ISO SFTP Provisioning and Setup Procedure

Document Owner: **ISO Information Security**

REVISION HISTORY

VERSION NO. (Must match header)	DATE	REVISED BY	DESCRIPTION
0.1	10/28/2016	Thomas Williams	Initial draft
0.2	12/7/2016	Nancy Strouse	Updated draft
1.0	3/7/2017	Nancy Strouse	Draft used for PG & E training meeting on 3/7/2107
1.1	3/29/2017	Nancy Strouse	Updated owner and edits from Information Security
1.2	4/11/2017	Thomas Williams; Nancy Strouse	Updated WinSCP installation instructions; updated for CIDI provisioning process
1.3	2/28/2018	Nancy Strouse	Updated process.
1.4	12/1/2021	Michael Petroski	Removed IP Addresses from the prerequisites section.
1.5	10/4/2024	Alexander Leyva	Updated process to align with latest CAISO.com and WinSCP interface

TABLE OF CONTENTS

1. Introduction

The ISO maintains a network protocol called Secure File Transfer Protocol (SFTP) to provide secure file transfers to its users. The main use of the ISO's SFTP is to transfer MRI-S financial statements. It is also used to transfer other sensitive files to and from the ISO.

2. Purpose

The purpose of this document is to provide instructions for users who need to establish a connection with the ISO's SFTP service in order to transfer MRI-S financial statements or other files.

3. Prerequisites

Before attempting to connect to the ISO SFTP server from a secured corporate network, a user may need to work with the company's network or security administrators to configure a firewall for access. The firewall may require a rule or policy based on an IP address rather than on a name.

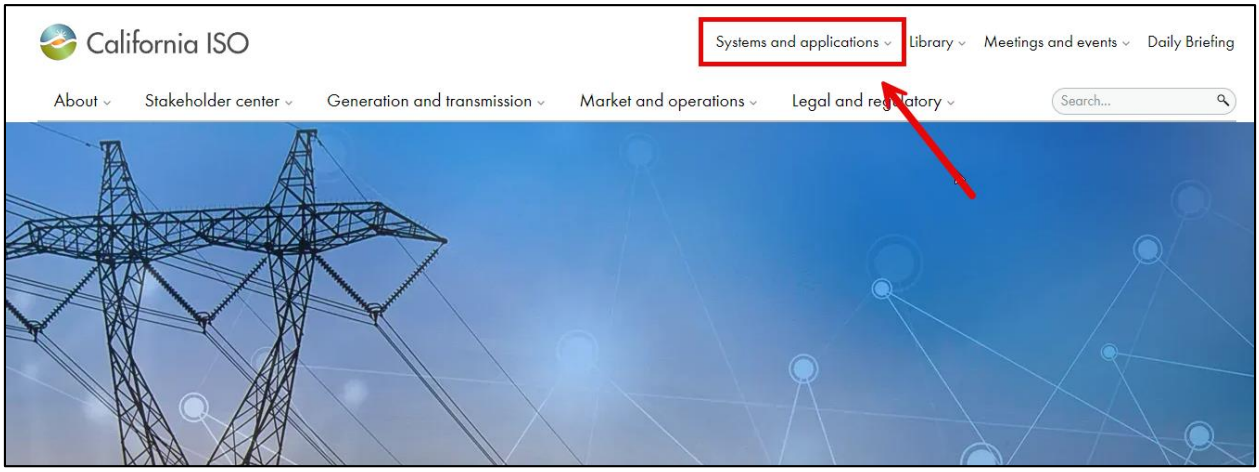
The IP information is considered sensitive and is not available in this ISO Public document. A version of this document containing the IP information can be found on CAISO's developer's website under the MRI-S application.

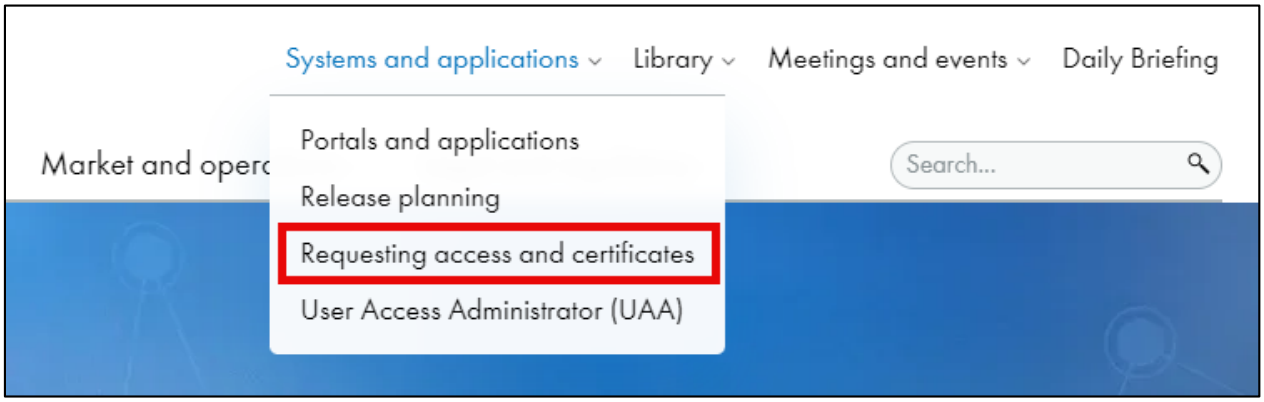
https://developer.caiso.com/

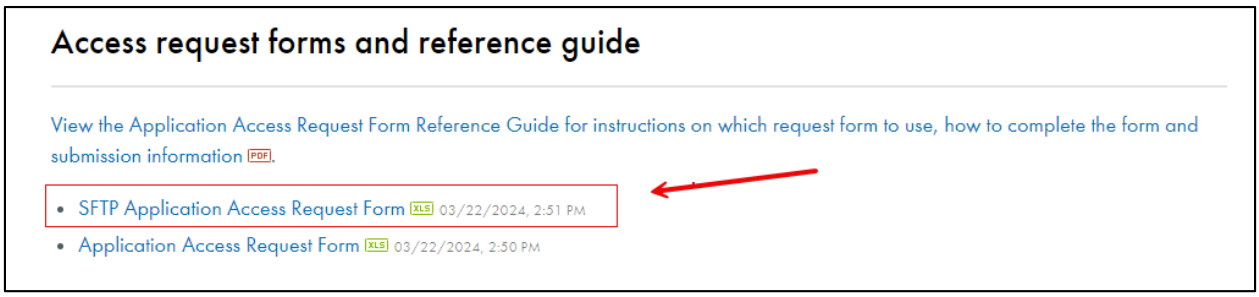
4. Requesting an SFTP Account

Users must request an SFTP account to securely transfer files with the ISO. To do so, users must:

1. Complete an SFTP Application Access Request Form (AARF), which can be accessed through the CAISO homepage.


California ISO
Systems and applications
Library
Meetings and events
Daily Briefing
About
Stakeholder center
Generation and transmission
Market and operations
Legal and regulatory
Search...


Systems and applications
Library
Meetings and events
Daily Briefing
Portals and applications
Release planning
Requesting access and certificates
User Access Administrator (UAA)
Search...


Access request forms and reference guide
View the Application Access Request Form Reference Guide for instructions on which request form to use, how to complete the form and submission information PDF.
SFTP Application Access Request Form XLS 03/22/2024, 2:51 PM
Application Access Request Form XLS 03/22/2024, 2:50 PM

2. Create a SSH **public** and **private** key pair.

3. Send the SFTP AARF and the **public** key to the ISO using the instructions in the SFTP AARF.

Note: Public keys should be saved as a plain-text file when submitting to the ISO.

5. SFTP Provisioning

5.1. SSH Authentication

Authentication to the ISO's SFTP server occurs by means of a cryptographically linked pair of keys called a secure shell (SSH) key pair. This method, more secure than standard username/password authentication, is called SSH key-based authentication. One key in the pair is **public** and the other key is **private**. The public key can be freely shared. The private key should never be shared. A security action performed by one key in the pair can be verified only by the other key in the pair. Proof of identity is one such action. In this way, the ISO can validate a user's identity assertion using the user's public key without ever needing the private key. One distinct advantage of SSH key-based authentication is that the user can automate file transfers without needing to hardcode a password in a script or program.

5.2. Client-Server Model

SSH authentication uses a client-server model. Using a pre-established network "socket" (a combination of host address and port), the server "listens" for incoming SSH connections. The client (SFTP user) initiates the connection then verifies that the server is known to it by acknowledging the **public** SSH key that the SFTP server presents. The client then presents its own credentials by performing an operation that demonstrates proof of control of the **private** key, but does **not** require presenting the **private** key itself, which would defeat the security entirely. The server validates these credentials – that is, verifies the client operation – by using the user's **public** key to perform the inverse operation. Cryptographic proof is assured by use of SSH keys with adequate bit strength.

5.3. Key Strength

The strength of a key is measured in bits. The higher the bits, the more resistant a key is to attack. With bit strength, however, there is such a thing as too strong (too many bits), which can lead to performance problems in some computing environments and which provides more security than risk warrants. Advances in computer power sometimes lead to deprecation of certain levels of bit strength that become computationally feasible to defeat in a relatively short period of time. Key bit strength is expressed in increments of powers of two and often in increments of 210 (1024). Bit strength of 1024 does not provide sufficient security against today's powerful attack agents. The ISO will not accept a 1024-bit public SSH key. Current required bit strength for ISO SSH key pairs is 2048.

5.4. Purpose of Public and Private Keys

Each key in the SSH key pair is a text thread with special meaning. The keys are mathematically linked such that one key cannot be derived from the other key and only one key can decrypt a message encrypted with the other key. The striking characteristic of the key pair is that one of the keys can be freely distributed publicly without compromising the other key that remains private.

6. SFTP Setup Procedure

6.1. Required Client Software

All required software is available at no cost and with high quality standards. There are different software tools and methods for different computer operating systems (Windows, Mac OS X, and UNIX/Linux). The ISO does not endorse any particular tool or method. The ISO does, however, have experience with what users seem to prefer and find easier to use, and the following instructions reflect that experience. In some cases, downloading tools from the internet is necessary. The ISO cannot assume responsibility for software its users choose to download in order to connect to the ISO's SFTP service. When downloading software from the internet, always follow good security practices, such as the following:

1. Use software or a service that blocks internet sites commonly acknowledged to be disreputable.

2. Use software or a service that checks each download for malware and quarantines or discards downloads infected by malware.

3. Verify the integrity of a downloaded file. The SFTP protocol has built-in integrity checks. Optionally, users might also prefer to apply a standard method of comparing a hash of the file to a hash value posted by the software a publisher has posted.[i]

6.2. User Tasks

In order to accomplish authentication using SSH keys, the user must perform these tasks:

1. Create an SSH key pair.
2. Send the SFTP AARF and the **public** key to the ISO using the instructions in the SFTP AARF.
3. Install the SFTP client software.
4. Configure an SSH authentication agent to the **private** SSH key to connect to the ISO's SFTP server.

The user therefore needs:

1. A tool to create an SSH key pair.
2. SFTP client software.

6.2.1 Download Tools to Create an SSH Key Pair

Downloading Tools with Windows
For Windows users, an excellent choice for transferring files is the free WinSCP software. WinSCP includes the PuTTY tools required for creating SSH keys.

Download the latest version of WinSCP from here:

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

WinSCP guides, including download and installation guides, as of the latest version of this documentation, are:

https://winscp.net/eng/docs/guides

Detailed WinSCP installation instructions are available here:

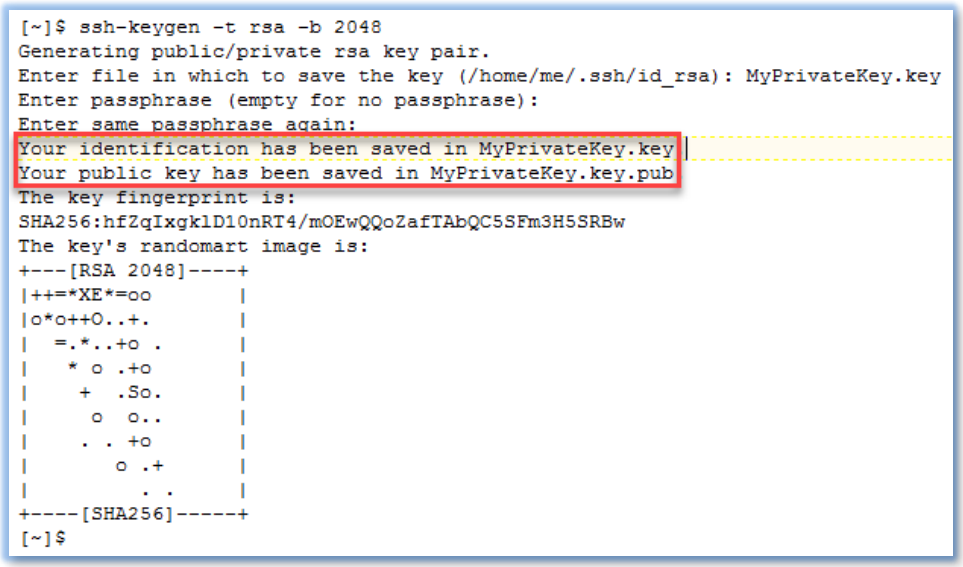
https://winscp.net/eng/docs/installation

Downloading Tools with Mac

Mac and **Linux/UNIX** users have a built-in command-line tool called **ssh-keygen** for creating an SSH key pair in one step. The basic command to create an SSH key pair of type RSA and length 2048 is:

```
ssh-keygen -t rsa -b 2048
```

Users will be prompted to name the key and optionally provide a passphrase. In this example, the process results in a public key **MyPrivateKey.key.pub** and a private key **MyPrivateKey.key**. Users should create a key pair. Keep the **private** key and send the public key to the ISO using the instructions in the SFTP AARF.



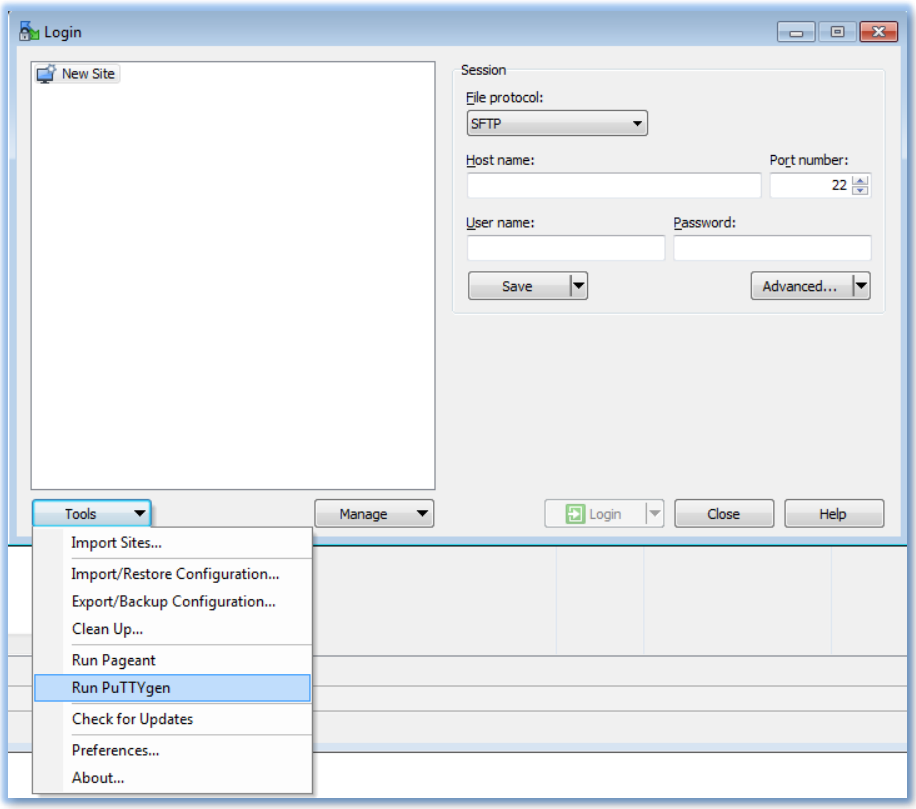
```
[~]$ ssh-keygen -t rsa -b 2048
Generating public/private rsa key pair.
Enter file in which to save the key (/home/me/.ssh/id_rsa): MyPrivateKey.key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in MyPrivateKey.key
Your public key has been saved in MyPrivateKey.key.pub
The key fingerprint is:
SHA256:hfZqIxgklD10nRT4/mOEwQQoZafTAbQC5SFm3H5SRBw
The key's randomart image is:
+---[RSA 2048]----+
|++=*XE*=oo       |
|o*o++O..+.       |
|  =.*..+o .      |
|   * o .+o       |
|    +  .So.      |
|     o  o..      |
|    . . +o       |
|       o .+      |
|         . .     |
+----[SHA256]-----+
[~]$
```

6.2.2 Create an SSH Key Pair Using the PuTTY Key Generator

To create a **public** and **private** SSH key pair using the PuTTY key generator tools, follow these steps, which assume use of PuTTY tools using the WinSCP graphical user interface:

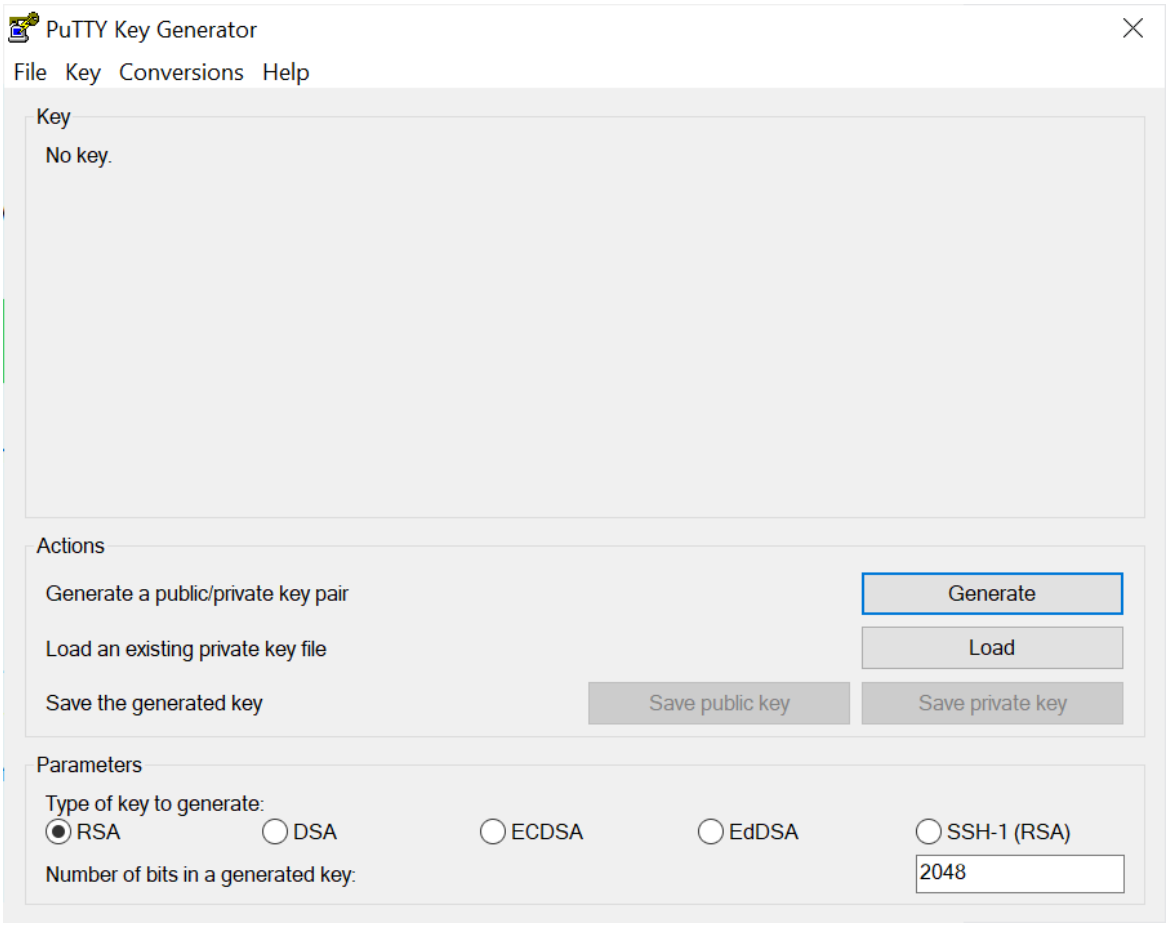
1. Start WinSCP.
2. Click **Tools** 

.
3. Select **Run PuTTYgen**.



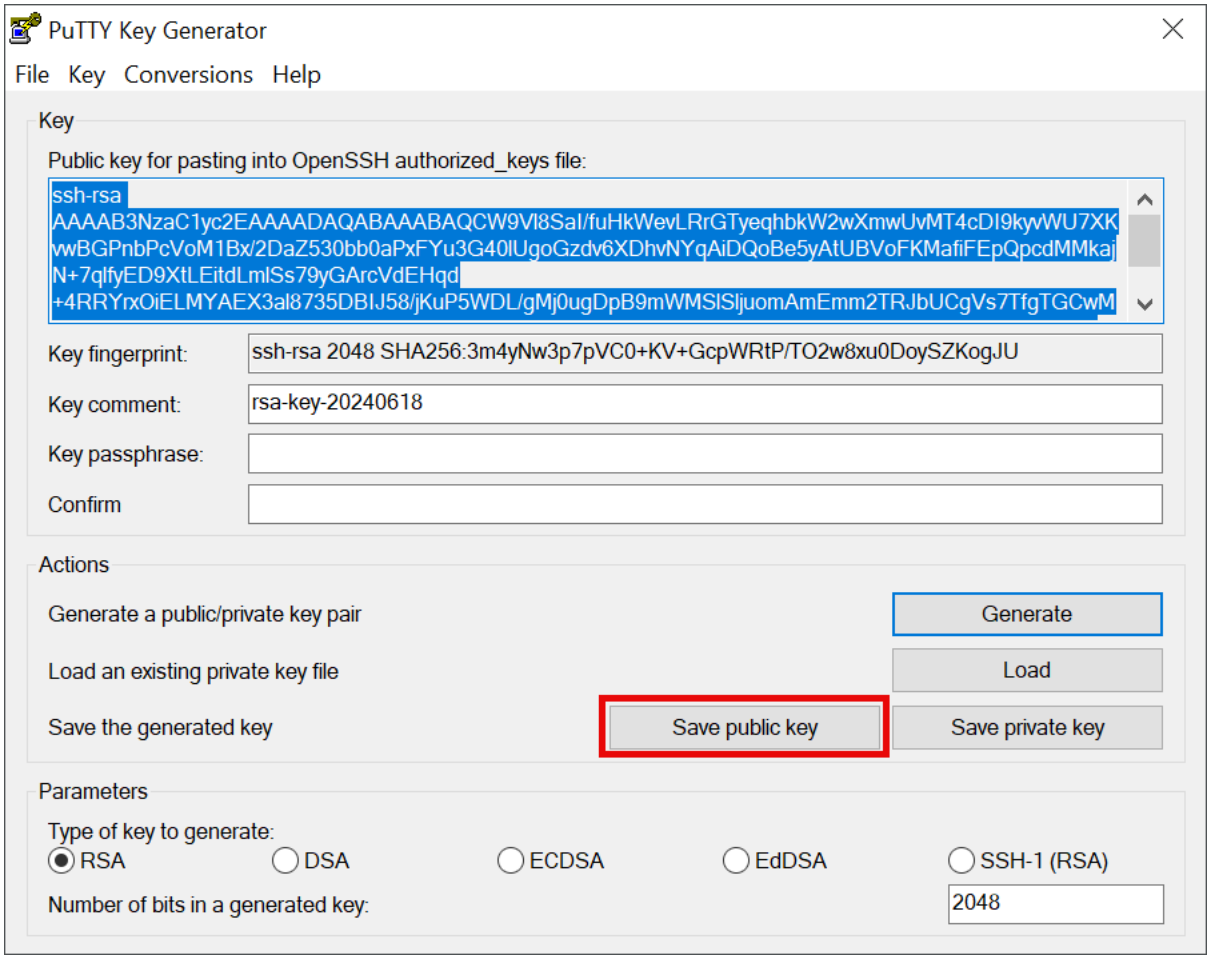
4. Select **RSA** for the key type.
5. Enter **2048** for the number of bits in the key.
6. Select **Generate** to generate a public/private key pair.

Note: Key pairs must be created using SSH-2 RSA encryption. Other formats will not be valid for SFTP authentication.



7. Click **Generate**.

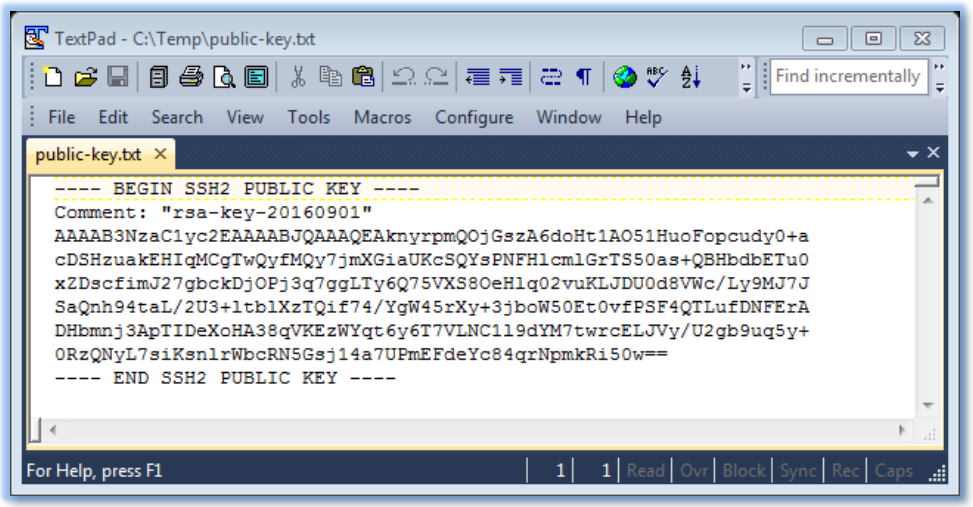
8. Randomly move the mouse pointer over the blank area in the key field. Randomness is an important cryptographic concept. Sufficient randomness, also known as entropy, assures creation of non-reproducible keys. When the PuTTY Key Generator determines that mouse input is sufficiently random, it will generate a key pair and display the result.



9. Click **Save public key**. Save the **public** key with a ".txt" extension.

10. Give the resulting **public** key text file a meaningful name. This text file will contain plain but not human-readable text.

11. Keep the **private** key and send the public key to the ISO using the instructions in the SFTP AARF.

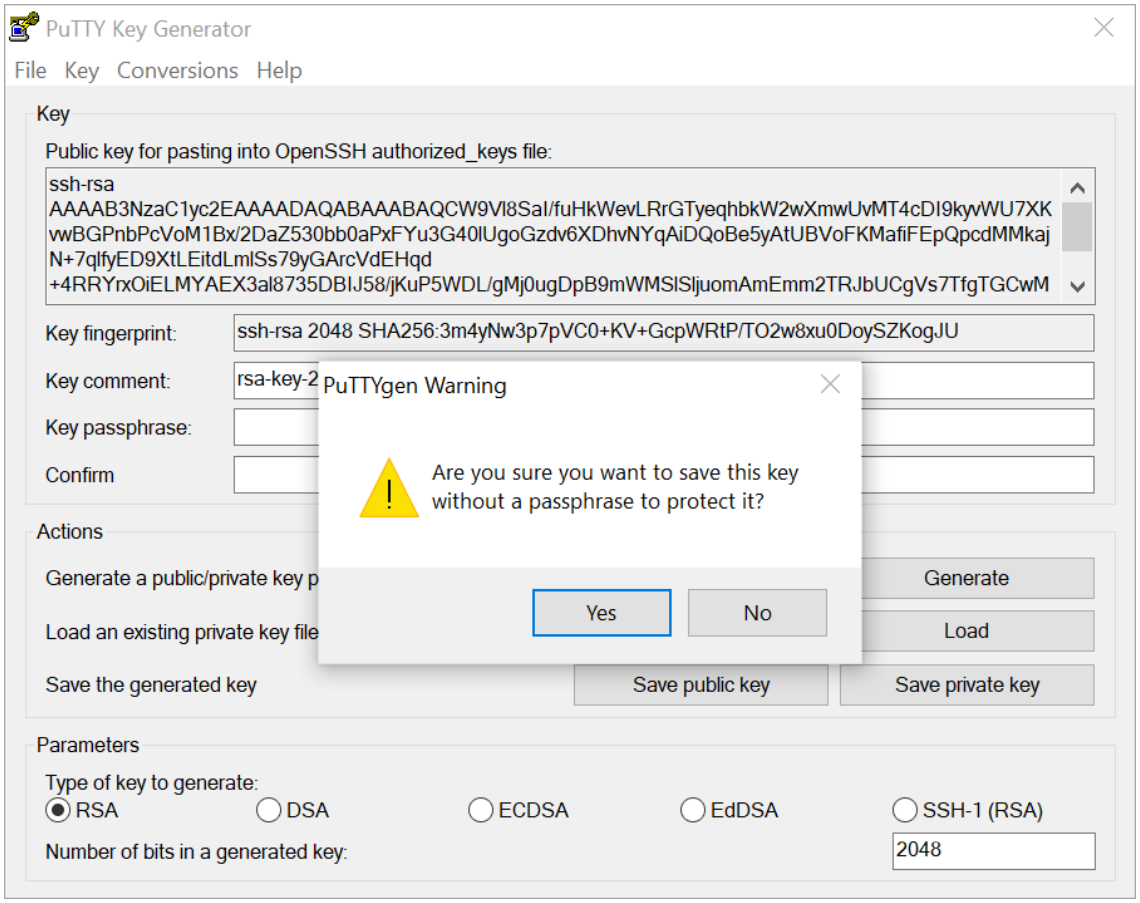


Note: Send the **public** key to the ISO via the instructions in the SFTP AARF. Do **NOT** send the **private** key.

12. Before saving the private key, type a **Key passphrase**. In general, it is important to apply a strong key passphrase in order to encrypt the private key and to protect it for private use. There are, however, some scenarios in which saving the private key without encryption (that is, without a passphrase) is legitimate. One of those scenarios is use of the private key to automate file transfers by means of an unattended script or program. In a case where the private key is not protected by a passphrase, it is very important that the computer on which the private key is installed is protected from intrusion by unauthorized users.

13. If applying a passphrase to the private key in order to encrypt it, re-type the key passphrase to **Confirm passphrase**.

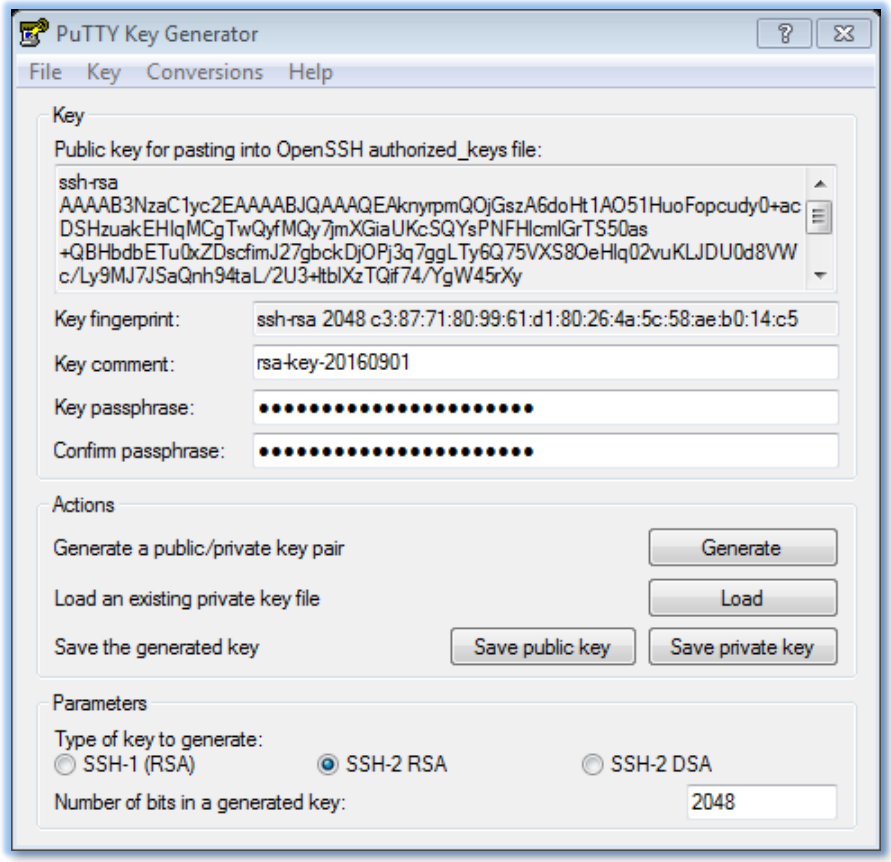
14. Click **Save private key** to save the private SSH key in the PuTTY format. If not applying a passphrase to the private key, click **Yes** at the following PuTTYgen warning.



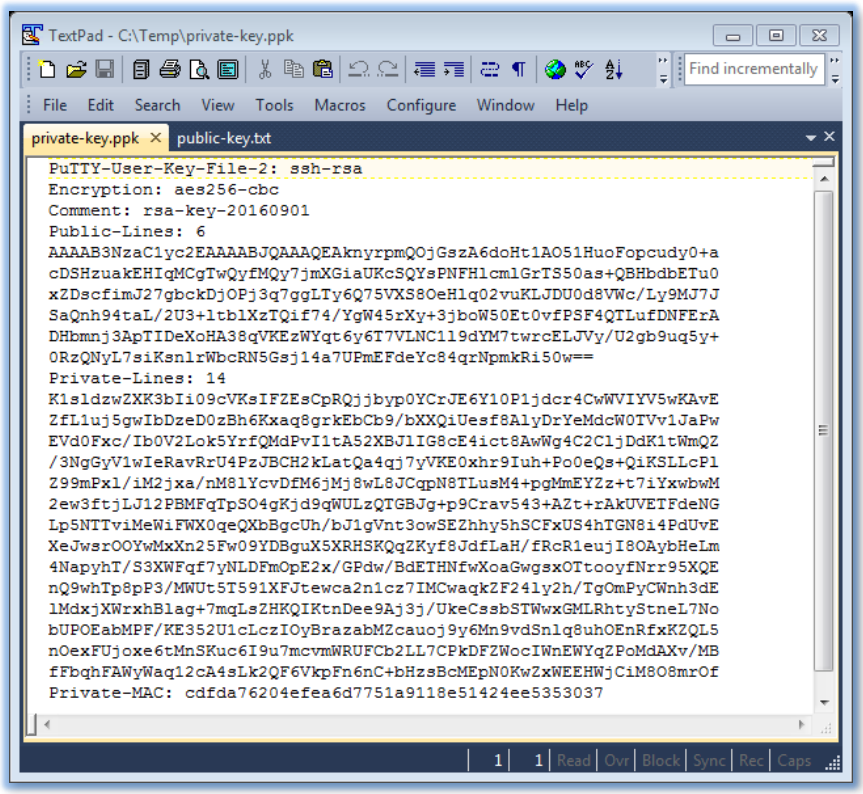
Saving the **private** key in PuTTY's format is required for the PuTTY SSH authentication agent called pageant.exe. PuTTY uses a ppk extension (PuTTY Private Key).

The PuTTY format has additional security and convenience:

- It contains the **public** key so that PuTTY can send the **public** key to the server automatically.
- The key is made tamperproof by means of a message authentication code (MAC).

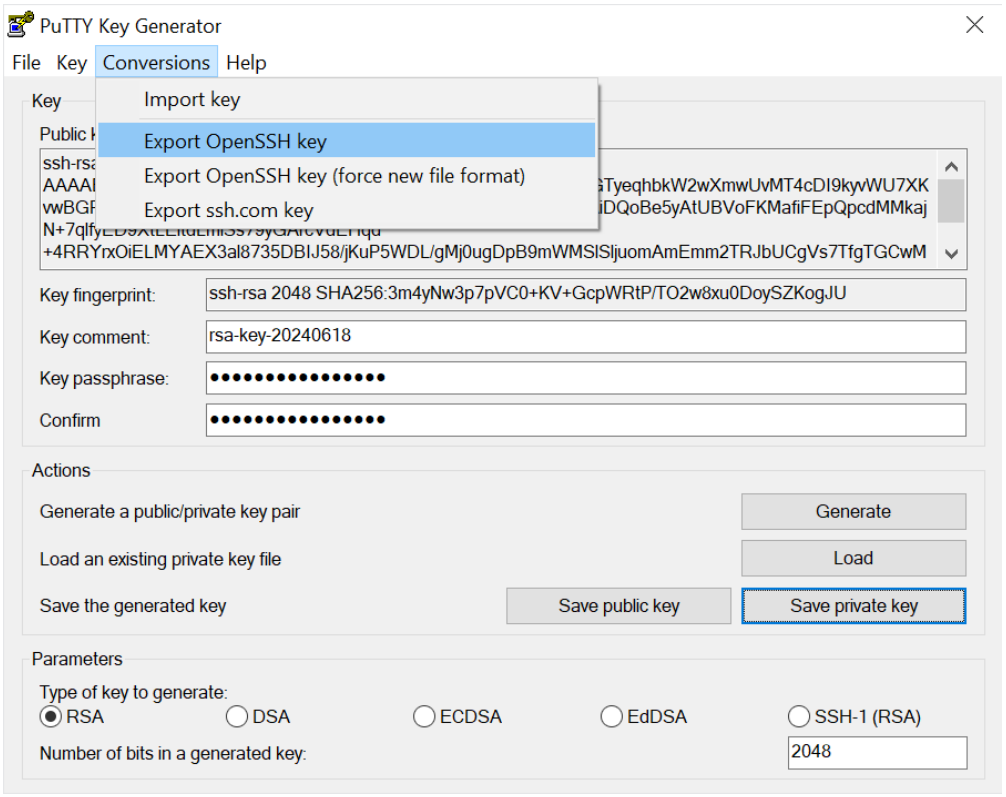


Again the expected result is plain but not-human-readable text.

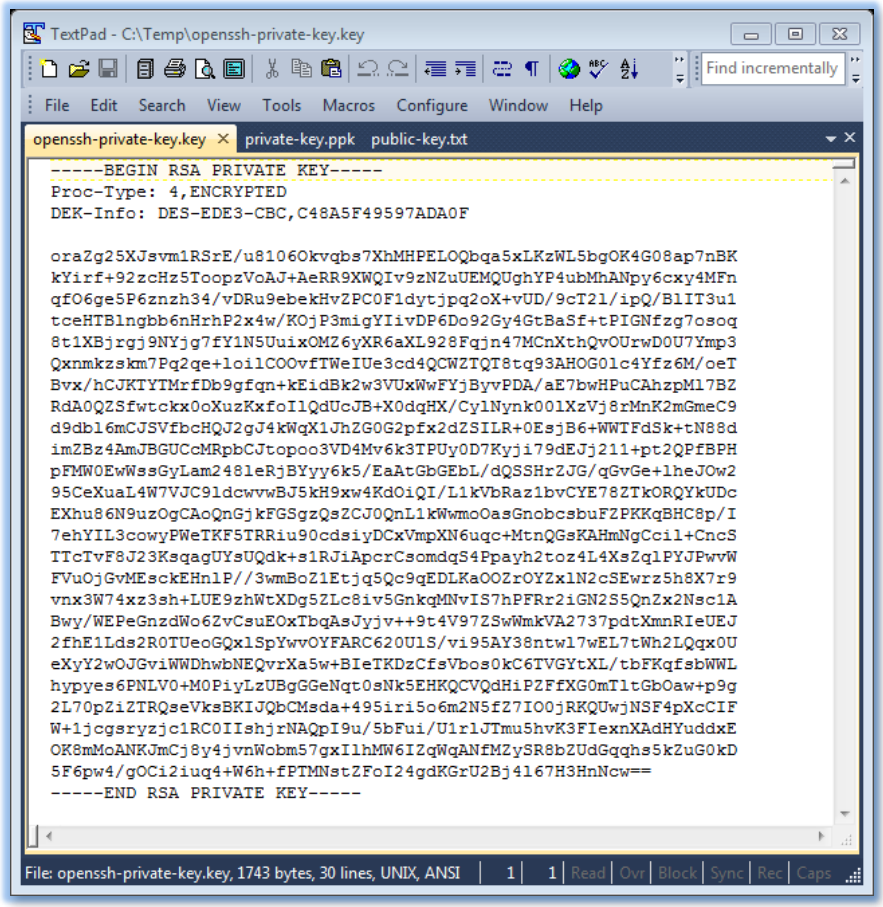


Methods other than PuTTY or WinSCP for file transfer will likely require a private key in OpenSSH format. Different users will have different needs.

If required, export the **private** key in RSA format by selecting Conversions > Export OpenSSH key.



15. Save the **private** key with a ".key" extension. As before, the expected result is plain but not human-readable text.



6.2.3 Complete the Setup Procedure

After sending the SFTP AARF and an SSH **public** key to the ISO using the instructions in the SFTP AARF, the ISO will create a Service Desk ticket for the new account.

6.2.4 What to Do about a Lost or Stolen Private Key

A private key is to be protected for authorized use. It is deemed to be compromised when lost or suspected to be stolen, creating the possibility of unauthorized use. In this case, create a new pair of SSH keys, send the new public key to the ISO Service Desk, and request that SFTP configuration be updated to use the new key.

6.2.5 How to Connect to the ISO's SFTP Server

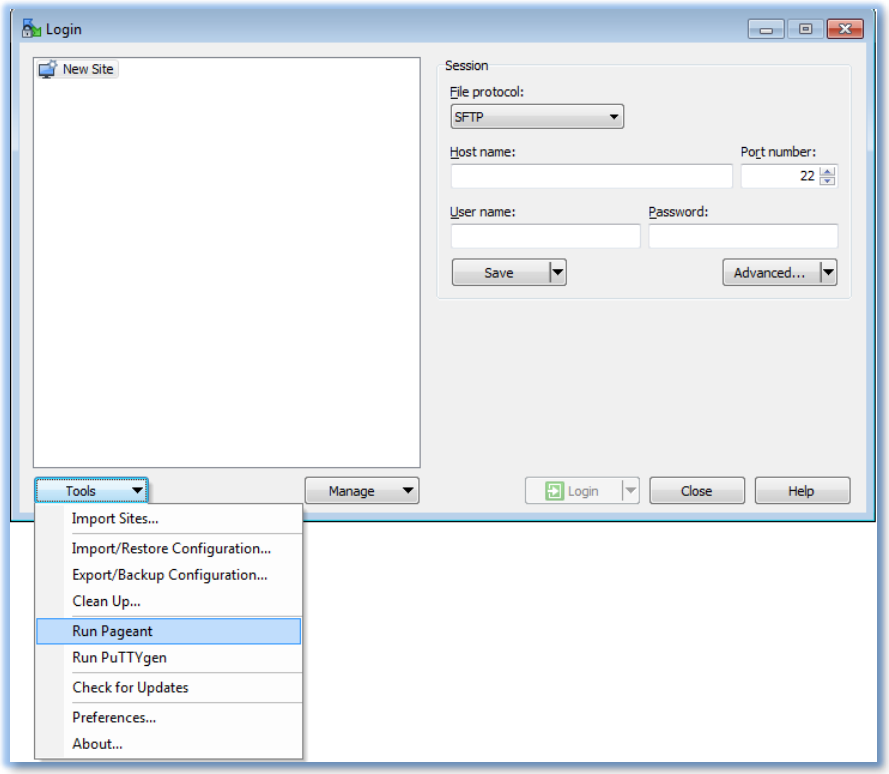
This section provides instructions for connecting to the ISO's SFTP server using WinSCP software.[ii]

These instructions assume that users have completed the following tasks:

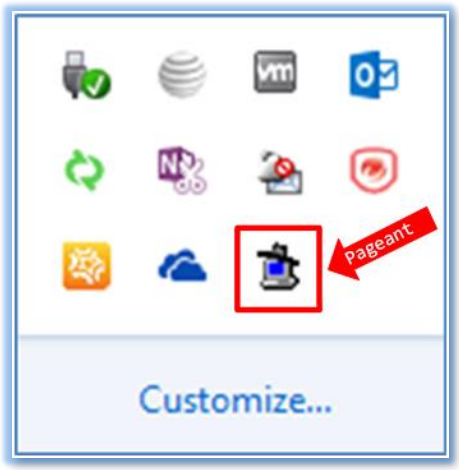
- Installed WinSCP, including PuTTY tools.[iii]
- Created SSH key pair.
- Completed the SFTP AARF and sent it to the ISO with the public key using the instructions in the SFTP AARF.

1. Configure WinSCP to use keys for authentication instead of a password.

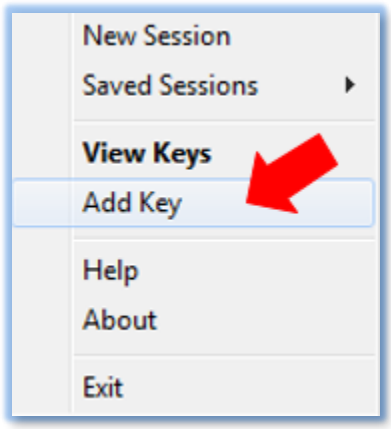
   a. Launch WinSCP.
   b. From the WinSCP Login form, click **Tools**.
   c. Select **Run Pageant**.



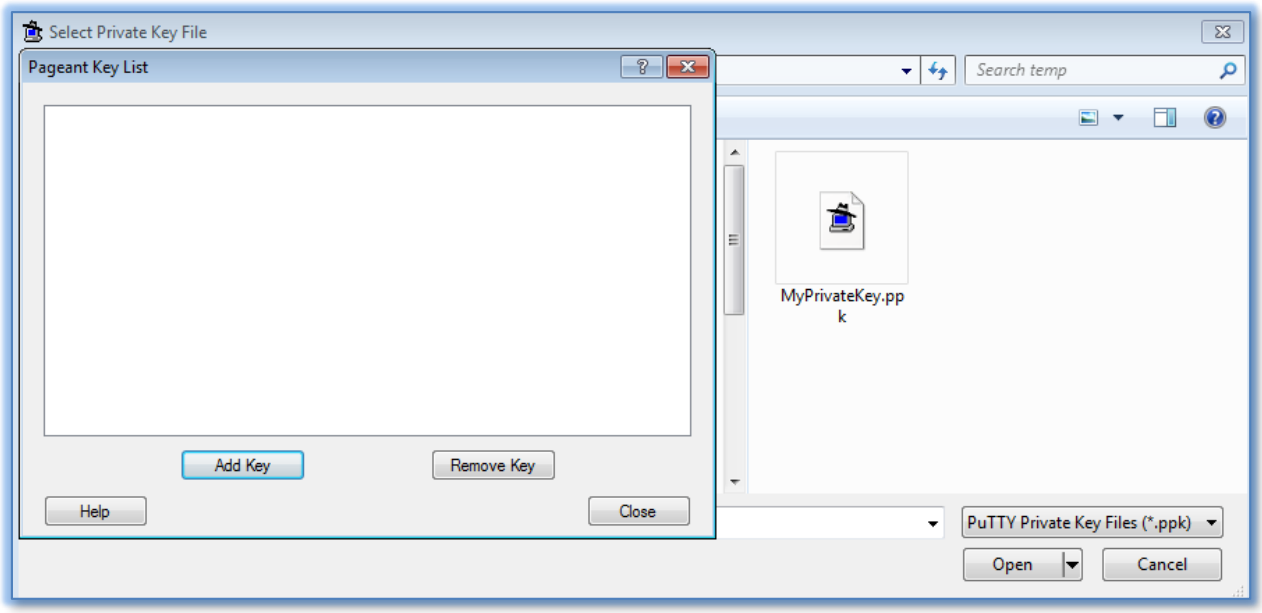
d. Open Pageant from the Windows taskbar. The Pageant icon is a computer wearing a hat.



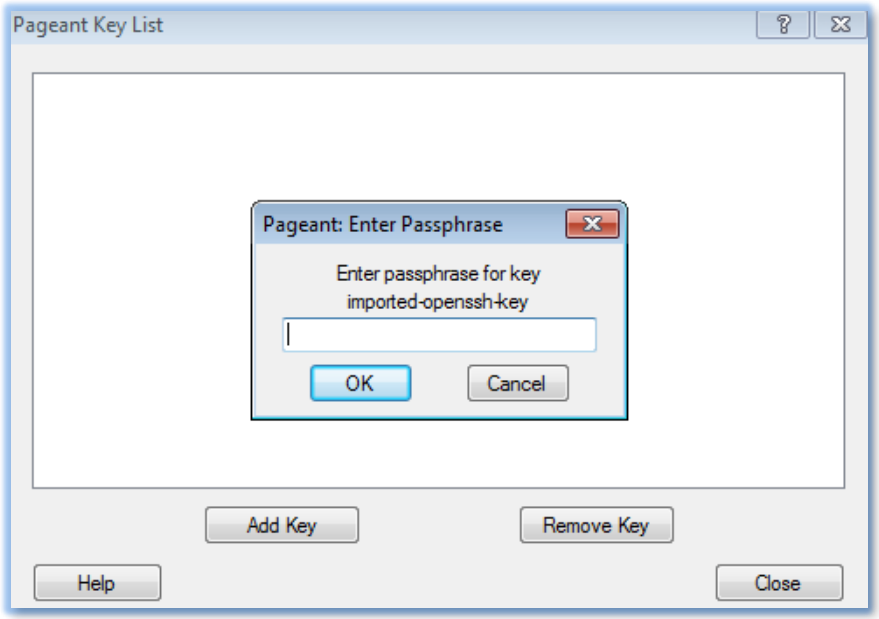
e. Right-click the Pageant icon and select **Add Key** to open the Pageant Key list form.



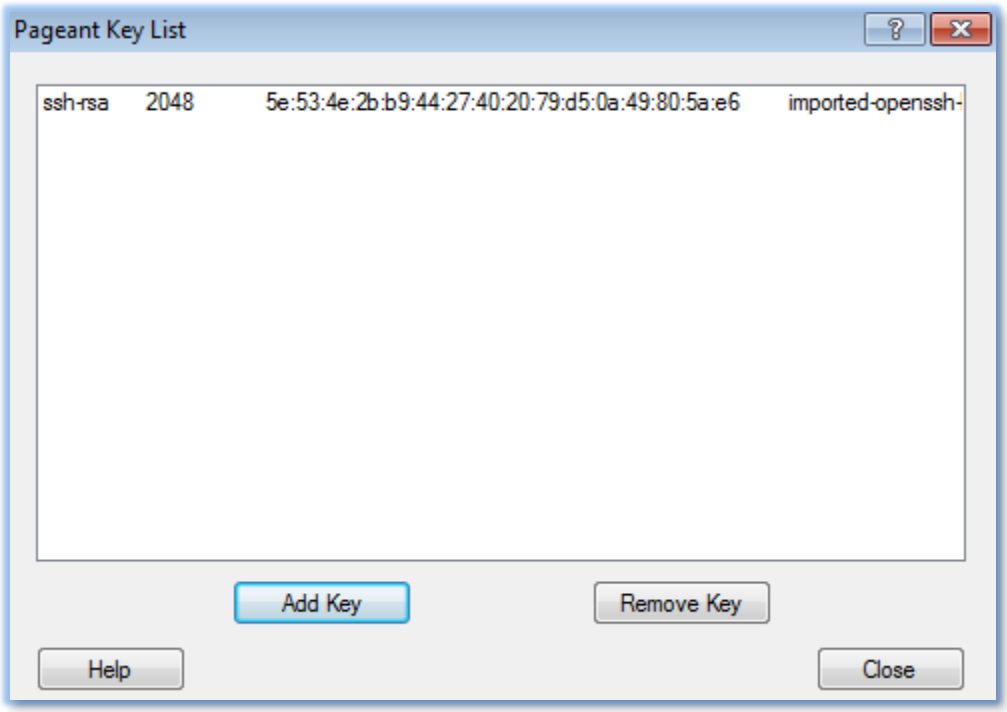
f. The Pageant Key List form will open. Select **Add Key** to open a **Select Private Key File** dialog.
g. Navigate to the private key and select **Open**.



h. If the private key is encrypted with a passphrase, enter the passphrase and click **OK**; otherwise just click **OK** to add the private key to the Pageant key list.



i. The result will be a **private** key in Pageant showing the type of key, its bit strength, a hexadecimal string called a fingerprint, and a key comment. WinSCP will use this key to authenticate when the username in the Login form matches the key's username.[iv]

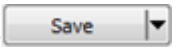


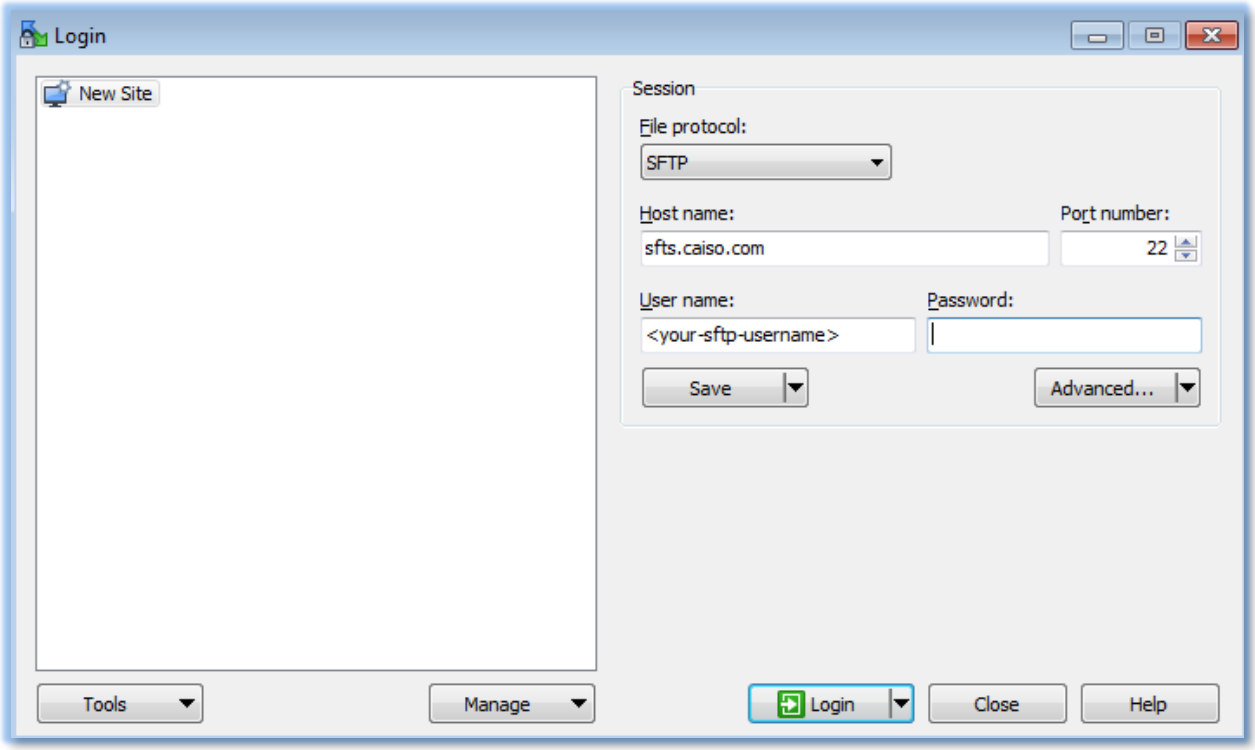
2. Configure the WinSCP Login form to use the ISO's SFTP Service.

   a. On the WinSCP Login form, enter the following:

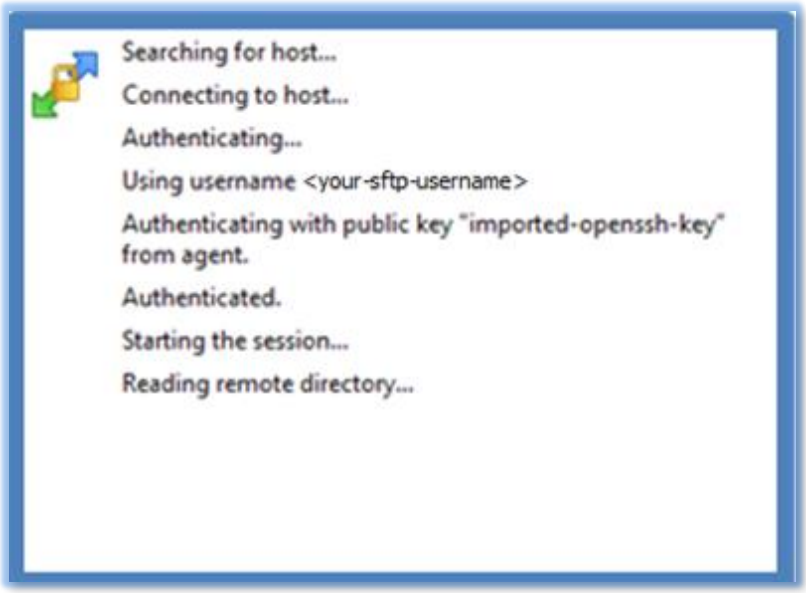
   - **File protocol:** SFTP
   - **Host name:** sfts.caiso.com
   - **Port number:** 22
   - **User name:** <ISO-provided username>
   - **Password:** <leave blank; the private key handles this>

Note: sfts.caiso.com is the name of the ISO's production SFTP server (synonymous with host). The ISO's MAPStage SFTP host name is **sfts-ms.caiso.com**.

b. To save configured settings for future use, click **Save**  and select **Save** from the drop down menu.
c. Click **Login** to connect to the ISO's SFTP service.



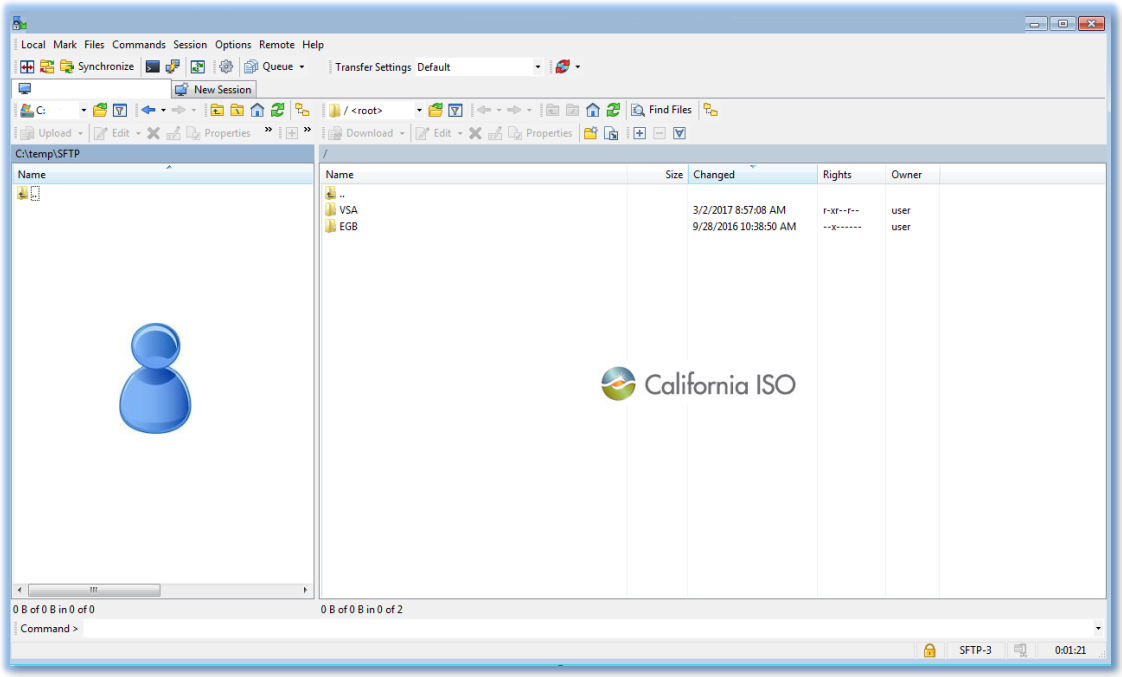
d. The PuTTY login status, as depicted below, will display use of the public key and associated username for authentication.



e. The result of a successful login will be a list of authorized ISO SFTP folders (on the right) and local user folders (on the left). In this example, the user has access to Voltage Stability Analysis (VSA) and Gas Burn Reports (EGB). A user who has access to only one application would directly see all the files in that application folder. The user would not need to navigate into the folder to see the files.

f. Transferring and receiving files is as simple as drag-and-drop:

- User drags from the **user folder** (on the left) to the **ISO folder** (on the right) to **upload**
- User drags from the **ISO folder** (on the right) to the **user folder** (on the left) to **download**


Local Mark Files Commands Session Options Remote Help
Synchronize
Queue
Transfer Settings Default
New Session
Find Files
Upload
Edit
Properties
Download
C:\temp\SFTP
/ <root>
Name
Size
Changed
Rights
Owner
VSA
3/2/2017 8:57:08 AM
r-xr--r--
user
EGB
9/28/2016 10:38:50 AM
--x------
user
California ISO
0 B of 0 B in 0 of 0
0 B of 0 B in 0 of 2
Command >
SFTP-3
0:01:21

7. SFTP Quick Launch Checklist

Users can set up an SFTP account via these simple steps:

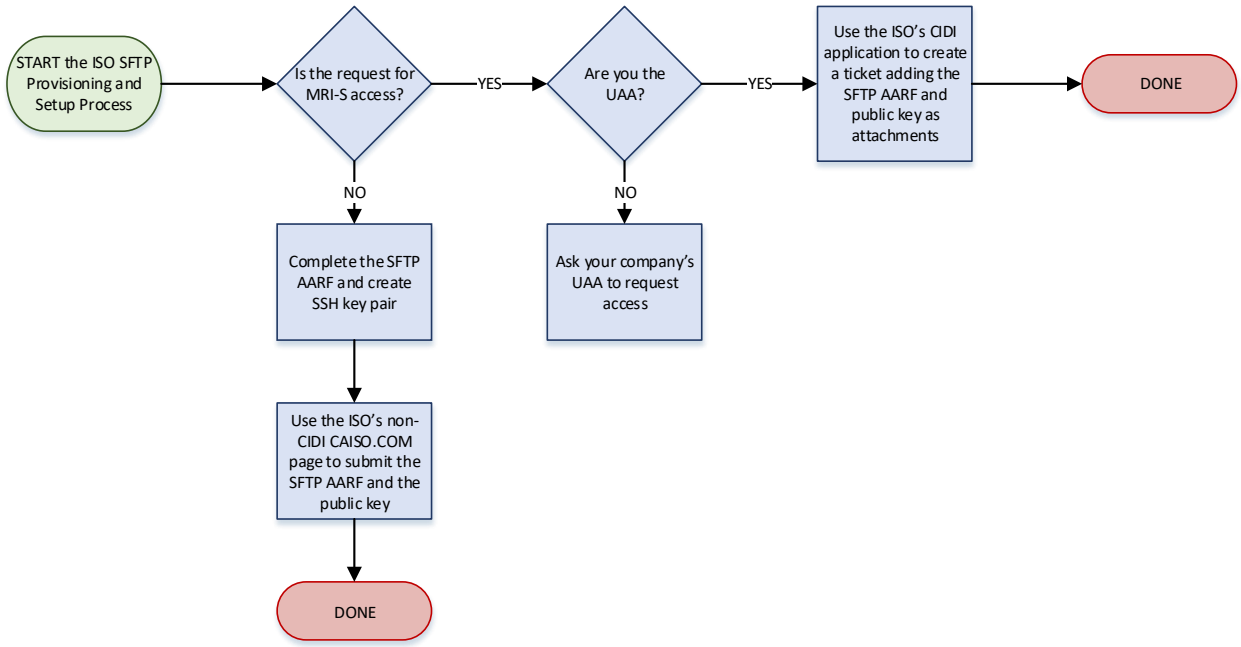
1. Download required client software.
2. Complete the ISO SFTP Application Access Request Form.

   For more help with the SFTP AARF, refer to the AARF Request Form Reference Guide.
3. Create SSH public and private key pair.
4. Send SFTP AARF and the SSH **public** key to the ISO using the instructions in the SFTP AARF.
5. Log in to the ISO's SFTP server.

Note: The ISO's SFTP server uses SSH key authentication rather than password authentication.

6. Transfer files or receive transferred files.

8. SFTP Access Request Diagram



[i] A hash is a cryptographically generated fixed-length digest or summary of file bytes. To verify the integrity of a file, compare a hash of the file after download to a hash published by the software developer; the two hashes must match exactly for you to be sure that the file did not change in transit, meaning that downloaded successfully and without corruption or modification. There are many ways to take a hash of a file. Built-in tools include certutil.exe (Windows) and, on other platforms, md5sum, sha1sum, and cksum. Full instructions are beyond the scope of this document but easily found through Internet searches.

[ii] The ISO does not endorse any particular tool or method. WinSCP is licensed as free software under the terms of the GNU General Public License (GPL).

[iii] There is no requirement to use WinSCP software to connect to the ISO's SFTP service. Users might already have SFTP software that will work. The ISO does not endorse any particular software for this purpose.

[iv] Pageant will hold this key until the computer is restarted or Pageant is closed.