STANDARD OPERATING PROCEDURE
Do not Photocopy

Document Information Classification: Unrestricted

Title:	**Secure File Transfer client setup**
Effective Date:	**14 Feb 2019**
Reference Number:	**SOP-09-14**
Version Number:	**1.5**
Owner:	**TRE Infrastructure and Security Management Process Owner,**
Review Date:	**24 Oct 2019**

Table of Contents

1. Purpose

This document provides guidance for installing, configuring and using WinSCP to securely transfer data. It also covers the use of SSH key-pairs, which provide the additional layer of secure authentication necessary for the TRE.

While this guidance is applicable to most uses of WinSCP, it is primarily aimed at the transfer of data into the TRE. This could either be the method used by the Data Controller to transfer their datasets directly onto the corresponding TRE project's storage server. Or it could be the method of data upload/download performed by users of an application server hosted within the TRE.

The TRE, and all systems contained within, is involved in handling information that must be managed in a way that ensures its confidentiality, availability and integrity. Implementing security controls throughout the lifecycle of a system can help the TRE achieve its ISMS objectives, regulatory requirements and the needs of its users.

2. Scope

Any person making a connection to, or from a machine (server or workstation) hosted within the TRE.

WinSCP can only be installed on a Windows (Microsoft) machine, but can be used to connect to a machine running any operating system.

3. Responsibilities

The TRE Operations Manager is responsible for:

- Agreeing with software applications will be prescribed for the purpose of transferring TRE data
- Coordinating the testing of software applications in the computing environment corresponding with TRE users' working environments

The TRE System Administrator is responsible for:

- Ensuring the deployed virtual machines support connections from WinSCP and are compatible with SSH key pairs generated using Putty Key Generator
- Monitoring and logging connections so that support can be provided when necessary

4. Procedure

4.1. Installing WinSCP

This procedure covers the scenario of a 3rd Party (e.g. Data Controller) transferring data onto a Linux server within the TRE. It assumes that a Linux user account has already been created for the person conducting the data transfer. In the example below, the user

Download the latest version of the WinSCP installer (WinSCP-x.x.x-Setup.exe) from:

https://winscp.net/eng/download.php

Complete the installation of WinSCP.

4.2. Generating SSH Key-Pairs

Each SSH connection to a machine running in the TRE must utilise an RSA SSH Private/Public key-pair. X2Go should include the puttygen.exe tool, which resides within the X2Go installation directly, often located at: C:\Program Files (x86)\x2goclient

Alternatively, download the latest version of Putty Key Generator (puttygen.exe) from

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

Putty Key Generator can't be installed. The application is launched by double-clicking on puttygen.exe, so the best method is to store this file in a permanent location (e.g. C:\Program Files) and create a shortcut to the desktop or taskbar.

Note: Putty Key Generator may already exist on a PC that has previously installed the full Putty package (putty-0.xx-installer.msi).

Open Putty Key Generator. Make sure the key type is set to 'RSA' and 2048bits. Then click on 'Generate' and follow the onscreen instructions for generating 'randomness' as per *Figure 1*:

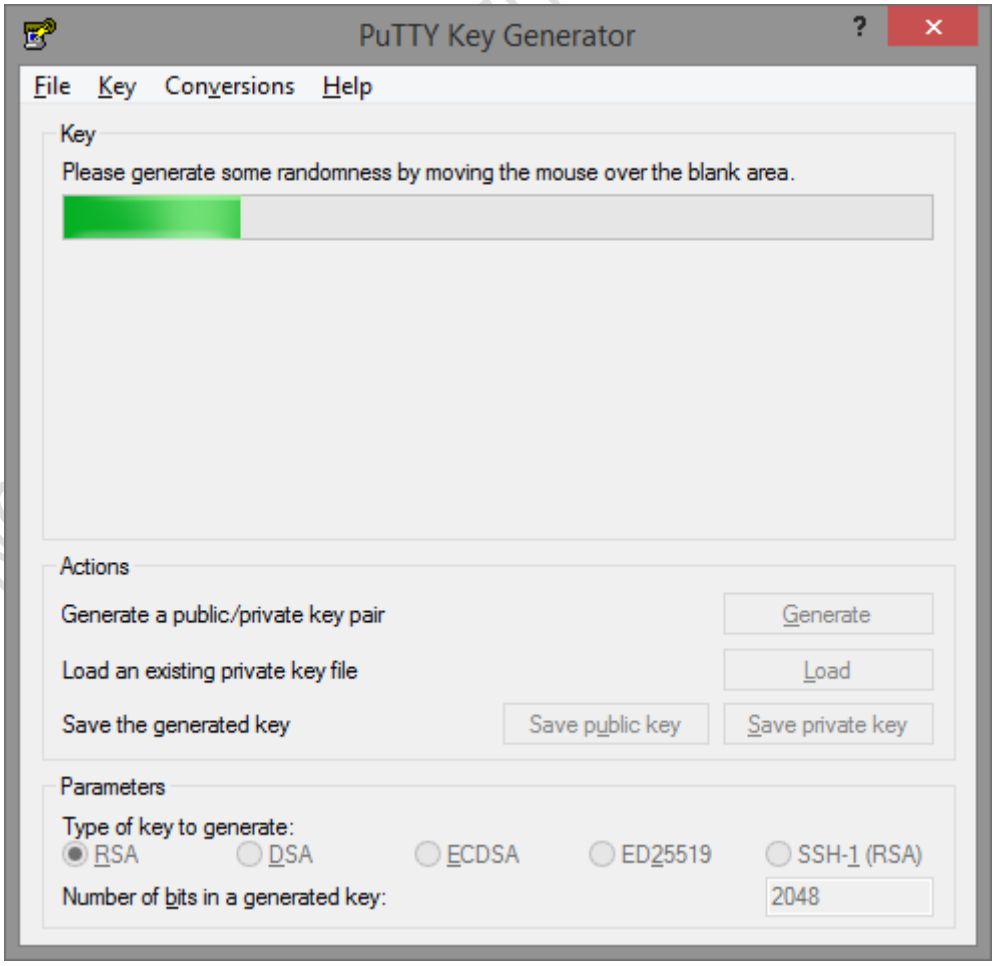

Figure 1

Once completed, it is then necessary to save both a private and public key by clicking on the buttons in turn. First, type a strong passphrase (if necessary use document ISMS-03-07 for guidance on creating passwords) into the 'Key passphrase' fields, as per *Figure 2:*

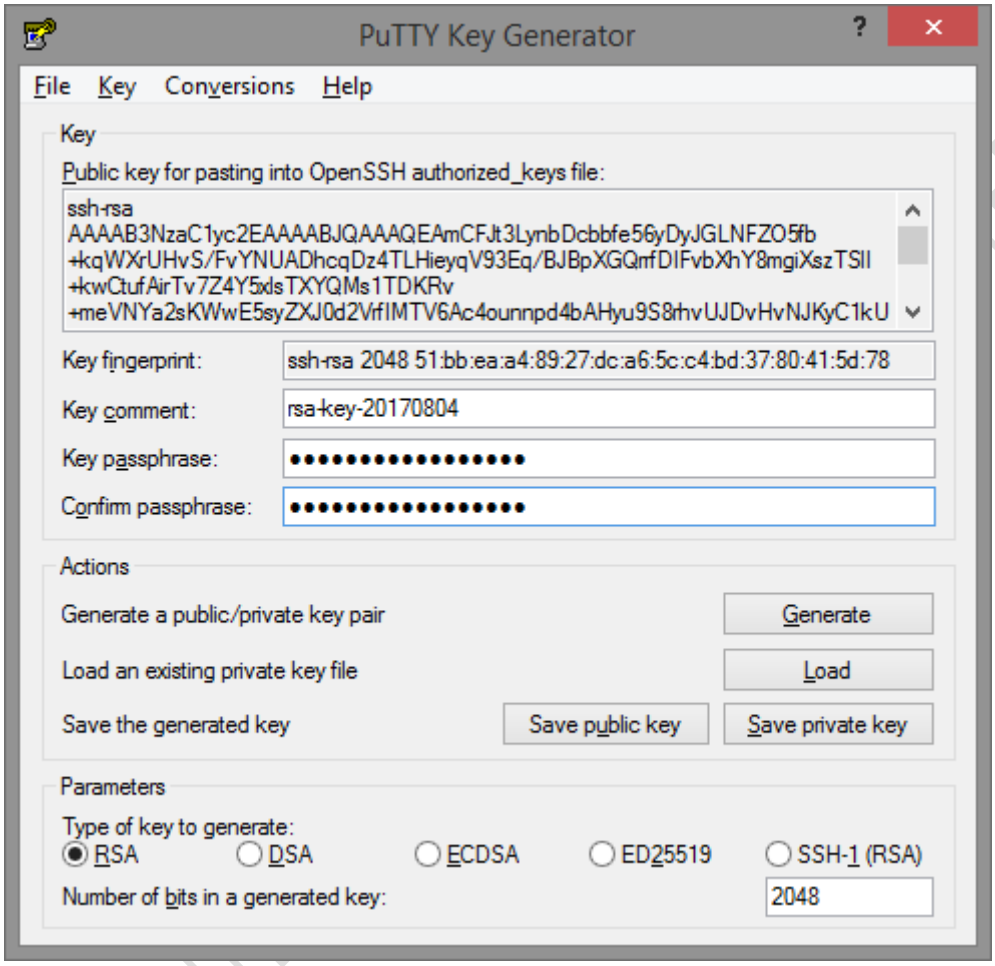

Figure 2

Click on 'Save private key'. This will open a 'Save private key as:' window. Select a secure and memorable location to save this private key on your workstation/laptop (and ideally not on a portable storage device that could get lost) and make a note of the location as it will need to be specified later. In the Filename field, type a filename using the following format: Your TRE Project ID (e.g. tre-00x) and your Linux username. If your Linux username isn't known, use the initials of your first and last name. For example, if your project name is 'TRE-050' and your name is John Smith, type in 'tre-050-js' and click 'Save'. Private SSH keys are given a .ppk extension, so for this example, the resulting private key will be named 'tre-050-js.ppk'.

Next, click on 'Save public key' and type in a similar filename as before but with the phrase 'public' at the end. Public SSH keys are created with no file extension. Following the previous example, the resulting SSH public key will have the following filename: 'tre-050-js-public' (note there is no file extension). It is OK to save the public key in the same location as the private key, but it is also OK to

store it somewhere else, and as before, make a note of the location as it will be necessary to access this public key at other times.

4.3. Configuring WinSCP

The public SSH key will need to be installed on the server that WinSCP will connect to. It is safe to send the public key by email to a system administrator of the destination server.

The procedure for installing the SSH public key on the server is described in SOP-09-01.

Open WinSCP again, select the login session created earlier, and click on 'Advanced'. From within the Advanced Site Settings window, from the left-hand-side menu, select 'SSH | Authentication'. Then specify the file path of SSH private key in the Private key file field, as shown in Figure 3:

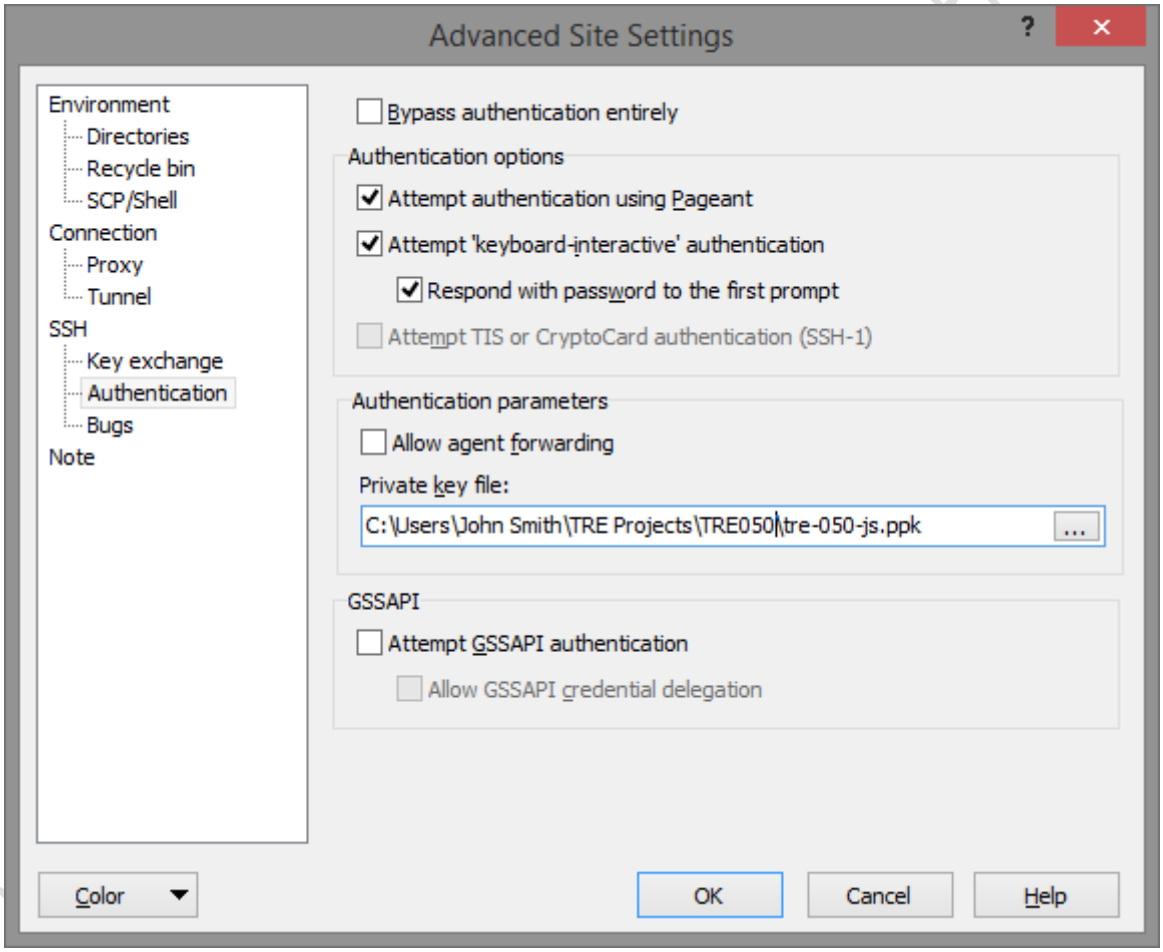

Figure 3

Click 'OK' and then 'Save' to complete the setup of the WinSCP connection.

It should now be possible to connect to the destination server by clicking on 'Login'. The next window that pops up will ask for the passphrase used to create the SSH key pair, as shown in *Figure 4:*

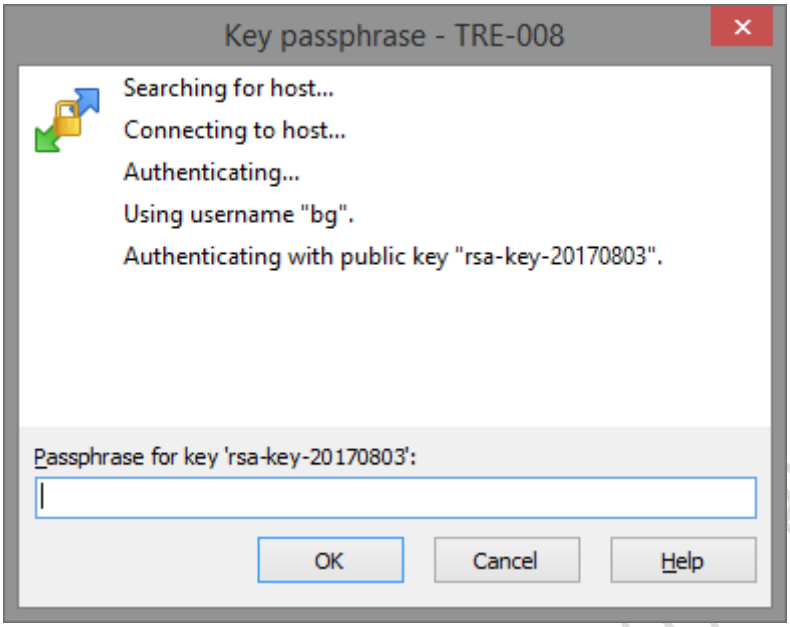

Figure 4

After successfully completing authentication, the main WinSCP window will display both the local and destination file systems, and data transfer can begin.

5. Cross-referenced ISMS Documents

Number	Type	Title
SOP-09-01	ISMS\SOP\TRE System Administration - SOP	Creating Linux User Accounts
ISMS-03-07	ISMS\Policy & Guidance\TRE Operations - policy & guidance	TRE Password Policy
SOP-03-24	ISMS\SOP\TRE Operations - SOP	Migrating Projects out of the TRE

6. Appendices

None