Integrated Public Number Database (IPND)

IPND Carriage Service Providers Access to Internet Interface Service (IIS)

Date: June 2024

Vers: 1.0

Approved by: Penny Waite

Title: IPND Manager

Author(s):	LogicalTech Pty Ltd
Application:	Integrated Public Number Database

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

Document Control

Version	Release Date	Written By	Reviewed By	Notes
1.0	June 2024	LogicalTech		Document created for Carriage Service Provider (CSP) access to IIS

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

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 downloaded from the IPND the following measures will be deployed as part of the IIS:

- VPN Secure Sockets Layer (SSL) tunnels
- 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 Carriage Service Provider (CSP) 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.

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 updated client utilities is the responsibility of Carriage Service Providers.

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

1.1.1. User Toolsets

There are two essential toolsets:

(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 (1-2)	*a) Linux/Windows Subsystem for Linux (WSL)*	*b) Windows: PowerShell or CommandPrompt (CMD)*	*c) Windows Desktop*
(1) VPN Client	openvpn	Not available (Must use GUI client)	OpenVPN Connect, OpenVPN GUI
(2) GPG (GNU Privacy Guard)	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) gpg, (2) VPN client

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

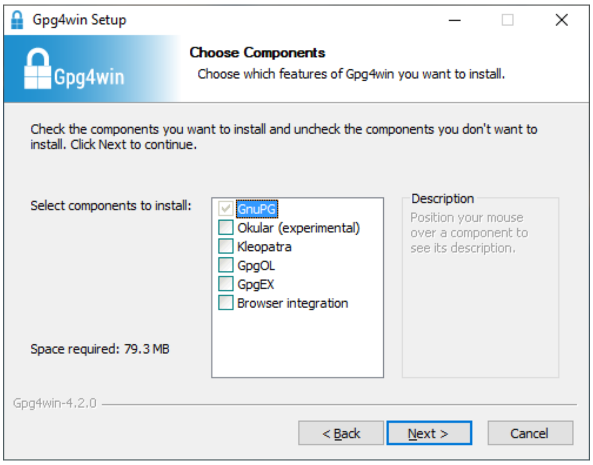
For Red Hat based systems:

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

sudo yum install gnupg2 openvpn -y
```

CLI: PowerShell, CommandPrompt:

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

Choose Components

Choose which features of Gpg4win you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

- ☑ GnuPG
- □ Okular (experimental)
- □ Kleopatra
- □ GpgOL
- □ GpgEX
- □ Browser integration

Description

Position your mouse over a component to see its description.

Space required: 79.3 MB

Gpg4win-4.2.0

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)

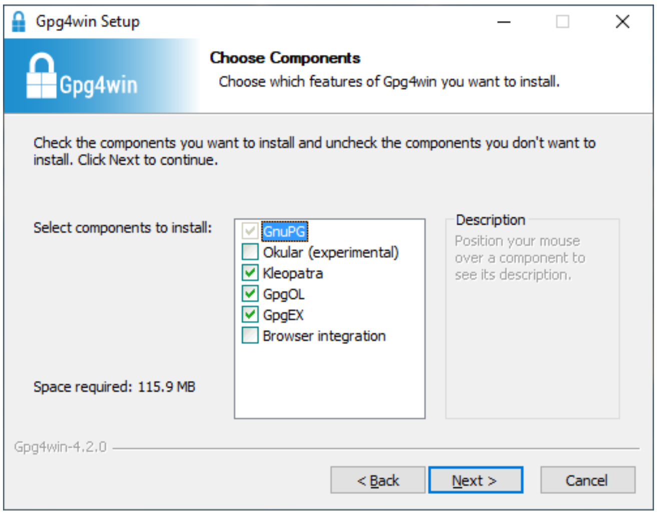
   or

   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.

2. 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 Setup

Choose Components

Choose which features of Gpg4win you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

- ☑ GnuPG
- □ Okular (experimental)
- ☑ Kleopatra
- ☑ GpgOL
- ☑ GpgEX
- □ Browser integration

Description

Position your mouse over a component to see its description.

Space required: 115.9 MB

Gpg4win-4.2.0

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 GUI Credentials (Username and Password)	Access to OpenVPN gateway	2.3 Downloading VPN Client and Configuration
Comment details (optional)	Input into GPG-key pair	4.3 Creating user 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:
ipnd-support@logicaltech.com.au

Element	Purpose	Section(s) referred
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

2.1. Overview

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

This section provides users the steps required to:

- Download their User VPN configuration file,
- Establish a VPN tunnel
- Check that the VPN tunnel has been established successfully.

Note: The VPN configuration file includes the Fully Qualified Domain Name (FQDN) 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 URL 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.

2.2. VPN Settings

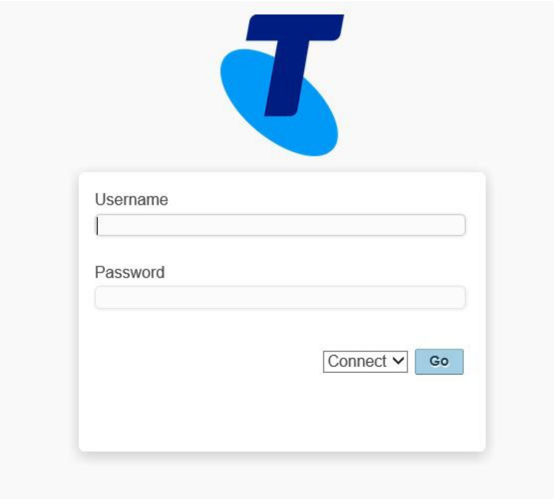
VPN Settings are included in the VPN Configuration file available for download as explained in the following section. More information is included in **APPENDIX 2 – OPENVPN CONFIGURATION FILE EXAMPLE**.

VPN Gateway URI	gw1.ipnd.com.au
VPN Connection Port UDP	1194
VPN Connection Port TCP	443
VPN Provisioning URL	https://gw1.ipnd.com.au

2.3. Downloading VPN Client and Configuration

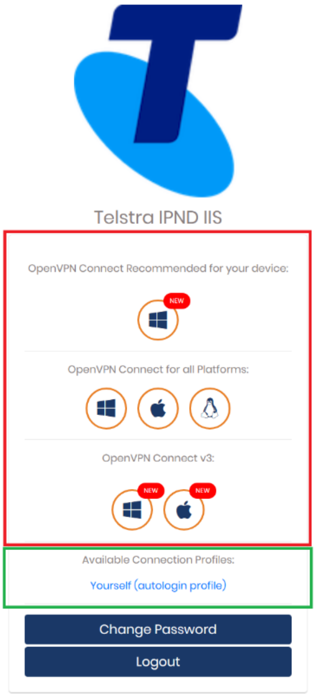
The IPND Support team will issue OpenVPN credentials to Users.

Upon receiving credentials, Users are required to log in and download the IIS OpenVPN Client and configuration files via the VPN Provisioning URL: https://gw1.ipnd.com.au



Screen 1 - VPN Login Page

Upon successful login, users will be directed to the following screen:


Telstra IPND IIS
OpenVPN Connect Recommended for your device:
NEW
OpenVPN Connect for all Platforms:
OpenVPN Connect v3:
NEW
NEW
Available Connection Profiles:
Yourself (autologin profile)
Change Password
Logout

VPN Client Application/Profile Download Page

There are 2 basic types of links on the Download page - Application links (3 levels) and a Connection Profile link.

1. Application Links: 🟥

   The 1st Application link is recommended based on the users operating system and browser.
   The 2nd Application level links is for OpenVPN Connect v2 for all supported platforms.
   The 3rd Application level is for OpenVPN Connect v3.

   The Windows and Apple links will allow users to download signed msi (Windows) and dmg (Apple) files to install.
   The Android and IOS links will navigate users to the appropriate app stores.
   The Linux link will navigate users to additional instructions on how to deploy a Linux distribution OpenVPN client app.

2. Available Connection Profiles link: 🟩

   The "Available Connection Profiles" link enables users to download their specific client.ovpn configuration file for import into their OpenVPN client.

   The 'autologin profile' enables users to establish a connection without the need for direct authentication with a password via their OpenVPN client. It is essential to keep this file secure and refrain from sharing it with unauthorized individuals. Please ensure the security of this file and use it exclusively on a secure server.

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 Provisioning URI (gw1.ipnd.com.au) is working.

Do NOT edit your VPN config file 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

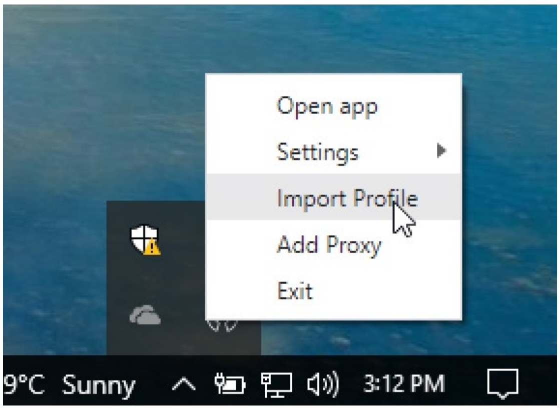
Linux/WSL Initial VPN Tunnel Test

```
## 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
```

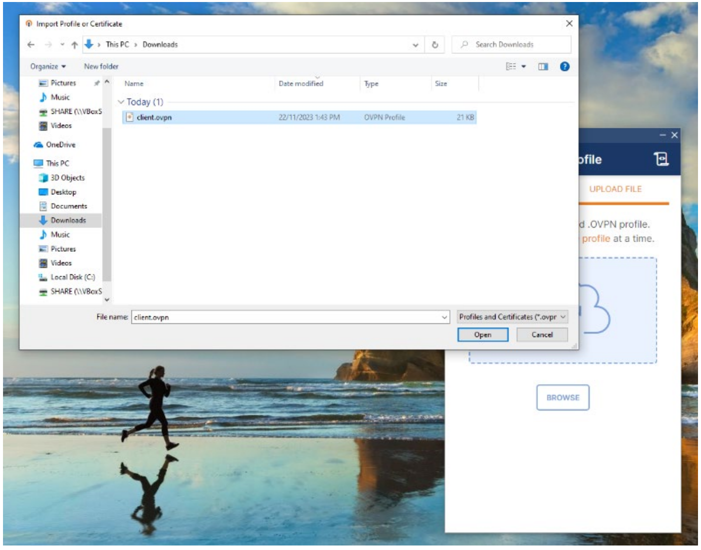
2.4.4.2. GUI: OpenVPN GUI/Connect

Upon completion of installation of the OpenVPN client, users should have a desktop icon and an app icon in their notification area.

1. To import the client.ovpn profile file, the user must right click on the OpenVPN Connect icon and select: Import Profile



Users will be prompted to BROWSE and select their client.ovpn profile file by clicking Open:

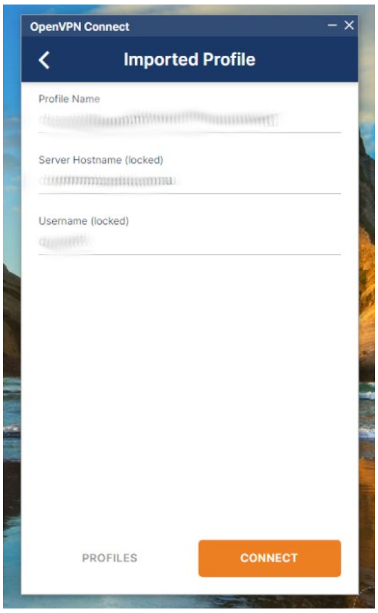


Name	Date modified	Type	Size
client.ovpn	22/11/2023 1:43 PM	OVPN Profile	21 KB

File name: client.ovpn

Profiles and Certificates (*.ovpr

Once the profile file is imported, the user must click on either ‘PROFILES’ (to save and return to main app page) or ‘CONNECT’ to save the file. Clicking the back arrow causes the profile to be un-saved.



OpenVPN Connect

Imported Profile

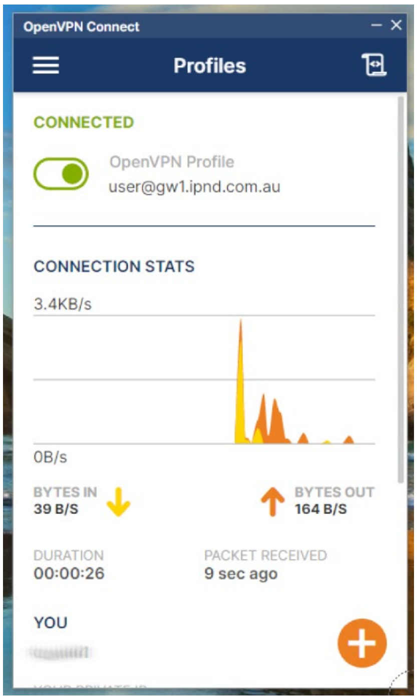
Profile Name

Server Hostname (locked)

Username (locked)

2. To connect

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



OpenVPN Connect

Profiles

CONNECTED

OpenVPN Profile
user@gw1.ipnd.com.au

CONNECTION STATS

BYTES IN 39 B/S

BYTES OUT 164 B/S

DURATION 00:00:26

PACKET RECEIVED 9 sec ago

YOU

OpenVPN Client – Connected

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 TLS VPN software. It shows that the local IP address assigned to the interface is 10.10.120.6.

To ensure that data intended for the IIS is routed accordingly 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

..
```

3. GPG KEY PAIRS

3.1. Overview

All files that are provided from the IPND via the IIS Web Portal will be encrypted using GnuPG.

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

3.2. 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.

3.3. 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.

3.3.1. 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
```

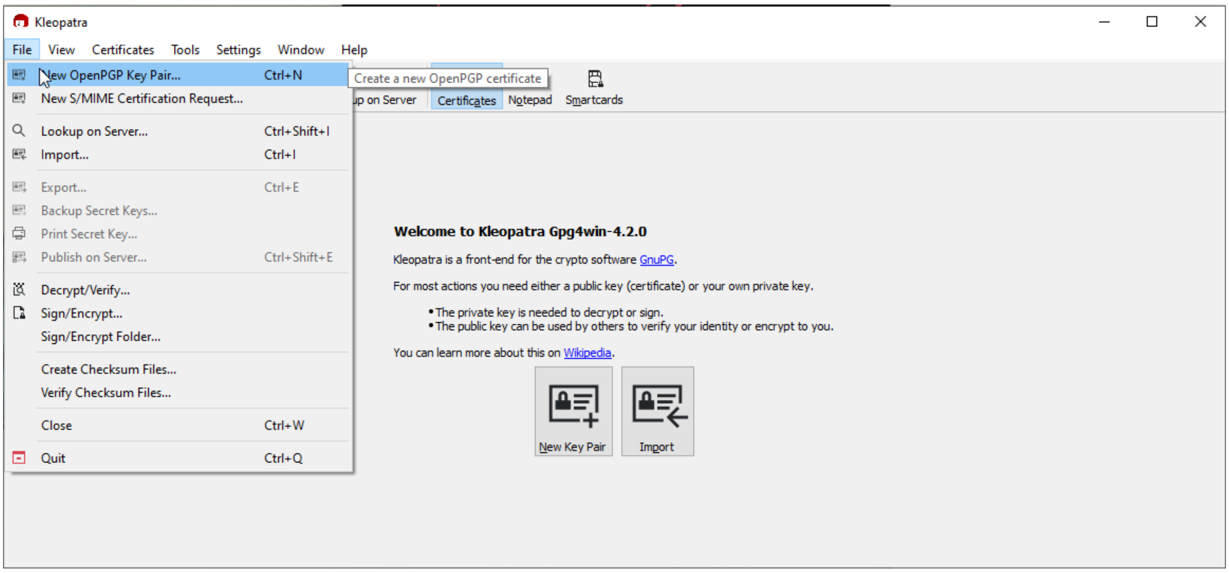
3.3.2. GUI: Windows Kleopatra

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

File View Certificates Tools Settings Window Help

New OpenPGP Key Pair... Ctrl+N
New S/MIME Certification Request...
Lookup on Server... Ctrl+Shift+I
Import... Ctrl+I
Export... Ctrl+E
Backup Secret Keys...
Print Secret Key...
Publish on Server... Ctrl+Shift+E
Decrypt/Verify...
Sign/Encrypt...
Sign/Encrypt Folder...
Create Checksum Files...
Verify Checksum Files...
Close Ctrl+W
Quit Ctrl+Q

Create a new OpenPGP certificate

up on Server Certificates Notepad Smartcards

Welcome to Kleopatra Gpg4win-4.2.0

Kleopatra is a front-end for the crypto software GnuPG.

For most actions you need either a public key (certificate) or your own private key.

- The private key is needed to decrypt or sign.
- The public key can be used by others to verify your identity or encrypt to you.

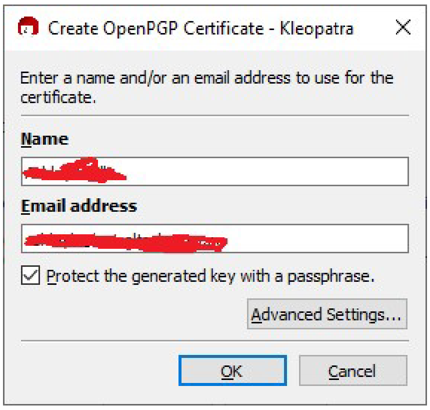
You can learn more about this on Wikipedia.

New Key Pair Import

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.


Create OpenPGP Certificate - Kleopatra

Enter a name and/or an email address to use for the certificate.

Name

[redacted]

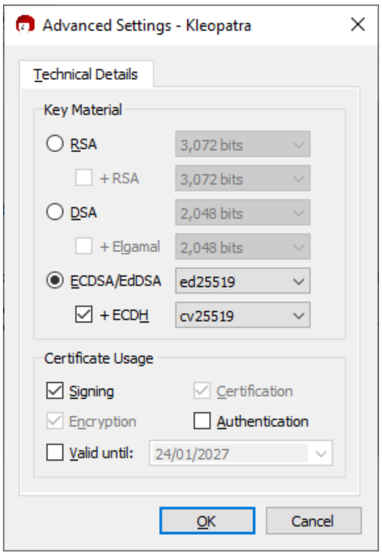
Email address

[redacted]

☑ Protect the generated key with a passphrase.

Advanced Settings...

OK Cancel


Advanced Settings - Kleopatra

Technical Details

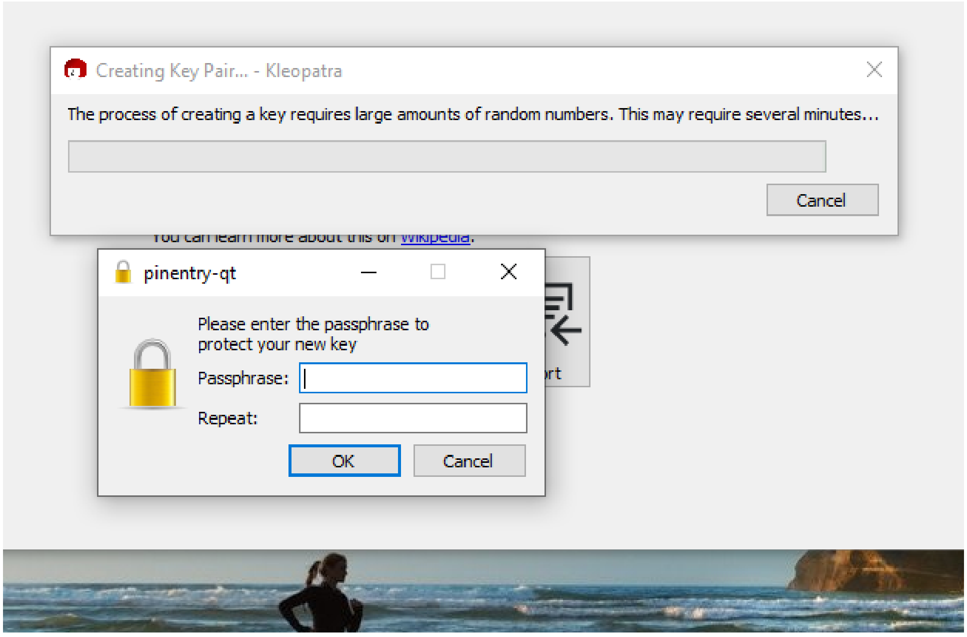
Key Material

○ RSA 3,072 bits
□ + RSA 3,072 bits
○ DSA 2,048 bits
□ + Elgamal 2,048 bits
● ECDSA/EdDSA ed25519
☑ + ECDH cv25519

Certificate Usage

☑ Signing ☑ Certification
☑ Encryption □ Authentication
□ Valid until: 24/01/2027

OK Cancel



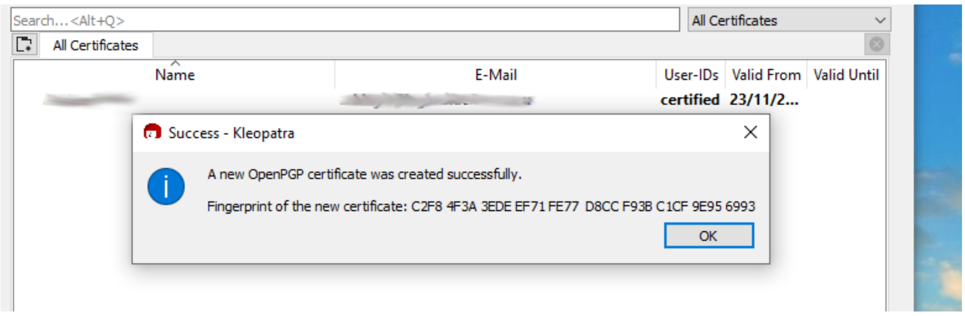
Creating Key Pair... - Kleopatra
Cancel
You can learn more about this on Wikipedia.
pinentry-qt
OK
Cancel

The process of creating a key requires large amounts of random numbers. This may require several minutes...

Please enter the passphrase to protect your new key

Passphrase:

Repeat:



Name	E-Mail	User-IDs	Valid From	Valid Until
[redacted]	[redacted]	certified	23/11/2...	

Success - Kleopatra

A new OpenPGP certificate was created successfully.

Fingerprint of the new certificate: C2F8 4F3A 3EDE EF71 FE77 D8CC F93B C1CF 9E95 6993

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. Connecting

4.1. Overview

This section describes how to connect to the IPND - IIS Web Portal. The basic steps are:

Downloading files from the Web Portal to the users' server

- Establish a VPN tunnel
- Log into the Web Portal
- Transfer the file to the users' home directory using the Web Portal and 'Download' the required file and log out of the Web Portal
- Terminate the VPN tunnel
- Decrypt the file with using the Private GPG key

4.2. Establish a VPN tunnel

Once the user has successfully established a VPN connection as described in Section 2.VPN the user can then log into the Web Portal. The tunnel needs to be maintained for the duration of the Web Portal session.

4.3. Environments

The IIS provides Web Portal access to the core IPND Production and User Test environments.

Refer to Appendix 1 for details of IP addresses etc.

4.4. Connection Management Guidelines

To facilitate file transfer between the users' server and the IPND Web Portal, the user must establish an authorized VPN connection.

4.4.1. 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 VPN sessions after completing file transfers to release resources and enhance security.

4.4.2. Security Considerations

Retaining open VPN 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. File Decryption

5.1. Overview

All files that are provided from the IPND via the IIS Web Portal will be encrypted using GnuPG. This section provides an overview on how to decrypt files.

5.2. Decrypting Files

5.2.1. CLI: Linux, WSL, PowerShell, CommandPrompt

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

## Check that you have access to your private key

```
        gpg -K

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

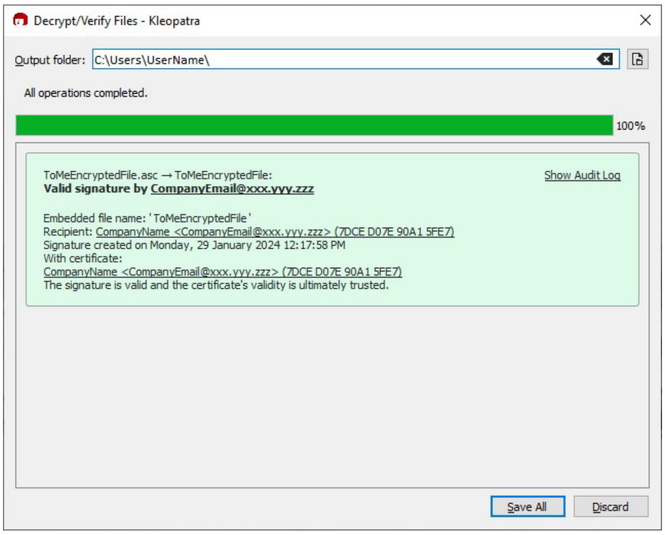
## When decrypting you must specify an output file, otherwise the output is to the screen
## NB: Your Encrypted file is unaffected.

## To Decrypt `<Encryptedfile>` as `<UnEncryptedFile>`

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

5.2.2. GUI: Windows Kleopatra

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



Output folder: C:\Users\UserName\

All operations completed.

100%

ToMeEncryptedFile.asc → ToMeEncryptedFile:
Valid signature by CompanyEmail@xxx.yyy.zzz

Embedded file name: 'ToMeEncryptedFile'
Recipient: CompanyName <CompanyEmail@xxx.yyy.zzz> (7DCE D07E 90A1 5FE7)
Signature created on Monday, 29 January 2024 12:17:58 PM
With certificate:
CompanyName <CompanyEmail@xxx.yyy.zzz> (7DCE D07E 90A1 5FE7)
The signature is valid and the certificate's validity is ultimately trusted.

Kleopatra: File Decryption screen

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

6. References

6.1. 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
TLS	Transport Layer Security
VPN	Virtual Private Network

7. APPENDIX 1 – FINGERPRINTS

7.1. GPG FINGERPRINTS

7.1.1. CLI: Linux, WSL, PowerShell, CommandPrompt

Once key has been loaded into keychain:

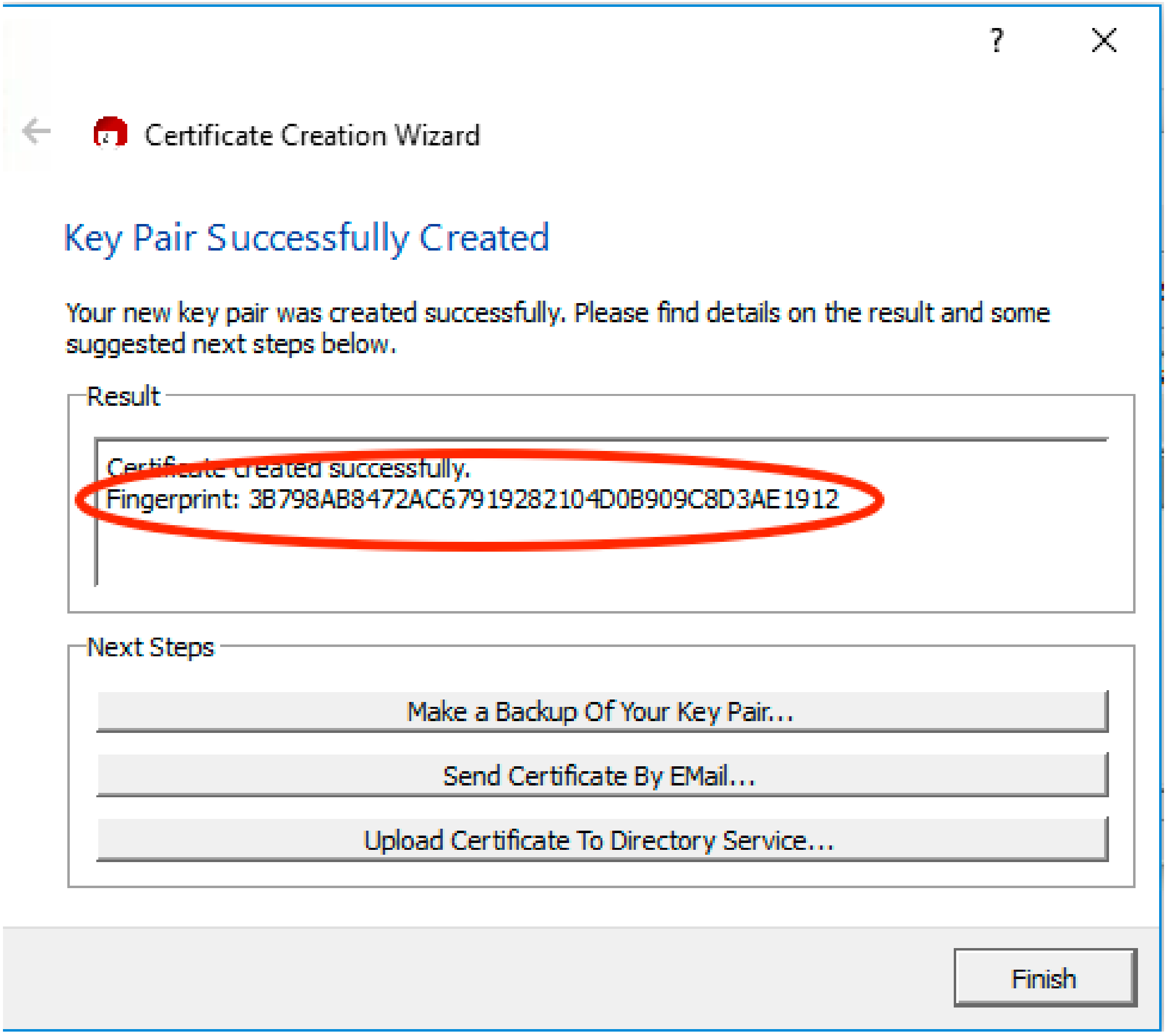
```
gpg --fingerprint <user>  ## Fingerprint shown in green
pub   rsa2048 2013-06-11 [SC]
      3777 04C9 34DD 3DAB DBED  D500 8947 60EF 77FD D883
uid           [  full  ] User Name <user@email.com>
sub   rsa2048 2013-06-11 [E]
```

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]
```

7.1.2. GUI: Windows - Kleopatra

When GPG key pair is created.


?
Certificate Creation Wizard

Key Pair Successfully Created

Your new key pair was created successfully. Please find details on the result and some suggested next steps below.

Result

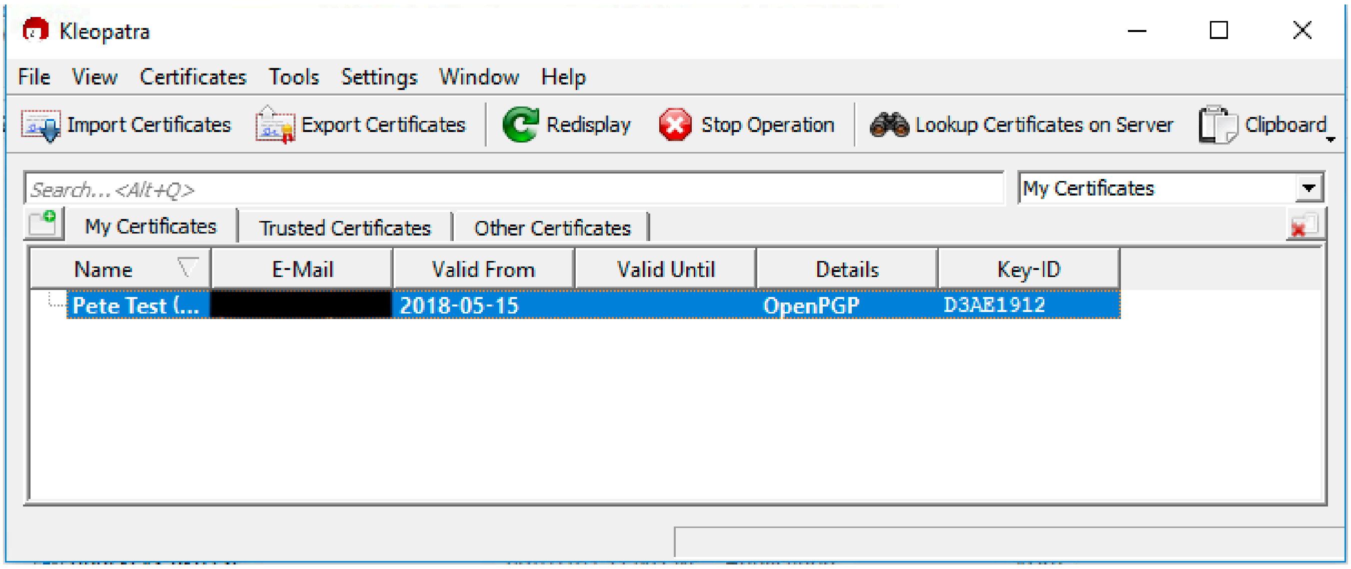
Certificate created successfully.
Fingerprint: 3B798AB8472AC67919282104D0B909C8D3AE1912

Next Steps
Make a Backup Of Your Key Pair...
Send Certificate By EMail...
Upload Certificate To Directory Service...
Finish

GPG Fingerprint - Kleopatra

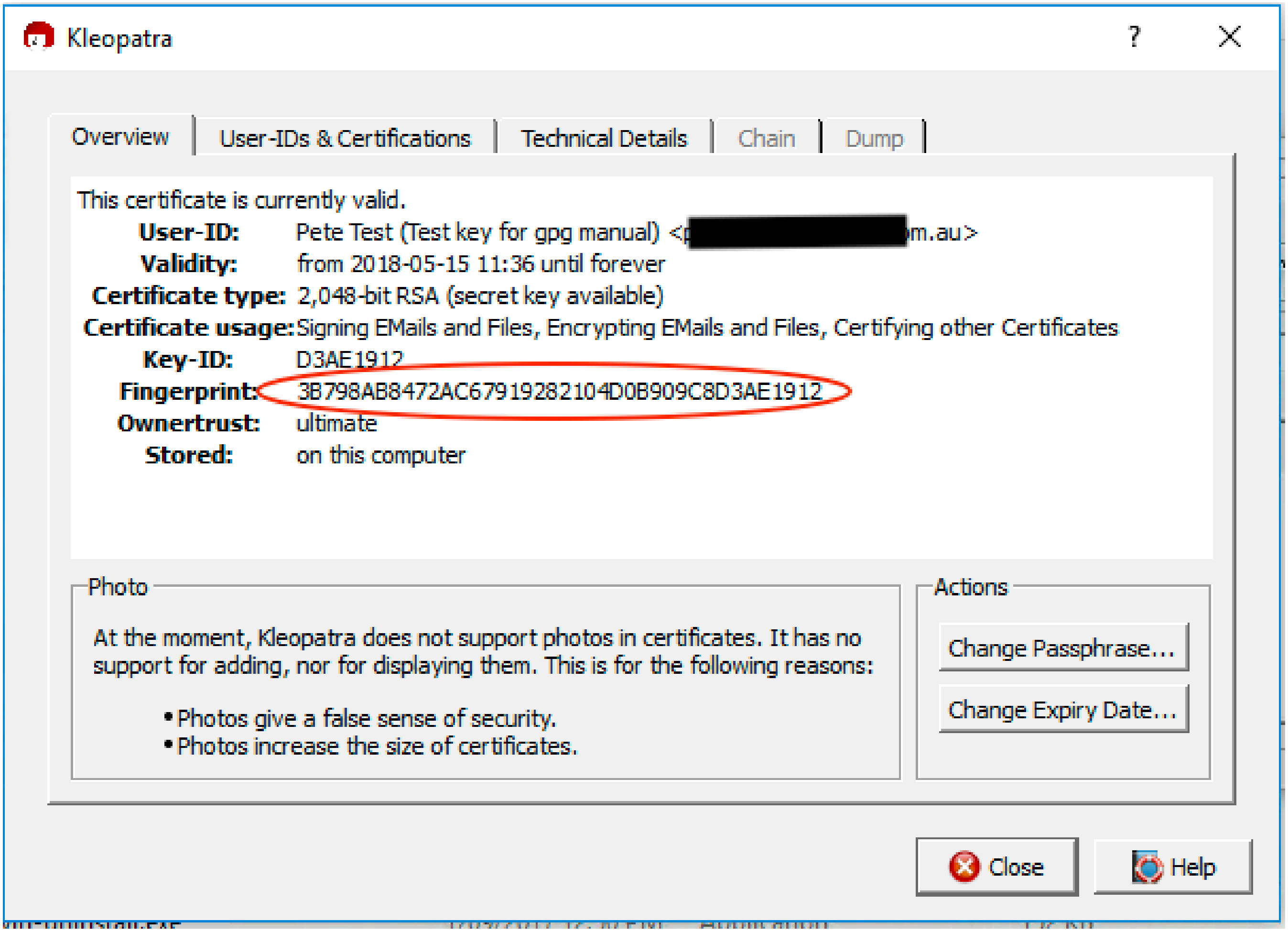
After key pair has been generated:

Double click on the key pair.



Name	E-Mail	Valid From	Valid Until	Details	Key-ID
Pete Test (...	[redacted]	2018-05-15		OpenPGP	D3AE1912

GPG Fingerprint - Kleopatra - post create



This certificate is currently valid.

User-ID:	Pete Test (Test key for gpg manual) <[redacted]m.au>
Validity:	from 2018-05-15 11:36 until forever
Certificate type:	2,048-bit RSA (secret key available)
Certificate usage:	Signing EMails and Files, Encrypting EMails and Files, Certifying other Certificates
Key-ID:	D3AE1912
Fingerprint:	3B798AB8472AC67919282104D0B909C8D3AE1912
Ownertrust:	ultimate
Stored:	on this computer

Photo

At the moment, Kleopatra does not support photos in certificates. It has no support for adding, nor for displaying them. This is for the following reasons:

- Photos give a false sense of security.
- Photos increase the size of certificates.

GPG Fingerprint - Kleopatra - post create 2

8. Appendix 2 – OpenVPN configuration file example

The VPN configuration file that users download (Ref: 2.3-Downloading VPN Client and Configuration) 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>
```

9. Appendix 4 – Trouble shooting VPN connection issues

9.1.1. 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.

9.1.2. 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 check DNS resolution check

9.1.3. Check Firewall settings

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

9.1.4. 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.

9.1.4.1. Check IP Path MTU Discovery is enabled

Check IP Path MTU Discovery is enabled

9.1.4.2. 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
```

9.1.4.3. 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
```

9.1.4.4. 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
```

10. 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
```

END OF DOCUMENT