

## STANDARD OPERATING PROCEDURE --- INFORMATION TECHNOLOGY

---

**TITLE:** REMOTE ACCESS  
**LOCATION:** ATA  
**PARTICIPANTS:** REMOTE USERS (SRI, SETI, OR AFFILIATES)

---

### CONTENTS:

[Description](#)  
[SSH Toolset](#)  
[Authentication Key/User Account configuration](#)  
[SSH Agent](#)

### DESCRIPTION:

This document describes how to setup and access the ATA bastion host blake7 via secure shell (SSH) with public key authentication. Users are assumed to be on a Windows platform in which case they are using some form of terminal emulator with SSH support than can provide a secure and encrypted link. Unix users are assumed to be using the openSSH set of tools. *Note – regardless of the OS and SSH tool used, users must generate their key pair from within the same tool set as their ssh access tool as key format is often unique to the tool set.*

### SSH TOOLSET:

Several tools exist to provide terminal emulation and SSH support within non-unix environments.

To install PuTTY (see Windows installer in download section);

<http://www.chiark.greenend.org.uk/~sgtatham/putty/>

To install X-win32:

<https://www.starnet.com/xwin32kb/using-key-based-authentication-with-x-win32-ssh/#install>

To generate with X-win32:

<https://www.starnet.com/xwin32kb/using-key-based-authentication-with-x-win32-ssh/>

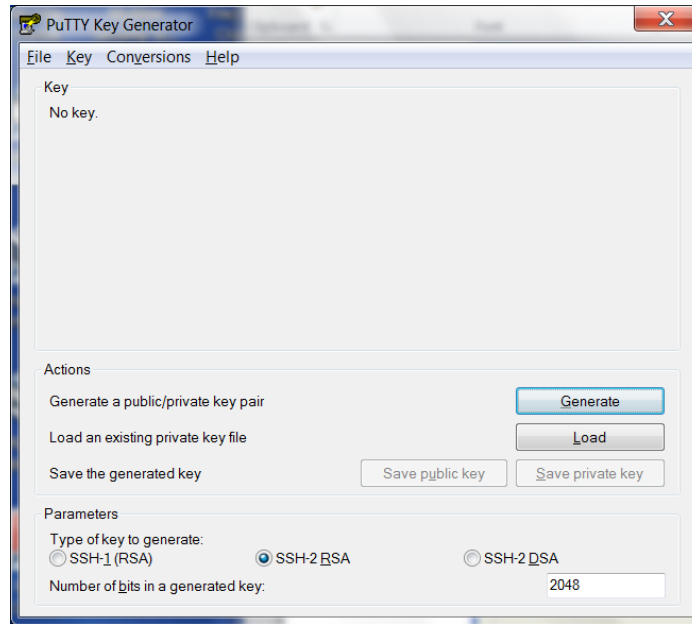
### AUTHENTICATION KEY/USER ACCOUNT CONFIGURATION:

Secure SSH (e.g., openSSH, etc.) requires the usage of a public/private key pair for authentication. Your private key (passphrase protected) is kept locally on your machine and your public key is installed onto sites to which you will want to connect.

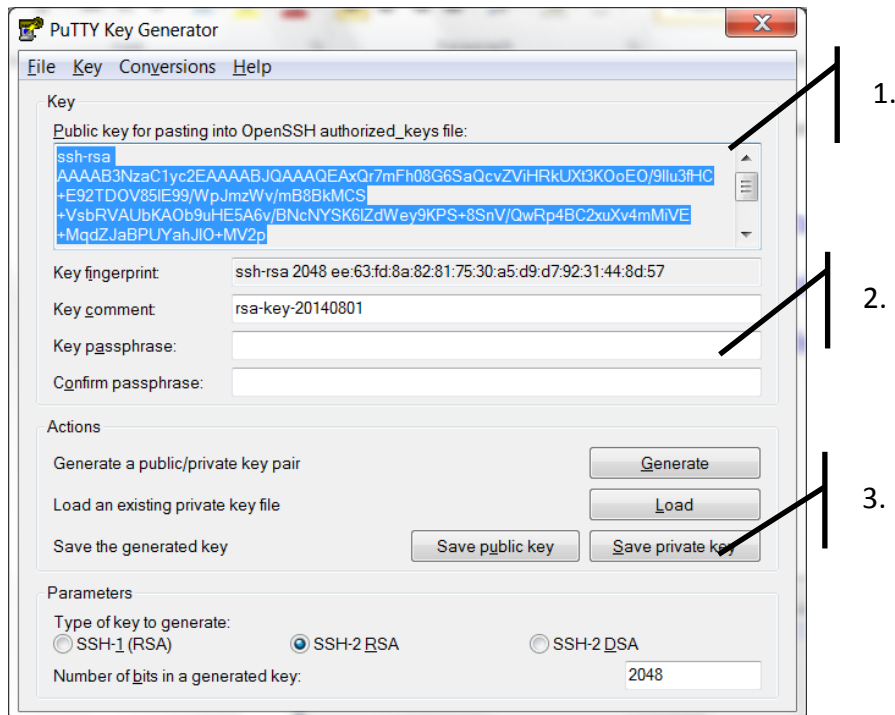
If you already have a public/private key pair for your origin machine, then you can use those.

The following example uses PuTTYgen.

- Click on/invoke the **PuTTYgen** executable.
- Select “SSH-2 RSA” type of key to generate
- Click on Generate



- Follow the instruction to move the mouse over the blank area of the program in order to create random data used by PUTTYGEN to generate secure keys. Key generation will occur once PUTTYGEN has collected sufficient random data.



- [1] Select the information contained in the "Public key for pasting...". Copy it (ctrl-C).
- Paste the copied information into a file or directly into an email message and send to the SRI representative. This is the public key (in required format) that will be installed in your ATA authorized keys file on blake7.

- [2] It is strongly recommended to specify a key passphrase for the private key. The passphrase is used to encrypt the private key (i.e., a local matter). See SSH authentication agent below to assist in passphrase management/usage.
- [3] Click on "Save private key". Use the default name. Save in directory you will remember. This file & location will be needed when setting up your PuTTY profiles. It is also recommended to save a backup copy of the private key (which will require yet another password). Once a passphrase is lost, the key is no longer useable (to you). If you leave your private key unprotected without a passphrase, then it can be compromised/stolen by others.
- Click on "Save public key" and save to a directory you will remember with an appropriate name. Note - this public key file contains the same information you copied and sent to SRI but has a slightly different header/footer format that is incompatible with Linux systems (such as at ATA).

### USING AN SSH AGENT – PUTTY PAGEANT KEYCHAIN:

To establish the secure remote connection, you will need your private key file and its passphrase. The corresponding public key will have been installed on the authorized keys file on the server. When you connect to the server via **PuTTY**, the keys are matched to verify your access. To help manage and share the keys between different applications, an SSH agent can be used. The PuTTY installed **Pageant** program provides a secure way of storing the private key and allows the user to connect multiple times without having to repeatedly type the passphrase. This is referred to as a "key chain".

Save the key that we send you, then open **Pageant** from the Start menu. You'll find it in the Putty directory of the start menu. You should see a small icon appear in the tool bar in the lower right of the screen. It is a small computer with a hat [4]. Right click on the icon and choose "Add Key" from the menu. You'll be presented with a dialog box from which you should pick the key file that we sent you. You will then be asked for the passphrase to unlock the key.

You will need to repeat this step each time you restart Windows.

