TERRADOTTA

Description: Hosted and SaaS clients who have purchased Terra Dotta's standard integration will follow an accelerated project timeline (after the technical kickoff meeting). To facilitate the accelerated timeline, Terra Dotta will run daily check-in meetings with technical and functional staff. NOTE: The accelerated integration timeline does not apply to clients who intend to implement the SEVIS module, as these projects typically last longer.

This document outlines the deliverables that the client is responsible for completing by each day (June 22nd - June 24th)

Deferred Fetch-Shibboleth Authentication		
Deliverable	Weekly Meeting	Phase
Key Pair, post public key in integration case	Day 1: June 22nd	Planning Phase
Provide Public (4) IP Address(es) to SFTP		
Test file to test SFTP/SSH connection		
CNAME added to DNS		
Provide CSR information (Custom URL)		
Obtain SSL Cert (Custom URL)		
Both Sample SIS file (Core and Custom) with final parameter set		
Provide all SCL info		
Provide *working* test user credentials		
Review applicant parameter settings	Day 2: June 23rd	Building Phase
Set up job to automate nightly file generation		
Schedule process to pick up pool file	Day 3: June 24th	Test Phase
Testing/Final Configurations		

TERRADOTTA

SSH Folder

[Carl Ellsworth] We have created an account for secure file transfer using sftp protocol. We require the use of public key exchanges for the authenticated connection to our SSH server, rather than passwords.

Please generate a public key for the connection and attach to this case:(Attached is the document for instructions on its use in a Linux and Windows environment to this case.)

- use SSH-2
- bit length: 4096
- username: USU-SA
- hostname: sftp-us-03.terradotta.com
- port: 22

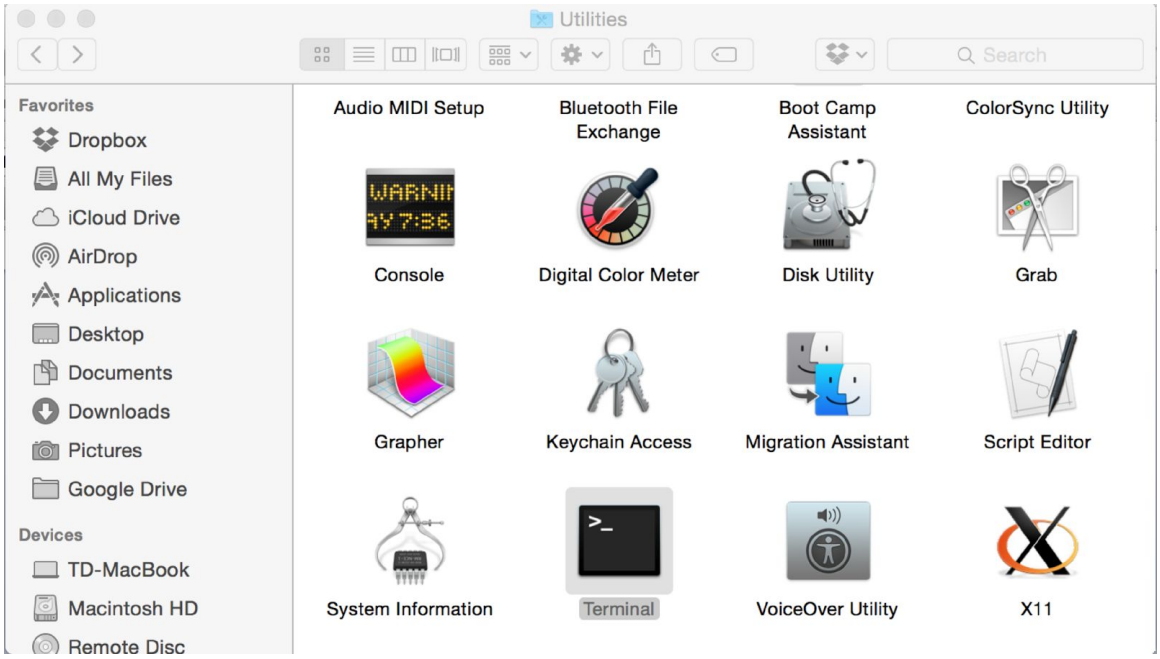
Note: For the connection we need to white list your public IP in our SFTP server. So Please provide your Public IP Address along with this case, maximum 4 IP address can be whitelisted.

TERRADOTTA

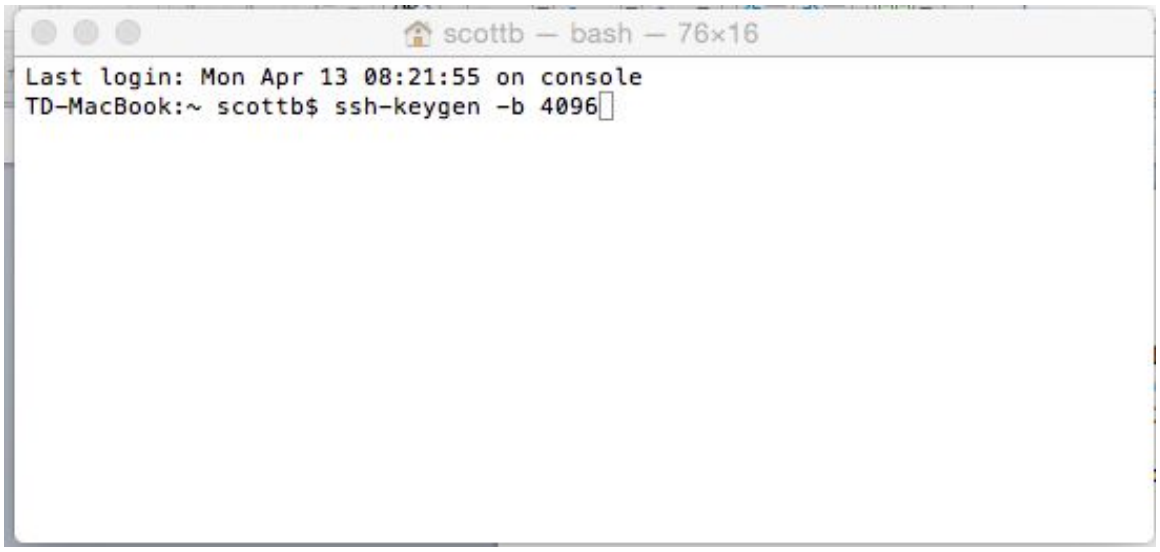
Generate a public key in a Linux Environment

How to create a new public-private key pair for authentication to Terra Dotta SSH servers on a Mac

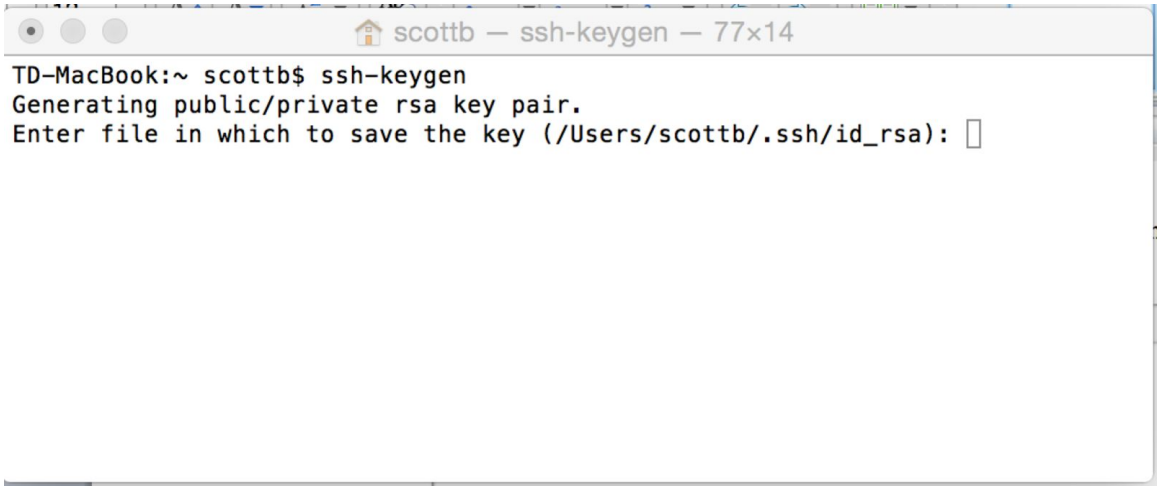
1. Launch Terminal from the Applications/Utilities folder or through Spotlight Search.



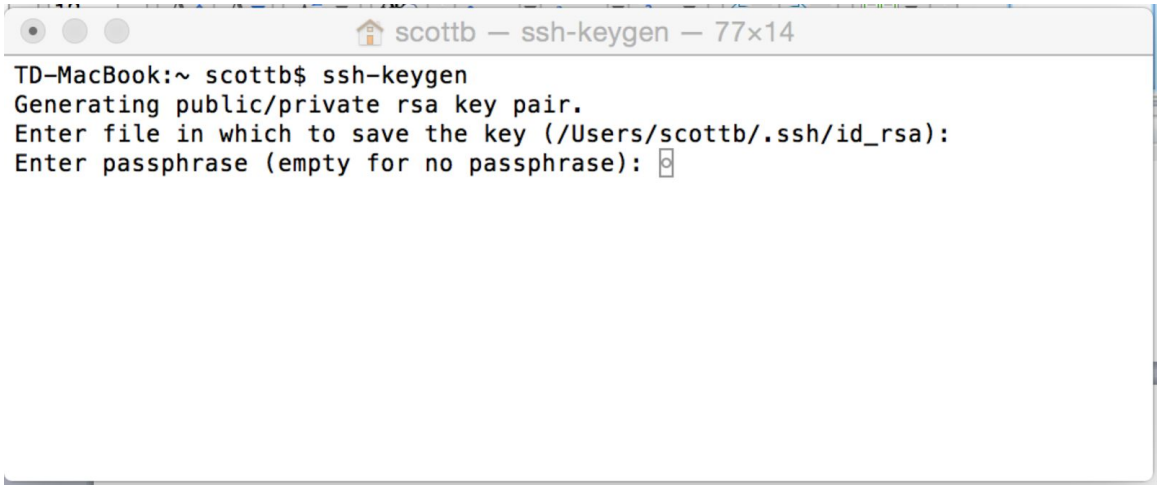
2. In the terminal window, type the following command and press the Return key: ssh-keygen -b 4096



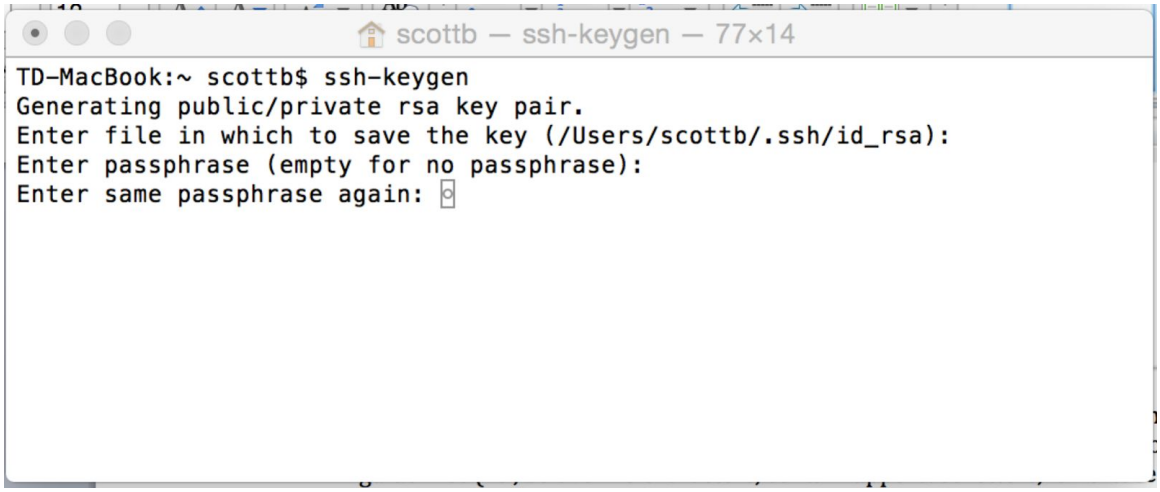
3. Press Return again to confirm the default location in which the new key pair will be stored.



4. Enter a passphrase that will protect access to your private key and press the Return key. This passphrase should conform to secure password generation guidelines (i.e., be over 16 characters, contain uppercase letters, lowercase letters, numbers and special characters, and should not be based on personal information or any words in any language).

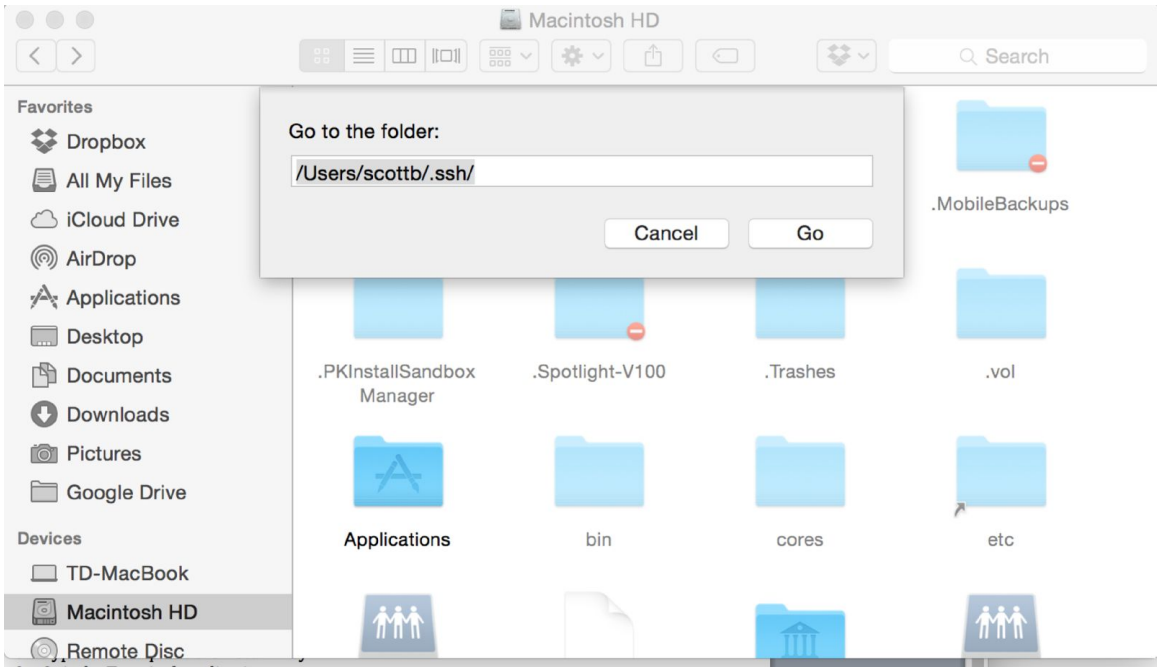

scottb — ssh-keygen — 77×14
TD-MacBook:~ scottb$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/scottb/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):

5. Verify the passphrase and press the Return key.



Be aware that your SFTP client may require this passphrase to initialize a connection successfully!

6. Record your passphrase and store it in a physically secure location and/or in an encrypted file or password management software program.
7. You should see that the key has been generated and stored in the default location.
8. Type exit and press the Return key
9. Quit the Terminal application.
10. Open the Finder and go to the Go menu and select Go To Folder.
11. In the new window, type /Users/[YourUserName]/.ssh and press the Return key.



12. Copy the id_rsa.pub file from the .ssh folder to a temporary directory. You may use your Documents folder, your Desktop, or you can create new folder in which to store the key.
13. You may communicate your public key to Terra Dotta in one of two ways:
    a. Attach the id_rsa.pub as a file to a reply to the email that you received from Terra Dotta that requested the key, or
    b. Open the id_rsa.pub key in a text editing program (e.g., Notepad) and copy and paste its contents into an email reply to the email that you received from Terra Dotta requested the key.
    c. Log into the TDS Support Portal and attach the public key to your integration case.

    Important Final Step! Back up both your public and private key in a physically secure location and/or in an encrypted file or secure password management program.

If you have any questions about this process or encounter any errors while generating your keys, please log into the Terra Dotta Support Portal and place a comment in your integration case.

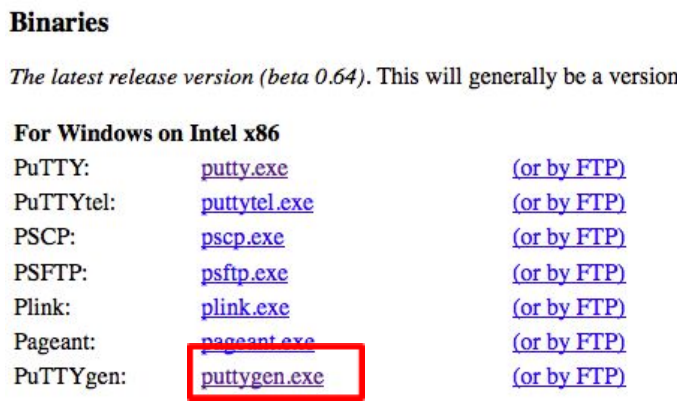
Return to top of 'Generate a Public Key in a Linux Environment'

TERRADOTTA

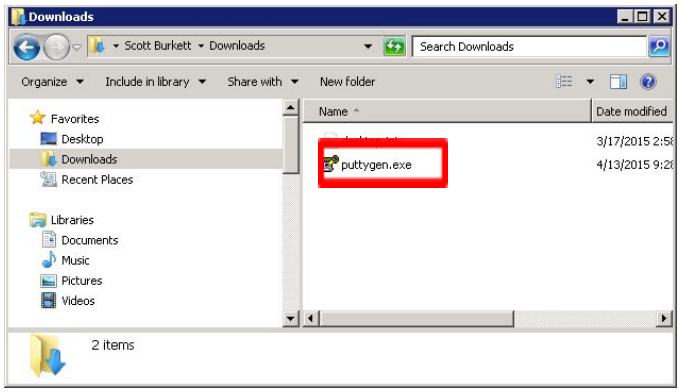
Generate a Public Key in a Windows Environment

How to create a new public-private key pair for authentication to Terra Dotta SSH servers on a Windows server or Windows workstation

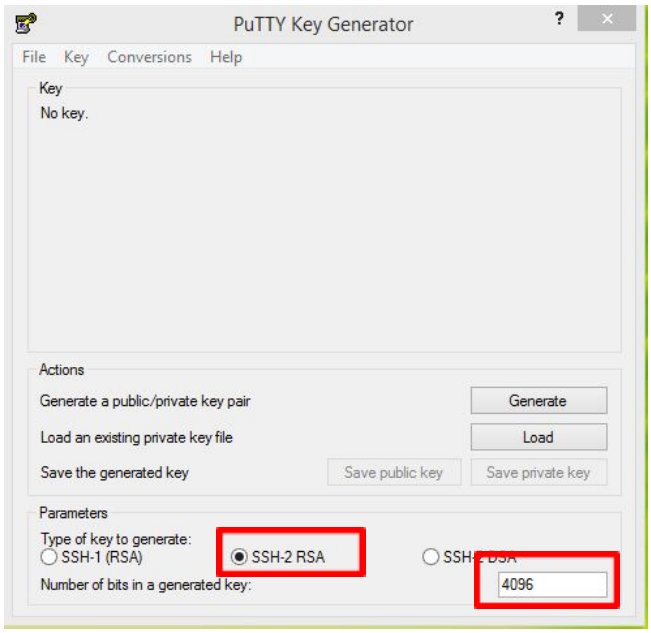
1. Download and install puttygen.exe from http://www.putty.org .



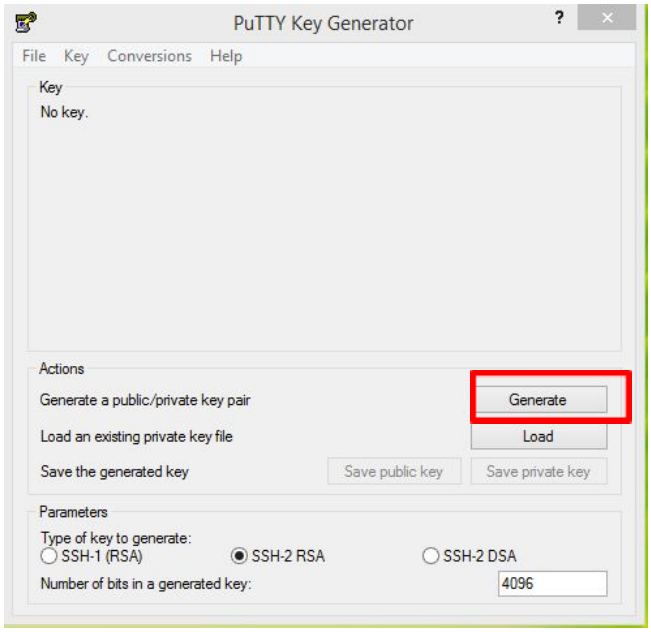
2. Launch puttygen.exe by double-clicking the file in your Downloads folder.



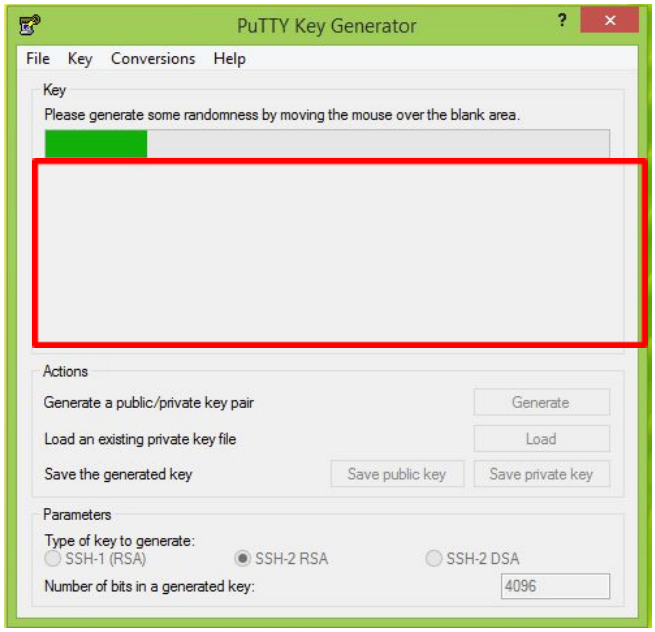
3. In the PuTTY Key Generator window, under the parameters heading, make sure that the type of key generated is set to SSH2-RSA and make sure the **Number of bits in a generated key is set to at least 4096**.



4. Under the Actions heading, click the Generate button.

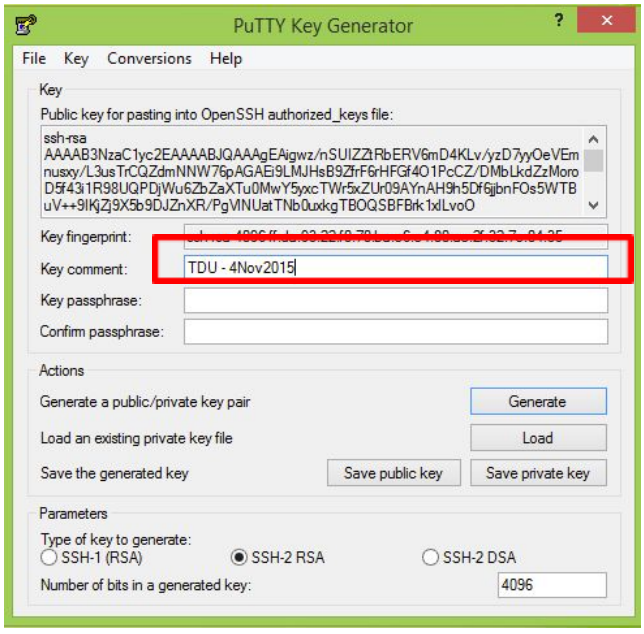


5. Move the mouse in the area underneath the green progress bar. Random movements of the mouse allow the PuTTY Key Generator to increase the randomness of the key that is being generated.

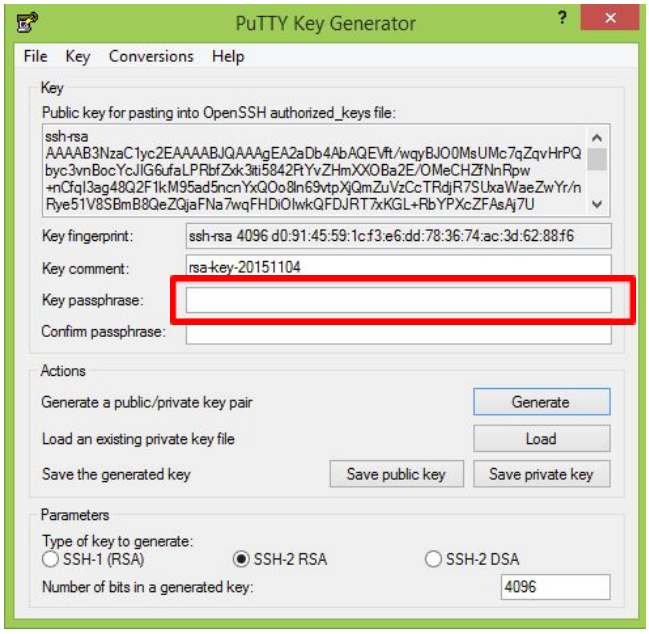


Note: This process may take several minutes to complete!

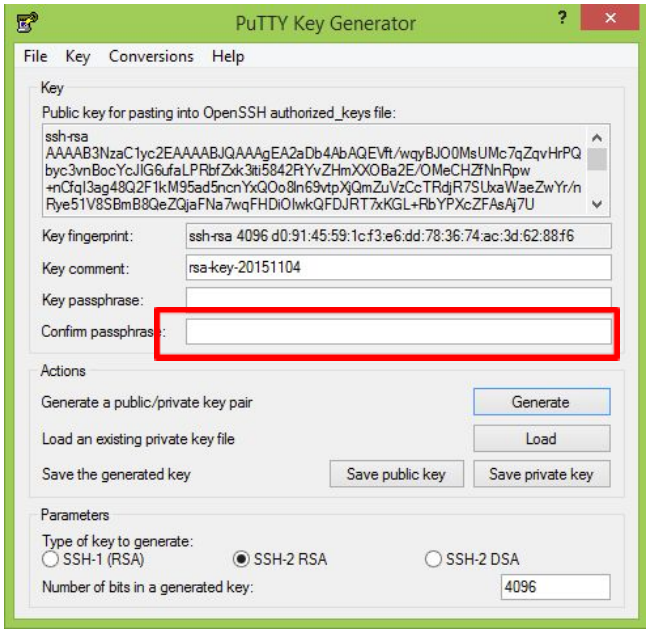
6. In the key comment section, enter a comment that identifies the college, university or organization that will be using this key and the date that the key is generated. For example, for a key that will be used for Terra Dotta University that will is generated on November 4, 2015, the key comment might be "TDU - 4Nov2015".



7. After the key has been generated, enter a passphrase that will protect access to your public and private keys and press the Return key. This passphrase should conform to secure password generation guidelines (i.e., be over 16 characters, contain uppercase letters, lowercase letters, numbers and special characters, and should not be based on personal information or any words in any language). Do not lose this passphrase. If necessary, record the passphrase and store it in a physically secure location and/or in an encrypted file or secure password management program.

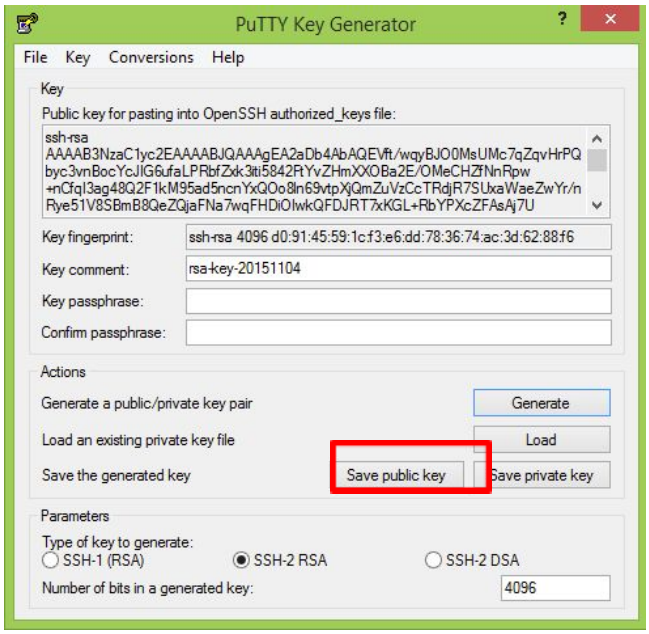


8. Confirm the passphrase in the field below the Key Passphrase field.

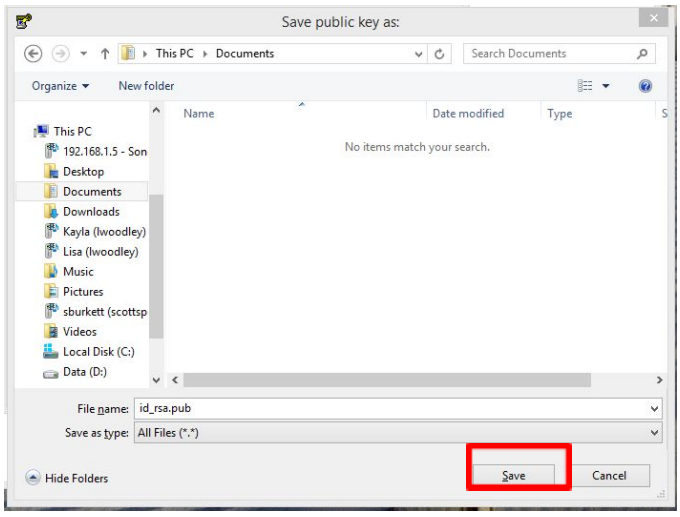


Be aware that your SFTP client will require this passphrase to initialize a connection successfully!

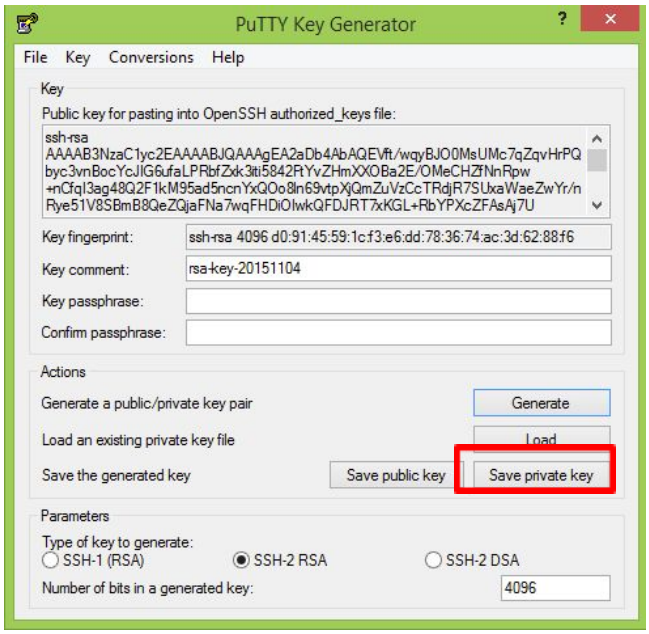
9. Click on the Save public key button.



10. Navigate to a folder in which you wish to save the public key file, name the file id_rsa.pub and click the Save button.

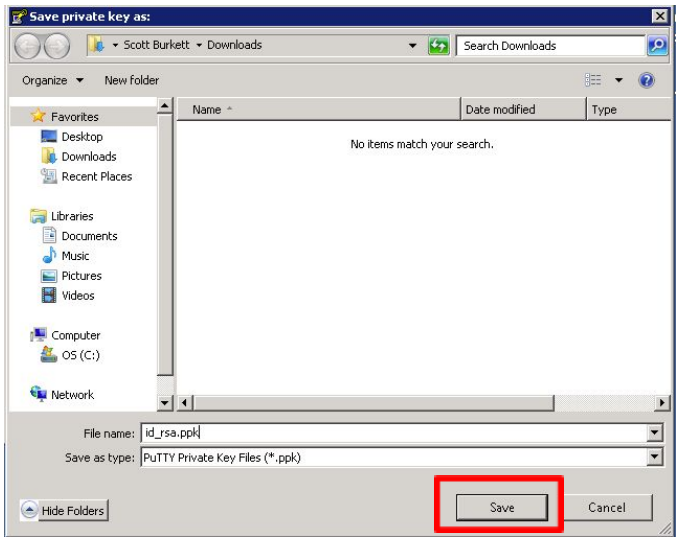


11. Click on the Save private key button.



12. Navigate to a folder in which you wish to save the private key file, name the file id_rsa.ppk and click the Save button.

> *Important Note! Do not share your private key with anyone. Anyone who has a copy of your private key can use it to impersonate you on the Internet.*





TERRADOTTA

13. You may communicate your public key to Terra Dotta in one of two ways:
    a. Attach the id_rsa.pub as a file to a reply to the email that you received from Terra Dotta that requested the key, or
    b. Open the id_rsa.pub key in a text editing program (e.g., Notepad) and copy and paste its contents into an email reply to the email that you received from Terra Dotta requested the key.
    c. Log into the TDS Support Portal and attach the public key to your integration case.

    Important Final Step! Back up both your public and private key in a physically secure location and/or in an encrypted file or secure password management program.

If you have any questions about this process or encounter any errors while generating your keys, please log into the Terra Dotta Support Portal and place a comment in your integration case.

Return to top of 'Generate a Public Key in a Windows Environment'

TERRADOTTA

Custom URL DNS Instructions and CSR Request:

Please consult with your Integration Analyst before completing any of the steps outlined below as they are to be completed in a specific order. This is done so that the project is completed efficiently and effectively.

[Blake Rich and Eric Allen] The procedure for using a Custom URL entails the creation of a CNAME record in DNS, aliasing a Terra Dotta host name.

1. The CNAME should reference USU-SA.terradotta.com.

Network admins: do not point DNS entries to the 'A' records/machine-host names for these intermediary names. For example, if USU-SA.terradotta.com responds to pings as hosting-lou-140.terradotta.com, DO NOT create your CNAME to alias hosting-lou-140.terradotta.com, only use USU-SA.terradotta.com. This is to facilitate a seamless transition in the event of hardware or IP address changes on Terra Dotta's side.

After making the DNS change, please let us know and we will setup your site to accept traffic from the custom URL.

2. Provide Terra Dotta with the following CSR information:
   Common Name: studyabroad.usu.edu
   Bit Length: 4096 bit
   Organization:
   Organization Unit: (The name of your office as reflected in the account settings of your website.)
   State:
   City:

3. Generate SSL certificate: Once Terra Dotta receives the information required to generate a CSR (#2 above), Terra Dotta will provide you with a CSR to generate the SSL certificate to cover the post login pages.

NOTE: Terra Dotta does not accept wildcard SSL certificates from clients. The SSL certificate you provide must be associated with the CSR Terra Dotta will generate for you.

After a new DNS host name is configured for your site, any other websites or pages that link to your Terra Dotta site will need to have their link URLs changed to the new URL. For that reason it's a good idea to wait until after configuring the host name to establish any links.



TERRADOTTA

Data Files

Please consult with your Integration Analyst before completing any of the steps outlined below as they are to be completed in a specific order. This is done so that the project is completed efficiently and effectively.

[Carl Ellsworth]

1. **Core Data File** should be named ***sis_user_info_core.txt*** and should contain only the following column headers:

    - UUUID
    - First Name
    - Last Name
    - *Middle Name
    - Email
    - DOB
    - Gender
    - Confidentiality Indicator

2. **Custom Data File** should be named ***sis_user_info_custom.txt*** and should contain the following column headers:

    - UUUID
    - Class Level
    - Academic Level
    - Country of Citizenship
    - Visa Status
    - Cell Number
    - Cumulative GPA
    - Financial Hold
    - Academic Hold
    - Major 1
    - Major 2
    - Minor 1
    - Minor 2
    - Expected Graduation Date
    - Preferred Name
    - Emergency Contact
    - Campus Address
    - Permanent Address

3. **HR File** should be named ***hr_user_info_core.txt*** and should contain only the following column headers:
    - UUUID
    - First Name
    - Last Name
    - *Middle Name
    - Email

NOTE: Column headers labeled with an asterisk (*) are not required.



TERRADOTTA

Provision via the SSH connection a SAMPLE of the data feed file(s) as defined at https://tdsupport.force.com/support/articles/General/Data-Feed-File-Requirements (The extract file should never be provided via a case ticket. Please SFTP/SCP it via the SSH connection.)

The sample file will be used as a template for the data loader and the intermediary data table, so it must be an exact representation of the structure/columns of the eventual production file. (If HR/staff data will be delivered in the same file as applicant data, the file must include a flag column indicating which records are to be considered HR/staff.)

With these steps complete, Terra Dotta will proceed with reviewing the files and completing the SIS integration and mappings.



TERRADOTTA

Authentication

Please consult with your Integration Analyst before completing any of the steps outlined below as they are to be completed in a specific order. This is done so that the project is completed efficiently and effectively.

[Eric Allen] Here is an overview of Shibboleth User Authentication:
The Terra Dotta servers will act as the Shibboleth Service Provider. A directory in the Terra Dotta system installation will be secured by Shibboleth, /secure. When a user needs to be authenticated, they will be directed to the secured directory. The Shibboleth service will redirect the user to the Shibboleth Identity Provider. The Identity Provider service is supplied/supported by the client. Once the user properly authenticates through the Identity Provider service, various attributes are sent back to the Service Provider. We parse the attributes and log the user into the Terra Dotta system as appropriate.

In order to set up Shibboleth authentication, we need the following:

1. Shibboleth Identity Provider metadata XML: this XML contains the IDP URL, which protocol is supported (SAML2, SHIB1, etc) as well as other things. These configuration steps are outlined at https://wiki.shibboleth.net/confluence/display/SHIB2/Configuration.

1. Provide the full SAML2 Name for the UUUID attribute that will be sent back from the IdP. We typically expect that this will be an oid number (example: name="urn:oid:2.16.840.1.113730.3.1.3")

*To create the user account initially, TDS looks up the additional parameters in a file provisioned with a full population of potential users based on the returned attribute.

1. Provide us with a required username and password for a test user so that we are able to test the the authentication system while setting up the integration..

1. Provide us with the UUUID attribute value that we will be receiving back for the test user.

*The test authentication credentials are an important element that is required for completion of the integration project. If a dummy test user must be created, please provide the dummy (generic) login credentials when you submit the other information above.

After TD receives this information, we will provide you with our Shibboleth metadata to our staging environment. Before setting up your shibboleth on the production environment, we will set everything up on our staging server, once we can verify authentication we will provide you with our Shibboleth metadata to the production environment. Once we are set up in production, our Shibboleth service restarts every morning at 5 AM. After the shibboleth restart in production, the authentication process will be up and running.