIS-publickey.gpg file

Select the file and click the Open icon.

Users should be presented with the below screen to indicate a successful import

⚠ Important: Before exiting the screen, the user **must** set the 'Trust' for the IPND-IIS-publickey.gpg key by clicking on the 'Certify' button.
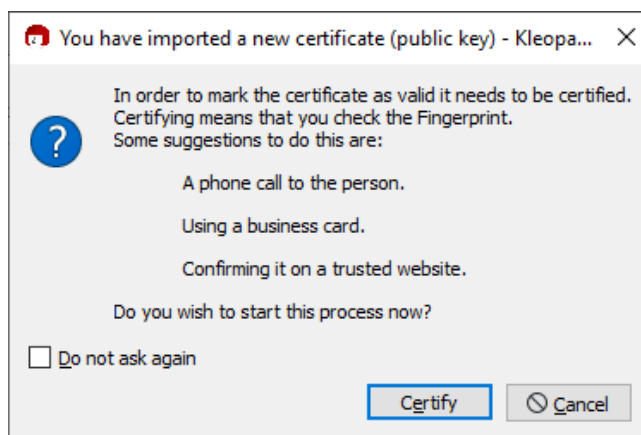
Kleopatra: Certify the IPND Public key

Click the ▶ on the lefthand side of Advanced to expand.

In the expanded section ensure that 'Certify for everyone..' and 'Certify as trusted introducer' are ticked

Click on the 'Certify' button on the bottom right hand side of the page.

Enter the GPG Key passphrase when prompted.

When successful the IPND Public key will be '**Fully**' Trusted:

Kleopatra: Certify the IPND Public key

4.4.2.2. GUI: WINDOWS TRUSTING A GPG KEY

Users can modify the trust (certification) level for an imported key only when the uses previously generated Public/Private GPG Key Pair are present.

If the trust of the IPND Public Key is not set when importing, the trust level can be modified at a later date using the below process:

Launch Kleopatra and select the IPND-IIS-publickey.gpg file

Right click and select 'certify'

Click the ▶ on the lefthand side of Advanced to expand.

In the expanded section ensure that 'Certify for everyone...' and 'Certify as trusted introducer' are ticked

Click on the 'Certify' button on the bottom right hand side of the page.

Enter the GPG Key passphrase when prompted.

If successful the IPND Public key will be '**Fully**' Trusted:
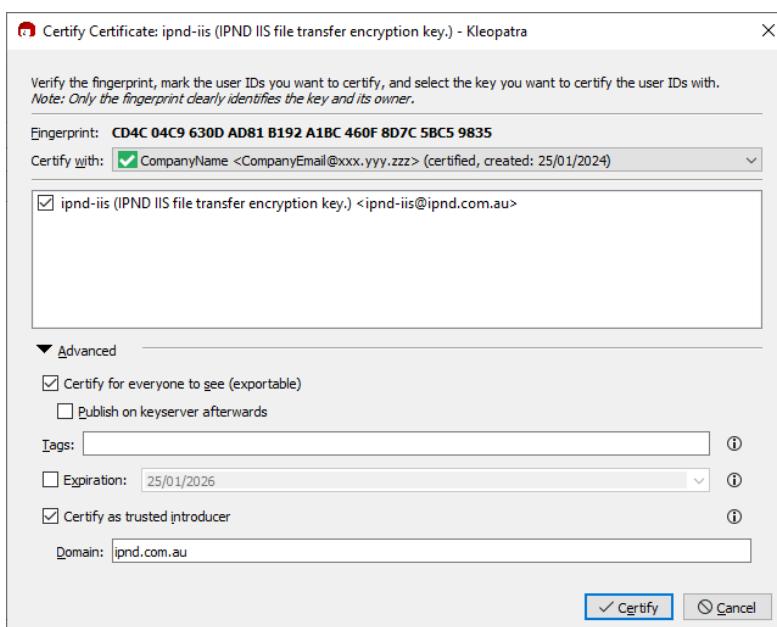
Kleopatra: Certify the IPND Public key

5. CONNECTING TO FTS: DATA PROVIDER + DATA USER (NA CSPS)

5.1.   Overview

This section describes how to connect to the IPND IIS FTS. The basic steps are:

Uploading files from the Users' server to the FTS

- Encrypt the file with the IPND Public Key
- Establish a VPN tunnel
- Transfer the file to the Users home directory using SFTP protocol and disconnect
- Terminate the VPN tunnel

Downloading files from the FTS to the Users' server

- Establish a VPN tunnel
- Transfer the file to the Users' home directory using SFTP protocol and disconnect
- Terminate the VPN tunnel
- Decrypt the file with using the Private GPG Key

5.2.   Establish a VPN tunnel

Once the User has successfully established a VPN connection as described in Section 2.VPN the User can then establish an SSH connection. The tunnel needs to be maintained for the duration of the SSH (SFTP) session.

5.3.   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.

5.4.   Connection Management Guidelines

To facilitate file transfer between the Users' server and the IPND, the User must establish an authorized VPN connection. The IPND exclusively supports secure file transfer protocols such as SFTP (Secure File Transfer Protocol) over SSH.

⚠ OpenSSH (v9.0+) has deprecated the legacy SCP protocol by default, so Users are recommended to use SFTP instead. SFTP is a standardized protocol (RFC 4254/4256) with robust features. SCP offers limited functionality and lacks modern features and proper error handling. While SCP is currently supported by the IPND system, SCP will be deprecated in the future on the IPND system, as it is not a formally standardized protocol.

5.4.1.   VPN Session Management

Idle VPN sessions are automatically terminated after 15 minutes of inactivity.

VPN sessions have a maximum duration of 24 hours and will be automatically terminated, even if actively in use.

It is highly recommended that Users' terminate both SSH and VPN sessions after completing file transfers to release resources and enhance security.

Wait at least 10-15 minutes before reconnecting to verify that uploaded file(s) have been processed and to download subsequent .err files.

5.4.2. Security Considerations

Retaining open VPN and SSH connections post file transfer poses security risks by extending the exposure window for unauthorized access. Extended session durations increase the likelihood of security vulnerabilities being exploited, providing malicious actors with a larger timeframe to compromise internal systems.

Promptly closing connections mitigates these risks by minimizing the opportunity for unauthorized access and reducing the overall surface area susceptible to potential security threats.

5.4.3. Server Access and Testing Protocol

All Users are provided access to the IPND UserTest/Onboarding File Transfer Server environment, where they are required to pass testing criteria before access to IPND Production environment is granted.

Please note the following:

- ALL testing should only be performed on the IPND UserTest/Onboarding environment.
- NEVER transfer REAL user data to IPND UserTest/Onboarding environment.
- NEVER perform testing on the IPND Production environment.

FTS Server Environment	URI	UserID
UserTest/Onboarding	ufts.ipnd.com.au	t_<user>
Production	pfts.ipnd.com.au	p_<user>

Users should confirm that their DNS resolves the URI in the table above. If it doesn't, Users should contact their network team for assistance or lastly update their server's hosts file.

5.5. Connection Testing

5.5.1. CLI: Linux, WSL, PowerShell, CommandPrompt

5.5.1.1. SFTP

When the User invokes sftp they will have a similar interface to standard FTP, such as put, get etc.

```
As a standard user <user>: Linux, WSL, Windows – PowerShell or CommandPrompt

## Ensure your VPN tunnel is running. Ref 2.5 - Checking the Tunnel


## Testing ssh connectivity to the UserTEst/Onboarding FTS

## If you are in the directory where you generated your ssh key-pair:

    sftp -i .ssh/<ShortCompanyName>_ed25519 <Your_IPND_UserAccountName>@ufts.ipnd.com.au
          Connected to <Your_IPND_UserAccountName>@ufts.ipnd.com.au.
          sftp> ls
          archived  download  received  rejected
          sftp> quit


## If you know the full path to your private ssh key file

## eg: <TheCurrentDirectory>/.ssh/<ShortCompanyName>_ed25519

    sftp -i <TheCurrentDirectory>/.ssh/<ShortCompanyName>_ed25519 <Your_IPND_UserAccountName>@ufts.ipnd.com.au
          Connected to <Your_IPND_UserAccountName>ufts.ipnd.com.au.
          sftp> ls
          archived  download  received  rejected
          sftp> quit
```

> *Note:* SFTP is the recommended option to use when testing or connecting to the FTS either interactively or with automated batch processes.

5.5.2. GUI: Windows WinSCP, FileZilla

The 2 most popular SSH based file transfer programs for Windows are WinSCP and FileZilla.
The configuration files for Windows' GUIs are stored as part of the Site details in the GUI setup.

5.5.2.1. WinSCP

Note: WinSCP only uses PuTTY format keys. If the user generated OpenSSH type Keys and select one of these **Private** Keys for authentication, then WinSCP will provide the User the option to convert and save it to PuTTY format (*.ppk).
NB: WinSCP supports SCP and SFTP and will typically use SFTP as the preferred protocol. Users must use SFTP instead of SCP.

Visit the official site, download and install WinSCP.
When the User first launches WinSCP a login dialog will appear. On subsequent launch of the WinSCP application the login dialog screen is available via 'Tabs/Sites/Site Manager'

General
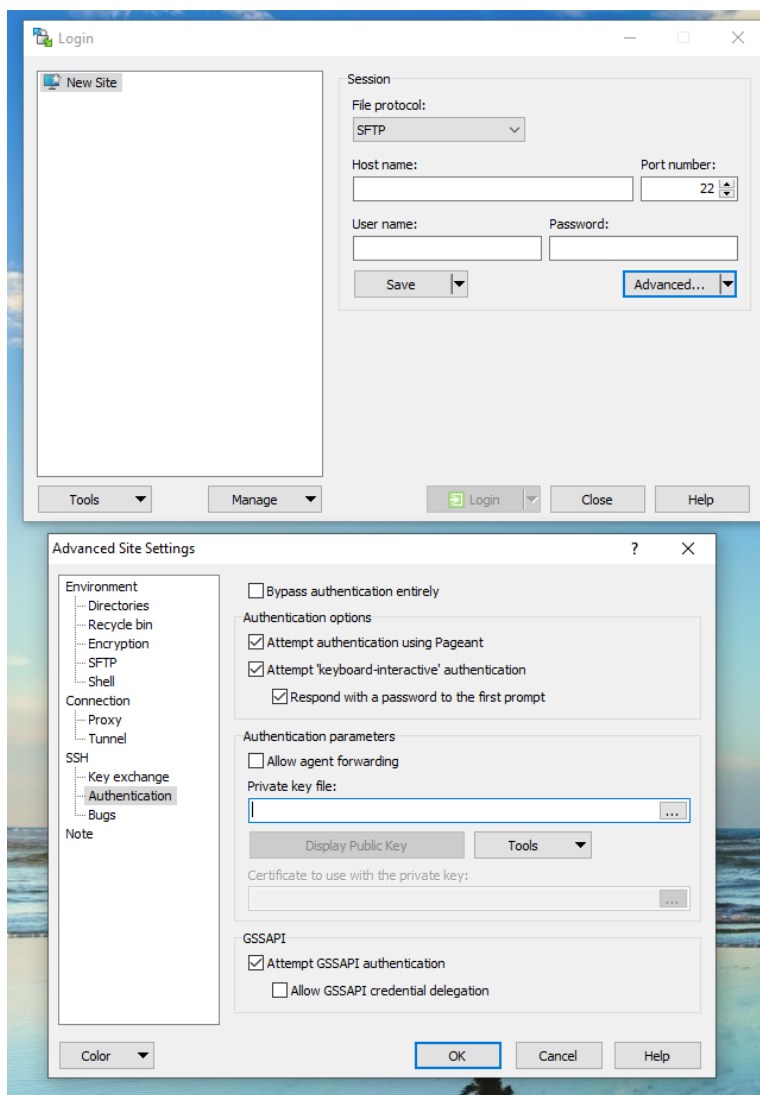
WinSCP: Configuration – initial setup

General

On the dialog:

- Make sure New site node is selected.
- On New site node and make sure the SFTP protocol is selected.
- For UserTest/Onboard Enter the URI ufts.ipnd.com.au into the Host field.
When accessing Production enter pfts.ipnd.com.au into the Host field.
- Enter the Users FTS account name to the Username field: t_username for ufts, p_username for pfts
- Leave the Password field empty
- Click on the Advanced button to open the 2nd screen On the Advanced Site Settings
  - Go to SSH > Authentication page.
  - In Private Key file box select the Users Private SSH Key file.
  - Save and close the Advanced site settings dialog with the OK button.
- Save the site settings using the Save button on the login page. The User will be prompted to name the login session.
- Highlight the new site in the left panel and press the Login using Login button.
- Verify the host key by comparing fingerprints with those collected before (see above).
- If Login is successful the Right-hand panel will show 4 folders known as directories (archived, download, received, rejected)
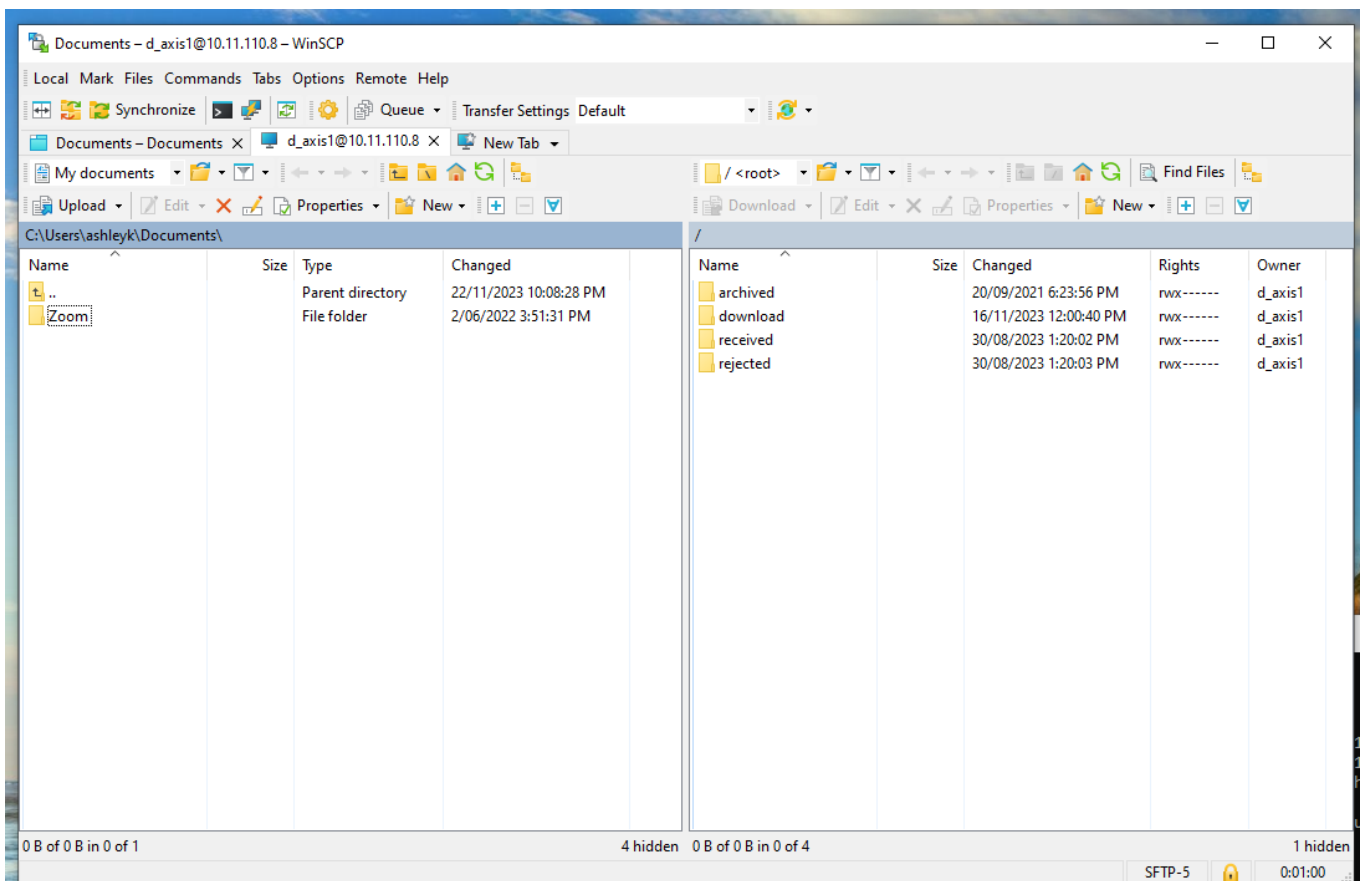
WinSCP: Connected Session

5.5.2.2. FILEZILLA

Visit the official site to download and install FileZilla.

- Open the **FileZilla** software. Press the Start button, search for **FileZilla**, and press **Enter**. This will open the **connect panel**.
- For UserTest/Onboard Enter the URI ufts.ipnd.com.au into the Host field.
  When accessing Production enter pfts.ipnd.com.au into the Host field.
- Enter the Users' FTS account name to the Username field: t_username for ufts, p_username for pfts
- Leave the Password field blank and enter 22 in the Port field
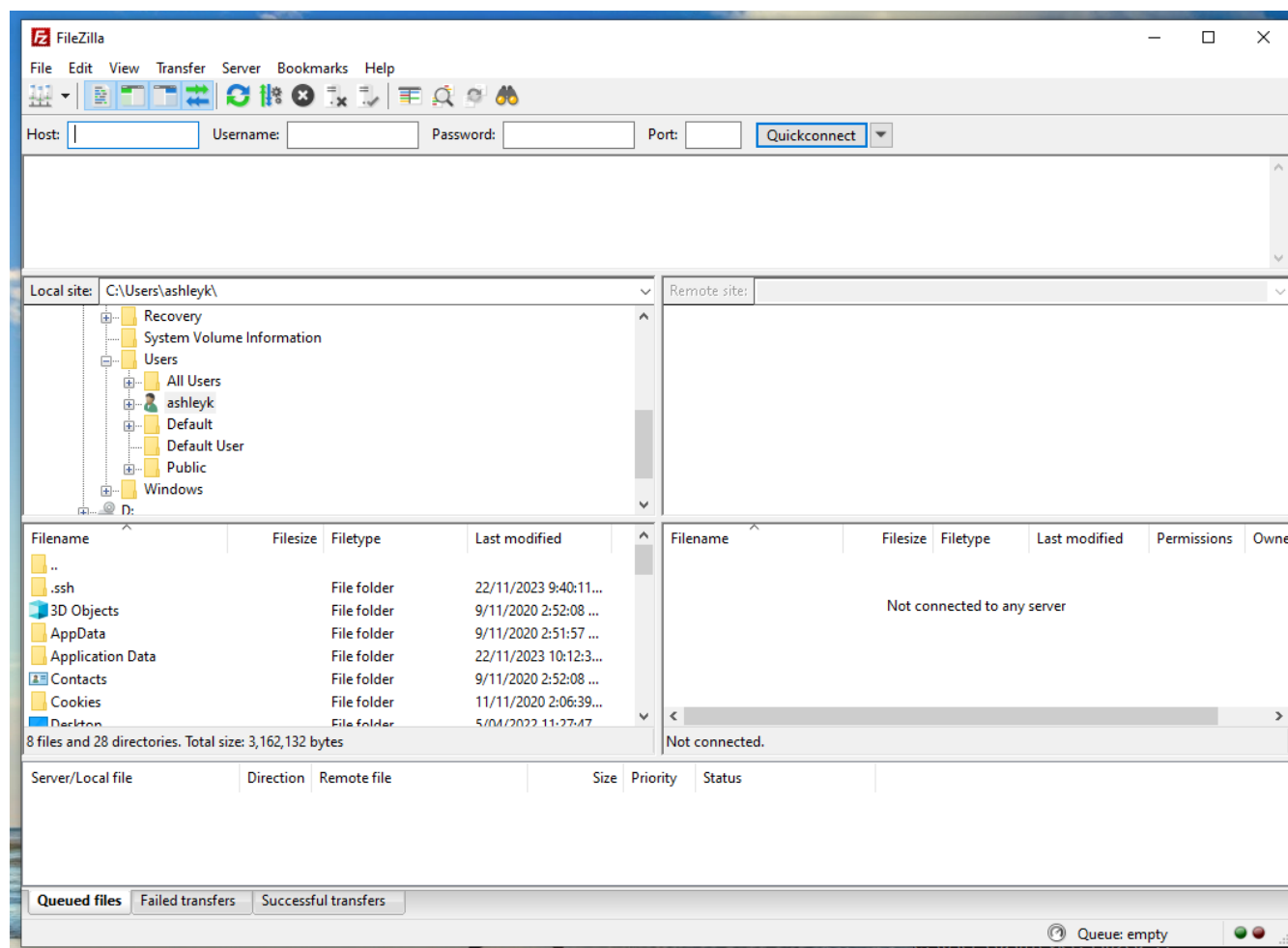
FileZilla: Configuration – initial setup

- Click on Edit and select Settings to open the settings page. On this page select SFTP, click add key and browse and load the Users' **Private** Key (PuTTY or OpenSSH), click OK to save.
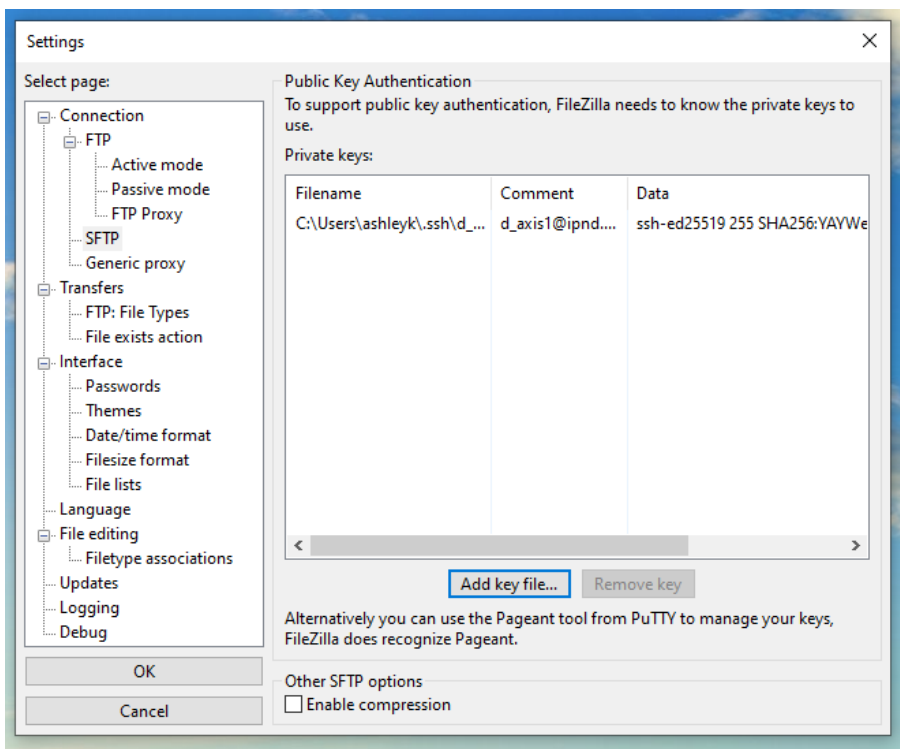
- Connect and the User should see a screen like the one below, where the Right-hand panel will show 4 folders known as directories (archived, download, received, rejected)
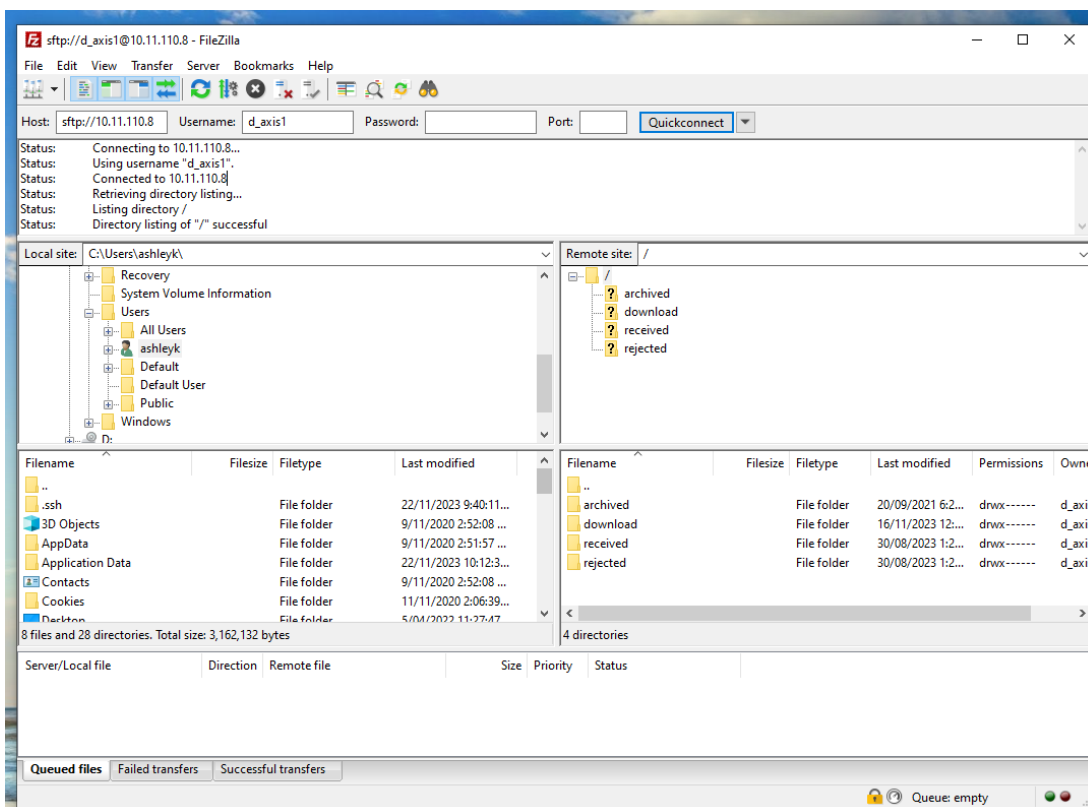
FileZilla: Connected session

5.6.   IPND FTS Directories

Do NOT use absolute paths in your scripts.
e.g. /data/prod/home/p_<user>/download/ ❌

Always use relative path names.
e.g. download/ ✅   or   ./download/ ✅

Each FTS environment consists of the User's home directory and four subdirectories.

1.   download
2.   received
3.   rejected
4.   archived

File uploads are restricted to the Users home directory. Once a file is uploaded, it remains visible in the Users home directory for approximately 5 seconds after which it undergoes initial validation.

All files are then given a timestamp prefix that denotes the time they were received and closed by the Users transfer client. The Files then undergo initial validation. Validated files are moved to the "received" directory. Invalid files are given an error code as a suffix and moved to the "rejected" directory, where they're stored with a zero size.

The initial validation ensures that files adhere to the correct naming format and are GPG ASCII-armored (ASC) encrypted. Files meeting these criteria are forwarded to the primary IPND application server for decryption. Any files that cannot be decrypted are given an error code suffix and sent back to the Users "rejected" folder.

Output files resulting from successful processing are encrypted using the Users GPG Key and sent back to their download directory.

1. download

This directory contains non-archived IPND files encrypted with the Users GPG Key that they may download.

2. received

This directory contains a copy of uploaded IPND files that pass initial validation. The file names are prefixed with a unique timestamp code. These are the files that are sent to the IPND system for processing.

3. rejected

This directory contains zero-byte (i.e. empty) versions of any uploaded IPND files that fail initial validation or are unable to be decrypted on the legacy system (i.e. fail secondary validation)

The files are prefixed with a unique timestamp code and a suffix indicating the reason for failure. Refer to section 8 Messages for a full list of the suffixes and failure reasons. Examples of failure reasons are:

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

4. archived

This directory contains further subdirectories for archived download, received and rejected IPND files. It contains files that are older than 6 months but still within the archive retention period.

6. FILE ENCRYPTION & DECRYPTION: (ALL USERS) DATA PROVIDER + DATA USER + CSP

6.1. 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 encrypt and decrypt files.

6.2. Encrypting Files

There are 3 critical components to encrypting files for the IPND.

1. Files must be ASCII armored
2. Encrypted files MUST be signed with the Users Private Key
3. Files must be encrypted using the IPND Public Key

> Note: Encrypted Files that are not created with these attributes will be rejected and NOT processed by the IPND FTS.

6.2.1. CLI: Linux, WSL, PowerShell, CommandPrompt

As a standard user <user>: Linux, WSL, Windows – PowerShell or CommandPrompt

```
## Check that you have access to your public gpg key and the IPND public gpg key

        gpg -k

                ---------
        pub   ed25519 2024-01-25 [SC]
                AC115A5CF00F1D5A252DBAAA7DCED07E90A15FE7
        uid           [ultimate] CompanyName <CompanyEmail@xxx.yyy.zzz>
        sub   cv25519 2024-01-25 [E]

        pub   rsa2048 2018-01-23 [SC]
                CD4C04C9630DAD81B192A1BC460F8D7C5BC59835
        uid           [ full  ] ipnd-iis (IPND IIS file transfer encryption key.) <ipnd-iis@ipnd.com.au>
        sub   rsa2048 2018-01-23 [E]
```

```
## Check that you have access to your private key

        gpg -K

                ---------
        sec   ed25519 2024-01-25 [SC]
                AC115A5CF00F1D5A252DBAAA7DCED07E90A15FE7
        uid           [ultimate] CompanyName <CompanyEmail@xxx.yyy.zzz>
        ssb   cv25519 2024-01-25 [E]
```

```
## To Encrypt <UnencryptedFile> as <UnencryptedFile>.asc in the same directory
## NB: Your Unencrypted file is unaffected.
        gpg --batch --encrypt --armor --sign --recipient ipnd-iis@ipnd.com.au <UnencryptedFile>
                ## You will be prompted to input your Private gpg key passphrase


## To Encrypt <Unencryptedfile> as <NewDirEncFile>.asc
## NB: Your Unencrypted file is unaffected.
        gpg --batch --encrypt --armor --sign --recipient ipnd-iis@ipnd.com.au --output <NewDirEncFile>.asc <UnencryptedFile>
                ## You will be prompted to input your Private gpg key passphrase
```

6.2.2. GUI: Windows Kleopatra

The Kleopatra start page.
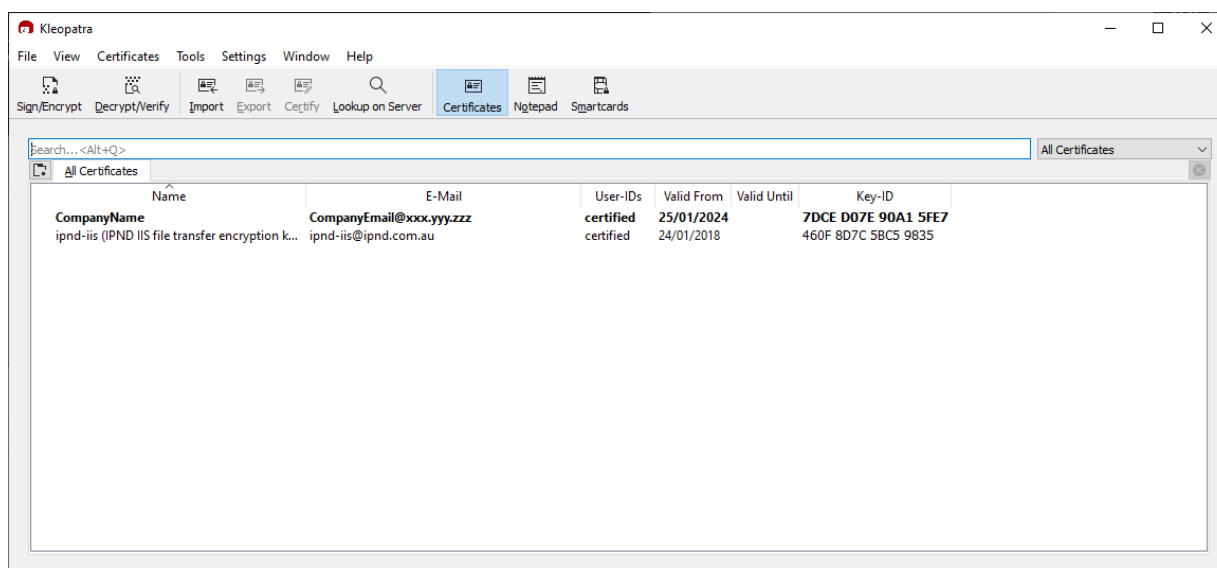
Kleopatra: Certificates screen

Kleopatra: Certify the IPND Public key

Configure ASC armor mode

1. Launch Kleopatra, then click on Settings and select "Configure Kleopatra..."
2. On the "Configure Kleopatra" window click "Crypto Operations"

Ensure that the "Create signed or encrypted files as text files" is ticked, then click "Apply" and then "OK"
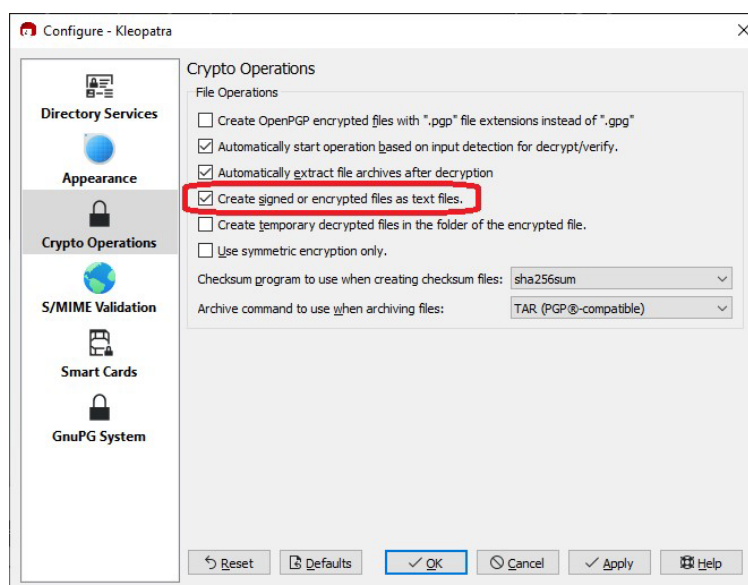
Kleopatra: File encryption settings

Encrypting

1.   Launch Kleopatra and click on "File" and select "Sign/Encrypt" or simply click the 'Sign/Encrypt" icon
2.   Users will be presented with a Files selection screen, browse and select the file to encrypt.
3.   Select the file and click "Open"
4.   On the next screen ensure the following is done
      a.   "Sign as:" as is selected and your key details are selected;
      b.   "Encrypt for me:" is unselected;
      c.   "Encrypt for others:" is selected and then click on the "Show certificate list" icon at the end of this line;
5.   A "Certificate Selection" screen will open, on this page select the 'ipnd-iis key', then click "OK"
Ensure "Encrypt with password.." is unchecked
In the Output box the user must provide their output file a .asc extension
6.   If Users are encrypting all files in a directory, Ensure the "Encrypt/Sign each file separately" is checked.
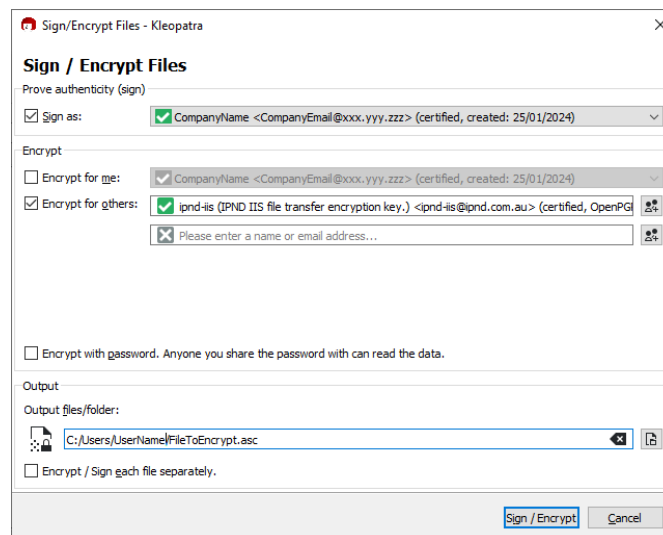
Kleopatra: File Encryption screen

7.   Click "Sign/Encrypt"
Users may receive a popup warning- message that "None of the recipients you are encrypting seems to be your own." Click "Do not ask again" and then click "Continue"
8.   If the Users GPG Key passphrase is not cached, they will receive a popup window requesting their Private Key's passphrase.
9.   If successful, the User will be navigated to a results page with a message
"<FileToEncrypt> → <FileToEncrypt>.asc: **Signing and encryption succeeded.**"
Click on "Finish"

6.3.   Decrypting Files

6.3.1.   CLI: Linux, WSL, PowerShell, CommandPrompt

As a standard user <user>: Linux, WSL, Windows – PowerShell or CommandPrompt

```
## Check that you have access to your private key

        gpg -K

                ---------
        sec   ed25519 2024-01-25 [SC]
              AC115A5CF00F1D5A252DBAAA7DCED07E90A15FE7
        uid           [ultimate] CompanyName <CompanyEmail@xxx.yyy.zzz>
        ssb   cv25519 2024-01-25 [E]


## When decrypting you must specify an output file, otherwise the output is to the screen
## NB: Your Encrypted file is unaffected.

## To Decrypt <Encryptedfile> as <UnEncryptedFile>

        gpg --batch --decrypt --output <UnEncryptedFile> <EncryptedFile>
```

### 6.3.2.   GUI: Windows Kleopatra

Decrypting

1.   Launch Kleopatra and click on "File" and select "Decrypt/Verify" or simply click the 'Decrypt/Verify" icon
2.   Users will be presented with a Files selection screen, browse and select the file to decrypt.
3.   Select the file and click "Open"
4.   If the users GPG Key's passphrase is not cached they will receive a pop-up screen to provide it
5.   If the file was verified/decrypted the User will be presented with a 'Save' screen
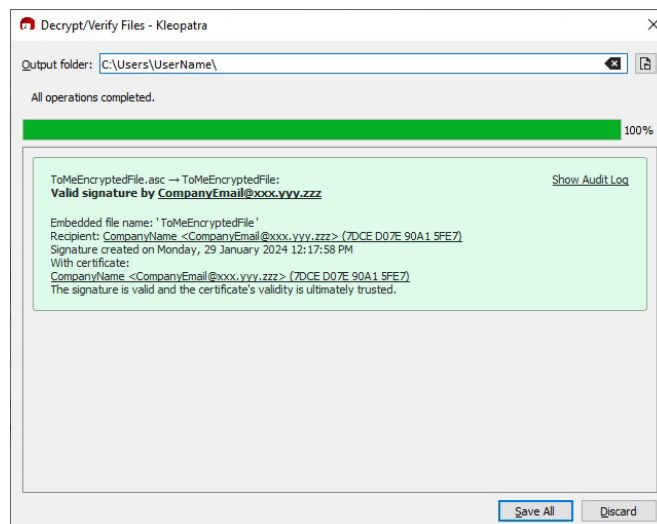
Kleopatra: File Decryption screen

6.   Select/Enter an Output directory and click "Save All" and follow the prompts to save the decrypted file.

7. FILE NAMES: DATA PROVIDER + DATA USER (NA CSPs)

7.1. Data Providers

7.1.1. Upload File

7.1.1.1. CUSTOMER RECORD SYSTEM EXTRACT IPND UPLOAD FILE

Data provider upload file formats are defined in section 6.1.2 of the Data Users and Data Providers Technical Requirement for the IPND document.

Data Provider upload files must be encrypted (refer 6.2 Encrypting Files) with the IPND Public Key and the filename must be in the format:

IPNDUP<XXXXX>.<NNNNNN>.asc

Where

<XXXXX>	is a valid File Source for the Data Provider,
<NNNNNNN>	is the file sequence number with a leading 0
"asc"	indicates that the file has been encrypted using the documented method.

> 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.

Filenames that do not match the expected format will be rejected. The Filesource <XXXXX> must be one associated with the SSH account. This will have been configured when the account is set up.

Example:

An IPND Data Provider with an (SSH) account of p_gentelco has been assigned a filesource of GENTE.

Using this SSH account, tt will only be possible to upload a file in the following format:

IPNDUPGENTE.NNNNNNN.asc

An invalid pattern will result in an empty file in the rejected directory. This empty file will have the same invalid filename, be prefixed with a timestamp, and suffixed with R001.

7.1.2. Download Files

Download files will be encrypted with the Public GPG Key provided by the individual organisation. Refer to Section 6.2 Encrypting Files.

7.1.2.1. IPND ERROR FILE REPORT TO DATA PROVIDERS

For each upload file received from a Data Provider that passes initial reject processing, there will be a corresponding error file. The error file format is described in section 6.1.3 of the Data Users and Data Providers Technical Requirement for the IPND document.

The error file name will be based on the name of the upload file for which it is generated. Each upload file is given a retry number when it is received by the IPND. This retry number is used to differentiate each version of the upload file loaded by an IPND Data Provider for audit trail purposes.

The filename format of the error file in the IIS is described below:

IPNDUP<XXXXX>.<NNNNNN>.<MMM>.err.asc

Where

<XXXXX>	is the File Source for the Data Provider
<NNNNNNN>	is the sequence number of the associated upload file
<MMM>	is the retry number i.e indicates the number of times sequence <NNNNNNN> has been uploaded
"err" <MMM>	indicates an error file associated with sequence <NNNNNNN> and retry <MMM>
"asc"	is the suffix indicating that the file is encrypted using the GPG Public Key associated with the Data Provider

NOTE: All error files include a retry suffix in the IIS environment. There is no symbolic link to the latest .err file as in the IPND Legacy environment.

7.1.2.2. DATA PROVIDER SNAPSHOT FILE

These reports are produced on request from a Data Provider. The output format for these files once decrypted will be as described in Section 6.1.20 of the Data Users and Data Providers Technical Requirement for the IPND document.

The filename format of these reports in the IIS is as follows:

IPNDRU.<XXXXX>.<MMMMMMM>.<NNNNNNN>.<PPP(P)>.asc

Where

<XXXXX>	Is the File Source code for the Data Provider
<MMMMMMM> of the	is the run number identifying the output file. It indicates that the file was part MMMMMMMth run of an extract for this filesource.
<NNNNNNN>	is the file sequence number of the last upload file from the Data Provider with this File Source.
<PPPP> or <PPP>	Span number. All Output On Request (OOR) download files are limited to 100,000 rows of data. The first 100,000 rows are written to span 001. Requests that generate > 100,000 rows are written to additional spanned files. If the number of output files exceeds 999, the spanned number will increment to 1000 onwards.
	If the number of output files exceeds 999, the spanned number will increment to 1000 onwards.
"asc"	is the suffix indicating that the file is encrypted using the GPG Public Key associated with the Data Provider

7.1.2.3. CHANGED DATA PROVIDER REPORT

The Changed Data Provider Report runs monthly on 1st of the month and documents all Data Provider changes from the previous month. The format of the file once decrypted is described in Section 6.1.19 of the Data Users and Data Providers Technical Requirement for the IPND document.

The filename format in the IIS is described below:

IPNDDP<XXXXX>.<NNNNNNN>.asc

Where

<XXXXX>	is the File Source code for the Data Provider
<NNNNNNN>	is the File sequence number with leading 0
"asc"	is the suffix indicating that the file is encrypted using the GPG Public Key associated with the Data Provider

7.1.2.4. DATA PROVIDER QUERY FILE

The DPQF is produced as part of the processing from the Data User Query File Sub-system. This file is described in detail in section 5.2.5.3.1 of the Data Users and Data Providers Technical Requirements for the IPND.

The format of this file once decrypted is described in Section 6.1.17 of the same document.

The filename format in the IIS is described below:

IPNDQP.<XXXXX>.<NNNNNNN>.asc

Where

<XXXXX>	is the File Source for the Data Provider
<NNNNNNN>	is a file sequence number with leading 0
"asc"	suffix indicating that the file is encrypted using the GPG Public Key associated with the Data Provider.

7.2.   Data Users

7.2.1.   Upload File

7.2.1.1.   IPND DATA USER QUERY FILE DUQF

Data Users can upload a Data User Query File. The DUQF Sub-system is described in Section 5.2.5 of the Data Users and Data Providers Technical Requirements for the IPND.

The format of this file is described in Section 6.1.13 of the same document.

The filename format in the IIS is described below:

IPNDQU<XXXXX>.<yyyymmddhhmmss>.asc

Where

<XXXXX>	is a valid File Source for the Data User,
<yyyymmddhhmmss>	is a date stamp indicating when the file was created.
"asc"	indicates that the file has been encrypted using the documented method.

> 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.

Filenames that do not match the expected format will be rejected. The Filesource <XXXXX> must be one associated with the ssh account. This will have been configured when the account is set up.

Example:

An IPND Data User with an (SSH) account of p_genuser has been assigned a filesource of GUSER.

Using this SSH account, it will only be possible to upload a file in the following format:

IPNDQUGUSER.yyyymmddhhmiss.asc

An invalid pattern will result in an empty file in the rejected directory. This empty file will have the same invalid filename, be prefixed with a timestamp and suffixed with R001.

7.2.2. Download Files

7.2.2.1. IPND DOWNLOAD FILES TO DATA USERS

The IPND will produce a distinct Download File for each Data User. There are 6 types of Data Users who receive Download Files. For more information refer to Section 5.2.2.7.2 of the Data Users and Data Providers Technical Requirements for the IPND. File formats for these files are described in Section 6.1.5 to 6.1.11 of the Data Users and Data Providers Technical Requirements for the IPND.

The filename format for these files in the IIS is described below:

IPND<TT>.<XXXXX>.<NNNNNNN>. asc

where

<TT>   refers to the file type and may be one of

"ES" for Emergency Services

"LA" for Law Enforcement Agencies
"DI" for Directory Publishers and Directory Assistance
"LD" for Location Dependent Carriage Service
"RS" for Researcher
"EW" for Early Warning System

<XXXXX>   refers to the individual DU File source code
<NNNNNNN>   refers to a sequence number uniquely enumerating the output file

"asc"   is the suffix indicating that the file is encrypted using the GPG Key associated with the Data User

7.2.2.2. OUTPUT ON REQUEST EXTRACT FILES

Data User output on request files are generated on a request basis. Refer section 5.2.6 to of the Data Users and Data Providers Technical Requirements for the IPND document for more detail. The file format of these files is described in Section 6.1.5 to 6.1.11 of the Data Users and Data Providers Technical Requirements for the IPND.

The filename format of output on request files for data users in the IIS is described below:

IPND<TT>.<XXXXX>.<MMMMMMM>.<NNNNNNN>.<PPP(P)>

Where

"IPND"   literal Identifier String

<TT>   file Type – may be one of the following:

General

"RE" for Emergency Services
"RL" for Law Enforcement Agencies
"RI" for Directory Publishers
"RD" for Location Dependent Carriage Service providers

"RR" for Researchers

"PR" for Health and Public Policy Researchers

<XXXXX>	refers to the DU file source code
<MMMMMMM>	run number uniquely identifying the output file. It indicates that a file was part of the MMMMMMMth run for that download file type <TT>
<NNNNNNN>	file sequence number with leading 0
<PPPP> or <PPP>	Span number. All Output On Request download files are limited to 100,000 rows of data. The first 100,000 rows are written to span 001. Requests that generate > 100,000 rows are written to additional spanned files. If the number of output files exceeds 999, the spanned number will increment to 1000 onwards.
"asc"	suffix indicating the file is encrypted with the GPG Public Key associated with the Data User.

7.2.2.3.   IPND DUQF ERROR FILE

The DUQF Error file is produced as part of the DUQF sub-system described in 5.2.5 of Data Users and Data Providers Technical Requirements for the IPND. The format of these files is described in Section 6.1.14 of the same document.

DUQF err files are produced for every DUQF upload.

The filename format in the IIS is as follows:

IPNDQU<XXXXX>.<yyyymmddhhmmss>.<MMM>.err.asc

Where

<XXXXX>	is the DU file source code
<yyyymmddhhmmss>	is a date time stamp indicating when the file was created
<MMM>	is an optional retry number (in case a duplicate DUQF filename was received)
"err"	indicates an error (status) file
"asc"	suffix indicating that the file is encrypted using the GPG Public Key associated with the Data User

7.2.2.4.   AMALGAMATED QUERY FILE PROCESS (DAQF)

The DAQF file is produced monthly as part of the DUQF sub-system. Refer to section 5.2.5.4 of the of Data Users and Data Providers Technical Requirements for the IPND for details and Section 6.1.18 of the same document for the format.

The filename format of the DAQF in the IIS is as follows:

IPND<TT>.<XXXXX>.<NNNNNNN>.asc

Where

<TT>	refers to the file type and may be one of
	"QE" for a Emergency Services DAQF
	"QL" for a Law Enforcement Agencies DAQF
	"QW" for a Early Warning System DAQF
	"QI" for a Directory Publishers DAQF
	"QD" for a Location Dependent Carriage Service DAQF
	"QS" for a Researcher DAQF
<XXXXX>	is the DU file source
<NNNNNNN>	is a file sequence number with leading 0
"asc"	suffix indicating that the file is encrypted using the GPG Public Key associated with the Data User

8. MESSAGES: DATA PROVIDER ONLY (NA DATA USER + CSP)

Error Files will report success or failure of uploads as documented in Section 6.1.4 of the Data Users and Data Providers Technical Requirements for the IPND document.

NOTE: All error files include a retry suffix in the IIS environment. There is no symbolic link to the latest .err file as in the IPND Legacy environment.

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

Files that are not able to be decrypted will result in:

- an empty file in the "rejected" directory with a R020 suffix
- a copy of the original file in the "received" directory for auditing purposes

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 muse be valid for User
R010	File must be encrypted
R020	File decryption failed
R100	Empty File
R200	File too large. This is an upper extreme limit applied to the encrypted file. It is separate to the row count applied by the legacy system.

9. REFERENCES

9.1. Glossary

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

10. APPENDIX 1: FINGERPRINTS

10.1. SSH KEY FINGERPRINTS

The following section describes how to obtain fingerprints for SSH and GPG Keys.

Never send key fingerprints via email. The IPND Support team will contact users to verify key fingerprints verbally.

10.1.1. CLI: Linux, WSL, PowerShell, CommandPrompt

```
ssh-keygen -lf /path/to/ssh/key
```

or to see an MD5 hash of it if generated using putty

```
ssh-keygen -E md5 -l -f ./t_genba.pub
```

Converting Windows Key to Unix

```
ssh-keygen -i -f keyfile.pub > newkeyfile.pub
```

WINDOWS

When generating using putty key gen look in the Key fingerprint: field

```
ssh-rsa 2048 13:dc:09:cd:4d:86:c9:00:87:47:68:1e:3d:70:fc:26
```

Alternatively load the key and read the fingerprint (you will need to provide the pass phrase to load the key.
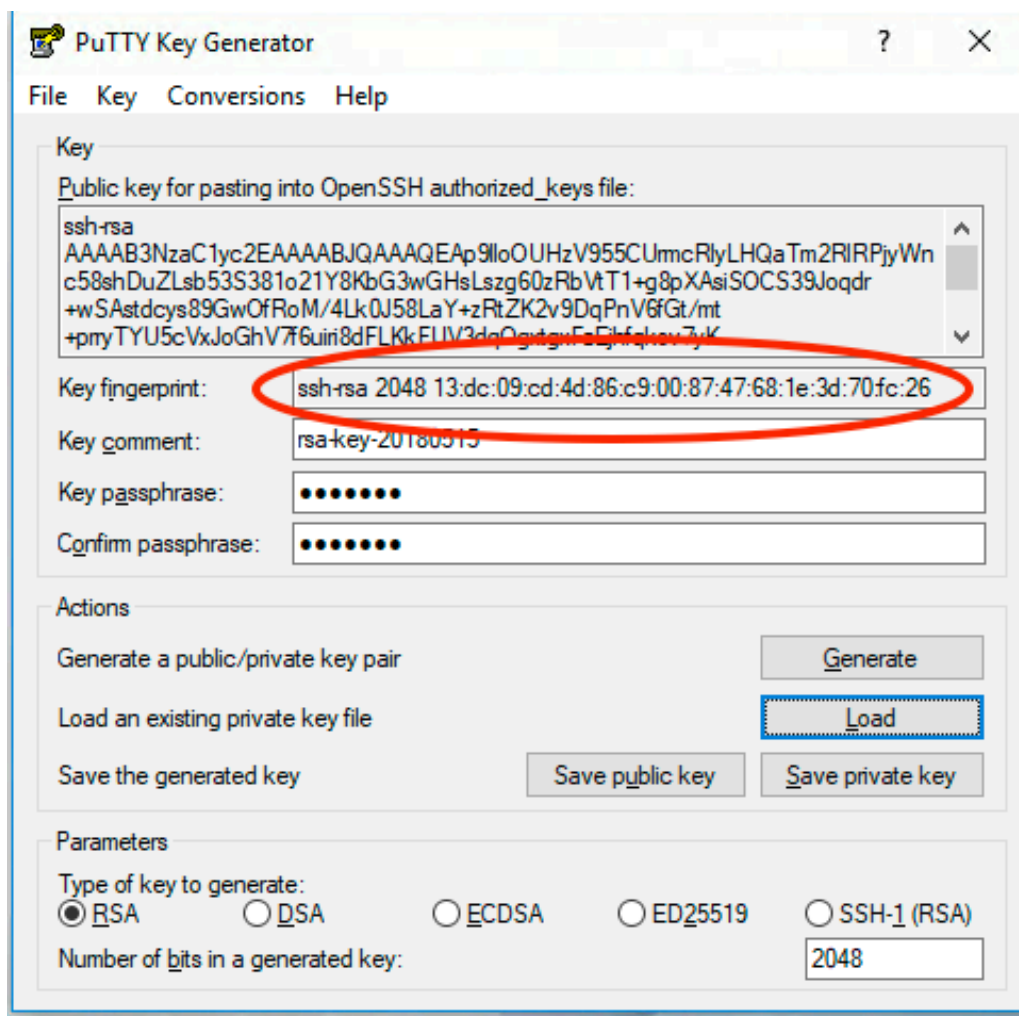
Fingerprint Identification

10.2. GPG FINGERPRINTS

10.2.1. CLI: Linux, WSL, PowerShell, CommandPrompt

Once key has been loaded into keychain:

```
gpg --fingerprint <user>  ## Fingerprint shown in green
pub   rsa2048 2013-06-11 [SC]
      3777 04C9 34DD 3DAB DBED  D500 8947 60EF 77FD D883
uid           [ full ] User Name <user@email.com>
sub   rsa2048 2013-06-11 [E]
```

Checking file if not loaded:

```
gpg <key>.asc
gpg: WARNING: no command supplied.  Trying to guess what you mean ...
pub   rsa2048 2013-06-11 [SC]
      377704C934DD3DABDBEDD500894760EF77FDD883
uid           User Name <user@email.com>
sub   rsa2048 2013-06-11 [E]
```

10.2.2. GUI: Windows - Kleopatra

When GPG Key pair is created.
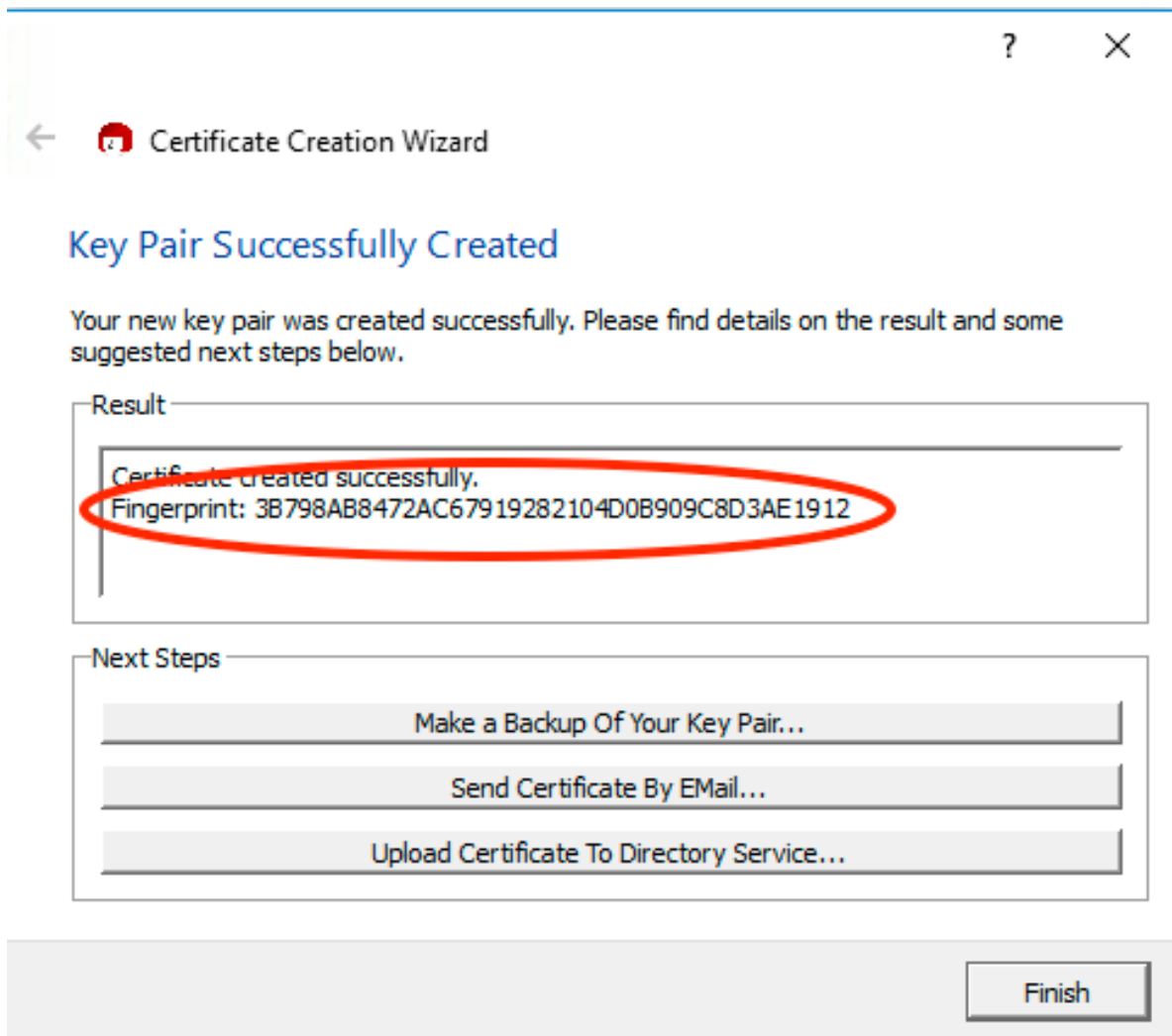
GPG Fingerprint - Kleopatra

After Key Pair has been generated:

Double click on the Key Pair.
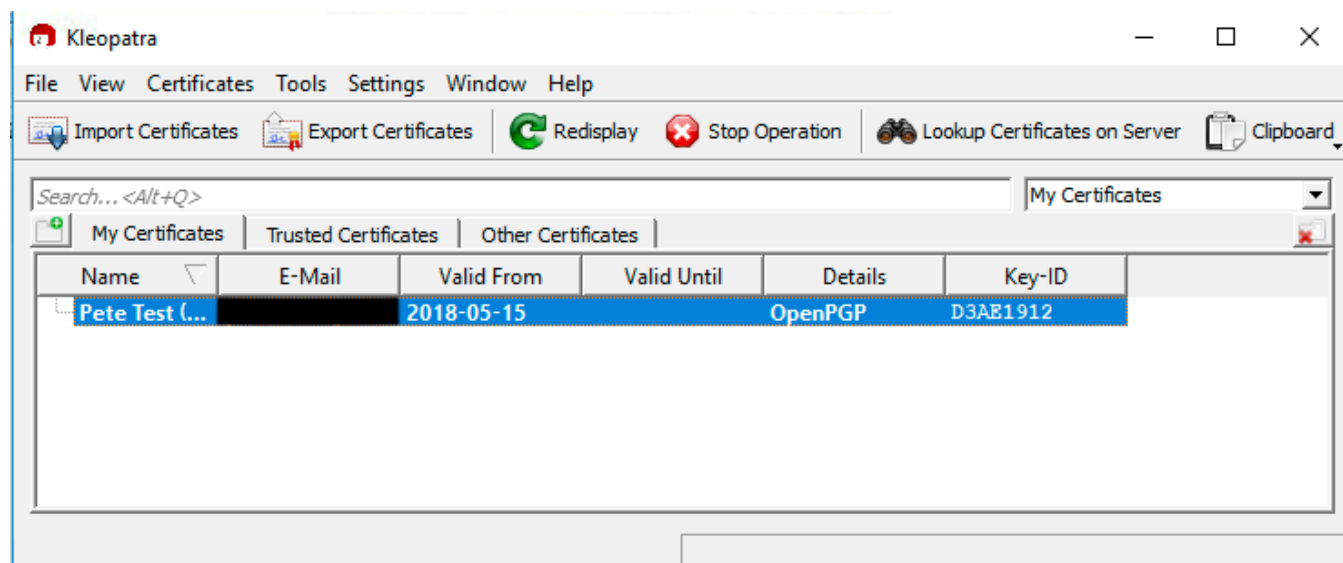
GPG Fingerprint - Kleopatra - post create
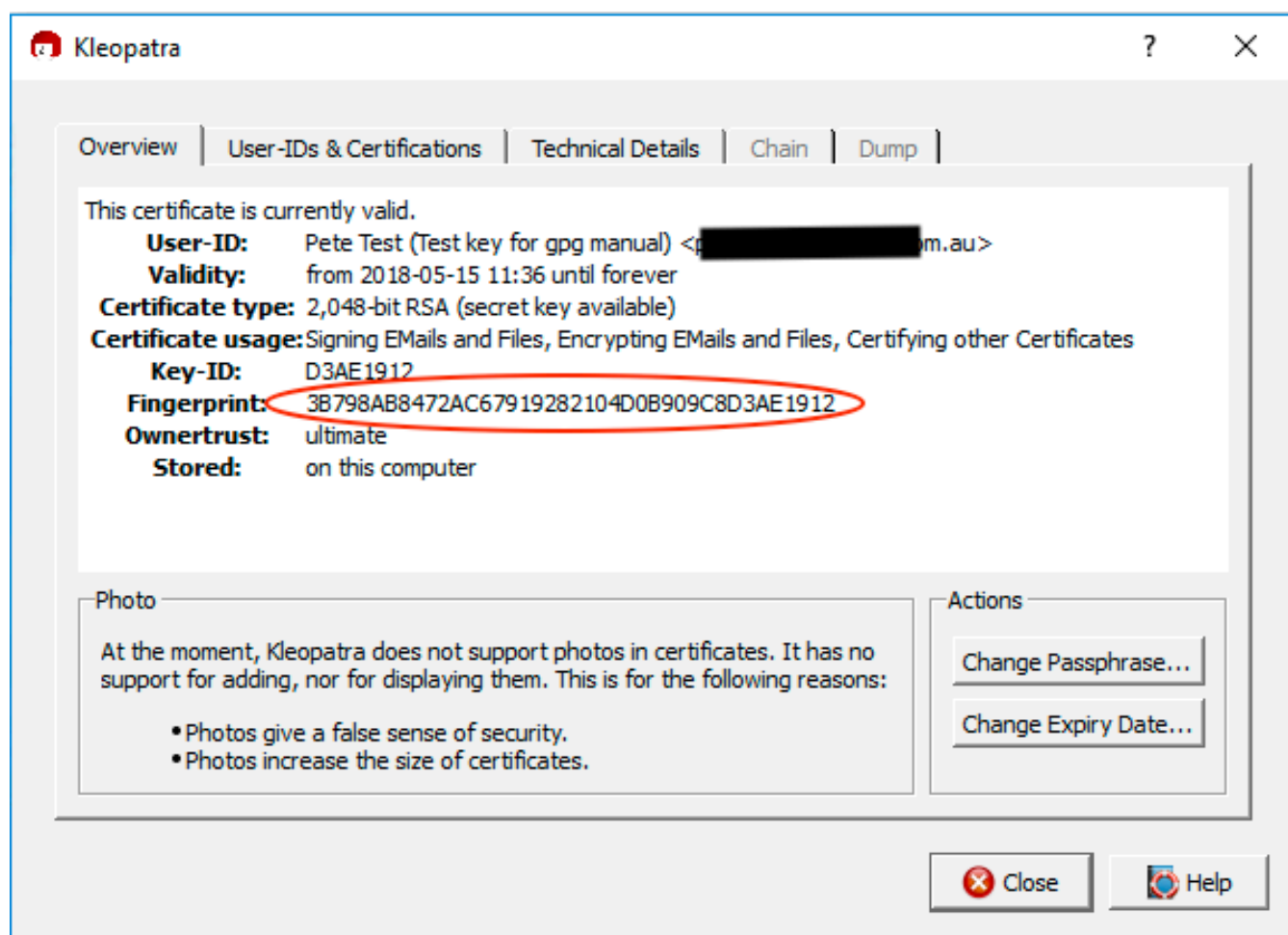
GPG Fingerprint - Kleopatra - post create 2

11. APPENDIX 2: OPENVPN PROFILE EXAMPLE

The VPN Profile that Users download (Ref: 2.3-Downloading VPN Profile and OpenVPN Client) should look similar to the one shown below. If it doesn't try downloading again.

```
# Automatically generated OpenVPN client config file
# Generated on Thu May  3 09:30:38 2018 by pvpn01
# Note: this config file contains inline private keys
#      and therefore should be kept confidential!
# Note: this configuration is user-locked to the username below
# OVPN_ACCESS_SERVER_USERNAME=<user>
# Define the profile name of this particular configuration file
# OVPN_ACCESS_SERVER_PROFILE=<user>@gw1.ipnd.com.au/AUTOLOGIN
# OVPN_ACCESS_SERVER_AUTOLOGIN=1
# OVPN_ACCESS_SERVER_CLI_PREF_ALLOW_WEB_IMPORT=True
# OVPN_ACCESS_SERVER_CLI_PREF_BASIC_CLIENT=False
# OVPN_ACCESS_SERVER_CLI_PREF_ENABLE_CONNECT=True
# OVPN_ACCESS_SERVER_CLI_PREF_ENABLE_XD_PROXY=True
# OVPN_ACCESS_SERVER_WSHOST=gw1.ipnd.com.au:443
# OVPN_ACCESS_SERVER_WEB_CA_BUNDLE_START
<information removed>
# OVPN_ACCESS_SERVER_IS_OPENVPN_WEB_CA=0
# OVPN_ACCESS_SERVER_ORGANIZATION=Telstra IPND IIS
setenv FORWARD_COMPATIBLE 1
client
server-poll-timeout 4
nobind
remote gw1.ipnd.com.au 1194 udp
remote gw1.ipnd.com.au 443 tcp
dev tun
dev-type tun
ns-cert-type server
setenv opt tls-version-min 1.0 or-highest
reneg-sec 604800
sndbuf 100000
rcvbuf 100000
# NOTE: LZO commands are pushed by the Access Server at connect time.
# NOTE: The below line doesn't disable LZO.
comp-lzo no
verb 3
setenv PUSH_PEER_INFO
<ca>
<information removed>
</ca>
<cert>
<information removed>
</cert>
<key>
<information removed>
</key>
key-direction 1
<tls-auth>
<information removed>
</tls-auth>
<information removed>
```

12. APPENDIX 3: ADVANCED BATCH SFTP TECHNIQUES

12.1. Paths

Do NOT use absolute paths in scripts.
e.g
/data/prod/home/p_<user>/download/ ❌

Always use Relative path names.
e.g.
download/ ✅
./download/ ✅

12.2. Directories

Each FTS environment consists of the User's home directory and four subdirectories. Files must only be uploaded to the home directory. Processed files and files available for download can be found in the subdirectories which are:

1. download
2. received
3. rejected
4. archived

1. download

This directory contains non-archived IPND files that Users may download.

2. received

This directory contains a copy of uploaded IPND files that pass initial validation. The file names are prefixed with a unique timestamp code. It is these files that are sent to the IPND system for processing.

Note: The files will appear in this directory ~ 5 seconds after being received.

> Note: files must only be uploaded into the user's home directory, not any other subdirectory.

3. rejected

This directory contains zero-byte (i.e. empty) versions of any uploaded IPND files that fail initial validation or are unable to be decrypted on the legacy system

The files are prefixed with a unique timestamp code and a suffix indicating the reason for failure. Refer to section 8 Messages for a full list of the suffixes and failure reasons. Examples of failure reasons are:

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

4. archived

This directory contains further subdirectories for archived download, received and rejected IPND files. It will contain files that are older than 6 months but still within the archive retention period.

12.3. Simple Directory Listing via SFTP

Users can use SFTP for file system operations such as listing directories, changing directories, and transferring files.

Most of the standard options for directory listing are available through SFTP.

Various examples with dummy data shown below

Note: Commands after the " " are interpreted by the local OS.

Various examples with dummy data shown below.

12.3.1. Short list the contents of your home directory

For example: $ echo "ls" | sftp user@host

archived
download
received
rejected

12.3.2. Long list the contents of your home directory

$ echo "ls -l" | sftp user@host

total 16

dr-xr-x---+ 3 root root 4096 Feb 28 2018 archived
dr-xr-x---+ 2 root root 4096 Dec 3 2018 download
dr-xr-x---+ 2 root root 4096 Dec 3 2018 received
dr-xr-x---+ 2 root root 4096 Dec 3 2018 rejected

12.3.3. List the directories of your home directory

$ echo "ls *" | sftp user@host
archived/   download/   received/   rejected/

12.4.   Advanced Directory Listing via SSH

12.4.1. List rejected/directory contents, long format, sorted by time (oldest first).

$ echo "ls -l rejected/" | sftp -P 22 user@host

total 12884

-r--r----- 1 t_USERX t_USERX   1314 Dec 3 2018 1543796454445212:IPNDQP.USERX.0000003.asc.R001
-r--r----- 1 t_USERX t_USERX   1254 Oct 10 2018 1539142898825600:IPNDQP.USERX.0000001.asc.R001
-r--r----- 1 t_USERX t_USERX   1254 Oct 10 2018 1539142700250161:fred.R001
-r--r----- 1 t_USERX t_USERX   1254 Oct 10 2018 1539142420638527:IPNDQP.USERX.0000001.asc.R001
-r--r----- 1 t_USERX t_USERX   6342 Oct 3 2018 1538524413133162:IPNDUPXXXXX.0000001.R001
-r--r----- 1 t_USERX t_USERX   6342 Oct 3 2018 1538523863403865:IPNDUPFRED.0000001.R001
-r--r----- 1 t_USERX t_USERX   0 Aug 24 2018 1535091432766621:IPNDUPUSERX.0000099.asc.R100
-r--r----- 1 t_USERX t_USERX   1046 Jun 13 2018
1528853104696409:IPNDUPUSERX.0000001.001.err.asc.R001
-r--r----- 1 t_USERX t_USERX   1046 Jun 6 2018
1528263911552345:IPNDUPUSERX.0000001.001.err.asc.R001
-r--r----- 1 t_USERX t_USERX 13137906 May 16 2018 1526438243657110:IPNDUPUSERX.0012294.R001
-r--r----- 1 t_USERX t_USERX   1046 May 3 2018
1526962263877394:IPNDUPUSERX.0000001.001.err.asc.R001

```
-r--r----- 1 t_USERX t_USERX    1197 Mar 21  2018 1521607917145442:IPNDUPUSERX 0000006.asc.R010
-r--r----- 1 t_USERX t_USERX    1197 Mar 21  2018 1521607821216482:IPNDUPUSERX 0000006.asc.R010
```

12.4.2. Verify IIS received file IPNDUPUSERX.0000002.asc (List ALL)

$ echo "ls received/*IPNDUPUSERX.0000002.*" | sftp -P 22 user@host

```
received/1526438542795880:IPNDUPUSERX.0000002.asc
received/1543796520382690:IPNDUPUSERX.0000002.asc
received/1543796971141478:IPNDUPUSERX.0000002.asc
received/1543796949131203:IPNDUPUSERX.0000002.asc
```

12.4.3. List ALL error files for IPNDUPUSERX.0000002

$ sftp -P 22 user@host <<< $'ls download/IPNDUPUSERX.0000002.???.err.asc'

```
download/IPNDUPUSERX.0000002.001.err.asc
download/IPNDUPUSERX.0000002.002.err.asc
download/IPNDUPUSERX.0000002.003.err.asc
download/IPNDUPUSERX.0000002.004.err.asc
```

12.4.4. List the latest error files for IPNDUPUSERX.0000002

$ sftp -P 22 user@host <<< $'ls download/IPNDUPUSERX.0000002.*.err.asc'|tail -1

```
 download/IPNDUPUSERX.0000002.004.err.asc
```

12.5. Downloading files

12.5.1. Download IPNDUPUSERX.0000002.004.err.asc

$ sftp -P 22 user@host <<< $'get download/IPNDUPUSERX.0000002.004.err.asc
DestinationDir/IPNDUPUSERX.0000002.004.err.asc'

12.5.2. Download the latest error file of uploaded file

```
# Set the upload file name
UPLOADFILE="IPNDUPUSERX.0000002.asc"
BASENAME="${UPLOADFILE%.asc}"


# Step 1: List all received files matching the base name and count them
sftp -P 22 user@host <<< $"ls received/*${BASENAME}.*" | tee received_list.txt


# Get the count (assuming file exists)
COUNT=$(wc -l < received_list.txt)
```

Step 2: Use the count to construct the expected .err.asc filename

EXPECTED_FILE="download/${BASENAME}.$(printf '%03d' "$COUNT").err.asc"

Step 3: Try to download that file

sftp -P 22 user@host <<< $"get $EXPECTED_FILE"

12.5.3.　　Deprecation of SCP

OpenSSH (v9.0+) has deprecated the legacy SCP protocol by default, so existing Users must migrate to use SFTP instead of SCP. SFTP is a standardized protocol (RFC 4254/4256) with robust features. SCP offers limited functionality and lacks modern features and proper error handling. While SCP is currently supported by the IPND system, SCP will be deprecated in the future on the IPND system, as it is not a formally standardized protocol.

The table below shows SSH/SCP commands in column 2 and their equivalent commands using SFTP in column 3.

Purpose	ssh/scp command (Unless specified commands are on 1 line)	sftp command (Unless specified commands are on 1 line)

(1) Short list the contents of your home directory	`ssh -q -p22 user@host ls`	```echo "ls"	sftp -q -p22 user@host```
			 or
			 ```sftp -q -p22 user@host << EOF```
			 `ls`
			 `EOF`
			 or
			 `echo "ls" > sftp_commands.txt`
			 `sftp -q -p22 -b sftp_commands.txt user@host`
			 or
			 `sftp -q -P 22 user@host <<< $'ls'`

(2) Long list the contents of your home directory	`ssh -q -p22 user@host ls -l`	```echo "ls -l"	sftp -q -p22 user@host```
			 or
			 ```sftp -q -p22 user@host << EOF```
			 `ls -l`
			 `EOF`
			 or
			 `echo "ls -l" > sftp_commands.txt`
			 `sftp -q -p22 -b sftp_commands.txt user@host`
			 or
			 `sftp -q -P 22 user@host <<< $'ls -l'`

(3) List the directories of your home directory	`ssh -q -p22 user@host "ls -d ./*/"`	```echo "ls -l ./*/"	sftp -q -p22 user@host|awk '$1 ~ /^d/ { print $NF}'```
			 or
			 ``sftp -q -p22 user@host << EOF
				awk '$1 ~ /^d/ { print $NF}'```
				 `ls -l ./*/`
				 `EOF`
				 or
				 `echo "ls -l ./*/" > sftp_commands.txt`
				 ```sftp -q -p22 -b sftp_commands.txt user@host|awk '$1 ~ /^d/ { print $NF}'```
				 or
				 ``sftp -q -P 22 user@host <<< $'ls -l'
					awk '$1 ~ /^d/ {print $NF}'```

(4) List rejected/directory contents, long format, sorted by time (oldest first)	`ssh -q -p22 user@host ls -t rejected`	```echo "ls -lt rejected"	sftp -q -p22 user@host```
			 or
			 ```sftp -q -p22 user@host << EOF```
			 `ls -lt rejected`
			 `EOF`
			 or
			 `echo "ls -lt rejected" > sftp_commands.txt`
			 `sftp -q -p22 -b sftp_commands.txt user@host`
			 or
			 `sftp -q -P 22 user@host <<< $'ls -t rejected'`

(5) Recursively list contents of home directory and all subdirectories	`ssh -q -p22 user@host ls -lR`	`# Direct sftp equivalent for 'ls -lR' is not available`

General

(6) Verify IIS received file IPNDUPUSERX.0000002.asc (List ALL)	`ssh -q -p22 user@host "ls received/IPNDUPUSERX.0000002.asc"`	```echo "ls received/IPNDUPUSERX.0000002.asc" | sftp -q -p22 user@host or sftp -q -p22 user@host << EOF ls received/IPNDUPUSERX.0000002.asc EOF or echo "ls received/IPNDUPUSERX.0000002.asc" > sftp_commands.txt sftp -q -p22 -b sftp_commands.txt user@host or sftp -q -P 22 user@host <<< $'ls received/IPNDUPUSERX.0000002.asc'```
(7) List ALL error files for IPNDUPUSERX.0000002	`ssh -q -p22 user@host "ls download/IPNDUPUSERX.0000002.???.err.asc"`	```echo "ls download/IPNDUPUSERX.0000002.???.err.asc" | sftp -q -p22 user@host or sftp -q -p22 user@host << EOF ls download/IPNDUPUSERX.0000002.???.err.asc EOF or sftp -q -P 22 user@host <<< $'ls download/IPNDUPUSERX.0000002.???.err.asc'```
(8) List the latest error files for IPNDUPUSERX.0000002	`ssh -q -p22 user@host "ls -1 download/IPNDUPUSERX.0000002.*.err.asc"|tail -1`	```echo "ls -1 download/IPNDUPUSERX.0000002.*.err.asc" | sftp -q -p22 user@host | tail -1 or sftp -q -p22 user@host <<EOF | tail -1 ls -1 download/IPNDUPUSERX.0000002.*.err.asc EOF or sftp -q -P 22 user@host <<< $'ls -1 download/IPNDUPUSERX.0000002.*.err.asc' | tail -1```
(9) Download IPNDUPUSERX.0000002.004.err.asc	`scp -q -p22 user@host:download/IPNDUPUSERX.0000002.004.err.asc DestinationDir`	```echo "get download/IPNDUPUSERX.0000002.004.err.asc" | sftp -q -p22 user@host or sftp -q -p22 user@host <<EOF get download/IPNDUPUSERX.0000002.004.err.asc EOF or sftp -q -P 22 user@host <<< $'get download/IPNDUPUSERX.0000002.004.err.asc DestinationDir/'```
(10) Download the latest error file of uploaded file where the bash variable UPLOADFILE holds the uploadfilename	```#1. Set Variable UPLOADFILE="IPNDUPUSERX.0000002.asc" #2. Run command scp -P22 user@host:`ssh -q -p 22 user@host ls download/${UPLOADFILE%.asc}.\\*$(ssh -q -p22 user@host ls "received/*${UPLOADFILE%.asc}.*"|wc -l).err.asc` <DestDir>```	```#1. Set Variable UPLOADFILE="IPNDUPUSERX.0000002.asc" #2. Set 2nd Varaiable COUNT=$(echo "ls received/${UPLOADFILE%.asc}." | sftp -q -p22 user@host | wc -l) #3. Set 3rd variable FILENAME=$(echo "ls -1 download/${UPLOADFILE%.asc}.*${COUNT}.err.asc" | sftp -q -p22 user@host) #4. Run command sftp -q -p22 user@host <<EOF get $FILENAME EOF or # 1. Set Variable UPLOADFILE="IPNDUPUSERX.0000002.asc" # 2. Run command using sftp to find the latest file```

| | | ```
# Get the list of files in the "received" directory and count matching entries

FILE_PATTERN=$(sftp -q -P 22 user@host <<< $'ls received/*'"${UPLOADFILE%.asc}".'*' | wc -l)

# Determine the latest error file from the download directory

LATEST_FILE=$(sftp -q -P 22 user@host <<< $'ls download/'"${UPLOADFILE%.asc}".'*${FILE_PATTERN}.err.asc')

# Download the file to the destination directory

sftp -q -P 22 user@host <<< $'get '"${LATEST_FILE}"' <DestDir>'
``` |

13. APPENDIX 4: TROUBLE SHOOTING VPN CONNECTION ISSUES

13.1.1. Check application logs

In Windows click on paper scroll icon on the top right-hand side to view app logs.

In linux check systemd logs or application logs depending on how they have been configured in the User app to start.

13.1.2. Check DNS settings

Re-confirm the DNS settings and resolution of the gw1.ipnd.com.au URL. Ref 2.4.1-Pre VPN Client Installation DNS resolution check

13.1.3. Check Firewall settings

Check that UDP 1194 and TCP 443 is not blocked by your Firewall.

13.1.4. MTU path issues

Always proceed cautiously with network changes. Users should document modifications for potential rollback. If issues persist, seek assistance from network administrators or support for further troubleshooting.

MTU path issues often cause packet fragmentation. Packet fragmentation in networking is problematic because it slows down data transmission, increases latency, wastes bandwidth, raises error probability, adds complexity, and poses security risks. Avoiding fragmentation is crucial for optimal network performance and efficiency. Fragmentation can cause connection issues with firewalls by leading to out-of-sequence packets, packet loss, reordering, security vulnerabilities, resource strain, and susceptibility to denial-of-service attacks.

13.1.4.1. CHECK IP PATH MTU DISCOVERY IS ENABLED

Check IP Path MTU Discovery is enabled

13.1.4.2. CLI: LINUX, WSL

A value of 0 means IP Path MTU Discovery is enabled, while a value of 1 means it's disabled.

```
# To Check run: sysctl net.ipv4.ip_no_pmtu_disc
```

```
# To Enable run: sudo sysctl -w net.ipv4.ip_no_pmtu_disc=0
```

13.1.4.3. GUI: WINDOWS

```
Check that the following registry parameter is 0
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\IPEnableRouter
```

```
To enable:
netsh interface ipv4 set subinterface "Your Network Interface Name" mtu=1500 store=persistent
```

13.1.4.4.   CLI: LINUX, WSL – RUN MTUSWEEP.SH

Run the mtusweep.sh script on any Linux/WSL instance in the same network. Ref 14 - Appendix 5 – Linux/WSL mtusweep script. OpenVPN uses a default (max) MTU of 1500. If mtusweep.sh identifies that the user has an MTU < 1500, then they must adjust the users VPN config file to use their lower non-fragmenting MTU value.

Note: If users alter the MTU in their VPN config file, do NOT set the MTU in the VPN config to > 1500, as this is the Maximum that OpenVPN uses.

As a standard user <user>: **Linux/WSL only**

```
./mtusweep.sh

Sending 32 bytes to www.ibm.com
----> Contiguous
Sending 750 bytes to www.ibm.com
----> Contiguous
Sending 1125 bytes to www.ibm.com
----> Contiguous
..
Sending 1272 bytes to www.ibm.com
----> Contiguous
Sending 1275 bytes to www.ibm.com
----> Fragmented
Sending 1273 bytes to www.ibm.com
----> Fragmented
Sending 1272 bytes to www.ibm.com
----> Contiguous

1272 bytes is the largest contiguous packet size (1300 includes 28 ICMP/IP Headers)
        Your MTU should be set to 1300
```

Try modifying the openvpn config file then add a line for the max mtu size that mtusweep.sh identifies eg: 1300

eg:
..
setenv PUSH_PEER_INFO

tun-mtu 1300

<ca>
..

Start the VPN client, and check the MTU.

As a standard user <user>: **Linux/WSL only**

```
ip a s|grep tun
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1300 qdisc pfifo_fast state UNKNOWN group default qlen 100
```

14. APPENDIX 5: LINUX/WSL MTUSWEEP SCRIPT

The `mtusweep.sh` is a script designed outbound testing to find the Maximum Transmission Unit (MTU) for a network where it's run. The MTU is the maximum packet size that can be sent over a network without fragmentation.

The script iteratively tests different packet sizes to determine the largest contiguous packet that can be successfully transmitted and received without fragmentation, ultimately suggesting an optimal MTU for the network.

mtusweep.sh

```
#!/bin/sh
# MTU Sweeping Script
# Test and determine the Maximum Transmission Unit (MTU) for network connectivity

export PATH=$PATH:"/usr/sbin:/bin:/usr/bin:/sbin"

MTU="32"
STEP="750"
MAX_ITERATION="999"
PACKETS_HEADER="28"
HOST_1="www.ibm.com"
HOST_2="www.google.com"
HOST_3="www.microsoft.com"
HOST_EXT="$1"

PrintHelp() {
    echo "MTU Sweeping Script"
    echo "Usage: $0 [external_host]"
    echo "Test and determine the Maximum Transmission Unit (MTU) for network connectivity."
    echo "If [external_host] is not provided, the script uses default internal hosts."
    echo
    echo "Options:"
    echo "  -h, --help    Show this help message."
    exit 0
}

PingHost() {
    # Ping the host with one ICMP-echo packet of variable size, and filter the output
    if [ "$HOST" != "" ]; then
        echo "Sending $1 bytes to $HOST"
        ping -c 1 -M do -s $1 $HOST > /dev/null 2>&1
        RESULT=$?
        # Recursive output message
        if [ "$RESULT" = "0" ]; then
            echo "----> Contiguous"
        else
            echo "----> Fragmented"
        fi
        echo
    fi
}

# Check for help option
if [ "$1" = "-h" ] || [ "$1" = "--help" ]; then
    PrintHelp
fi

# Identify the 1st host from the list that is pingable. Use the initial MTU value(32)
for HOST in "$HOST_EXT" "$HOST_1" "$HOST_2" "$HOST_3"; do
    PingHost $MTU
    if [ "$RESULT" = "0" ]; then
        # If the 1st host succeeds, break and use it
        HOSTGOOD="1"
        break
    else
        HOSTGOOD="0"
    fi
```

```
    done

    # No valid hosts found: exit...
    if [ "$HOSTGOOD" != "1" ]; then
        echo "No reachable hosts (tried): $HOST_EXT $HOST_1 $HOST_2 $HOST_3"
        exit 1
    fi

    # The host is pingable, so let's go on with larger packets...
    MTU="$STEP"
    ITERATION="0"
    while [ "$ITERATION" -lt "$MAX_ITERATION" ]; do
        STEP=`expr "$STEP" / 2 + "$STEP" % 2`
        PingHost $MTU
        if [ "$RESULT" = "0" ]; then
            if [ "$MTU" = "$MTU_LASTGOOD" ]; then
                break
            else
                MTU_LASTGOOD="$MTU"
                MTU=`expr "$MTU" + "$STEP"`
            fi
        else
            MTU=`expr "$MTU" - "$STEP"`
        fi
        ITERATION=`expr "$ITERATION" + 1`  # Limit the max loop retries in case of successive host failures
    done

    # Maximum retries value reached: exit...
    if [ "$ITERATION" = "$MAX_ITERATION" ]; then
        echo
        echo "Test limit exceeded"
        exit 2
    fi

    # Add ICMP default header to the found value
    MTU=$((MTU + PACKETS_HEADER))
    echo
    echo "$MTU_LASTGOOD bytes is the largest contiguous packet size ($MTU includes $PACKETS_HEADER ICMP/IP Headers)"
    echo
    echo "Your MTU should be set to $MTU"
    echo
    ###################
    ./mtusweep.sh
    Sending 32 bytes to www.ibm.com
    ----> Contiguous
    Sending 750 bytes to www.ibm.com
    ----> Contiguous
    Sending 1125 bytes to www.ibm.com
    ----> Contiguous
    Sending 1313 bytes to www.ibm.com
    ----> Contiguous
    Sending 1407 bytes to www.ibm.com
    ----> Contiguous
    Sending 1454 bytes to www.ibm.com
    ----> Contiguous
    Sending 1478 bytes to www.ibm.com
    ----> Fragmented
    Sending 1466 bytes to www.ibm.com
    ----> Contiguous
    Sending 1472 bytes to www.ibm.com
    ----> Contiguous
    Sending 1475 bytes to www.ibm.com
    ----> Fragmented
    Sending 1473 bytes to www.ibm.com
    ----> Fragmented
    Sending 1472 bytes to www.ibm.com
    ----> Contiguous

    1472 bytes is the largest contiguous packet size (1500 includes 28 ICMP/IP Headers)
    Your MTU should be set to 1500
```

15. APPENDIX 6: IPND SFTP BANNER

14.1.1. Overview

Upon connecting to the IPND system in non-quiet mode via SFTP, Users are presented with a login banner outlining terms of use and indicating the current system status.

This banner serves two main purposes:

1. **Legal and Security Notice** – It informs Users that their activities may be monitored and that unauthorized access is prohibited.
2. **System Availability Indicator** – It communicates whether the system is online or offline for maintenance.

14.1.2. Banner Display States

Standard Legal Notice Banner

The standard banner is displayed when the system is online and available for authorized Users:

```
|---------------------------------------------------------------|
| This system is for the use of authorized users only.          |
| Individuals using this computer system without authority, or in |
| excess of their authority, are subject to having all of their  |
| activities on this system monitored and recorded by system    |
| personnel.                                                     |
|                                                               |
| In the course of monitoring individuals improperly using this |
| system, or in the course of system maintenance, the activities |
| of authorized users may also be monitored.                    |
|                                                               |
| Anyone using this system expressly consents to such monitoring |
| and is advised that if such monitoring reveals possible       |
| evidence of criminal activity, system personnel may provide the |
| evidence of such monitoring to law enforcement officials.     |
|---------------------------------------------------------------|
```

Maintenance Mode Banner

Users will be locked out during scheduled maintenance windows.

During lock out periods the following banner is displayed to inform users of system unavailability:

```
|-----------------------------------------------------------|
|                                                           |
| The system is OFFLINE FOR MAINTENANCE.                    |
| Please try again after the Maintenance Window.            |
|                                                           |
| During this time you will get the following error message |
| when attempting to log in:                                |
|                                                           |
| Permission denied (publickey,gssapi-keyex,gssapi-with-mic)' |
|                                                           |
|-----------------------------------------------------------|
```

NB:The "Permission denied (publickey,gssapi-keyex,gssapi-with-mic)" error message is an artifact of the lockout process and does not indicate that the User's SSH Key is invalid. This is expected behaviour during maintenance periods.

14.1.3. Connection Details

- The banner displays automatically when Users connect to the XXXX system via SFTP
- Banner display only occurs in non-quiet mode connections
- No banner is displayed when quiet mode is enabled for SFTP connections

14.1.4. Banner Management

- The system automatically selects the appropriate banner based on current system status

- During maintenance windows, the system displays the maintenance banner to notify Users that the system is not available

<div style="border:1px solid black; text-align:center;">

END OF DOCUMENT

</div>