# Oracle Financial Services Revenue Management and Billing Cloud Service

## sftp Authentication

ORACLE WHITE PAPER | JANUARY 2016

## Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle’s products remains at the sole discretion of Oracle.

## Table of Contents

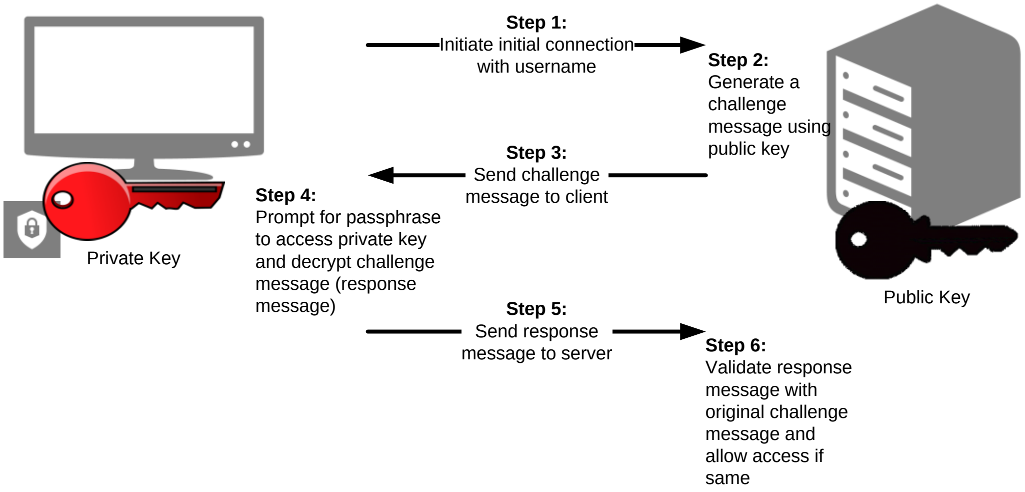
.

## Introduction

This document outlines how to establish authentication with the sftp hosts in the ORMB cloud service using keys.

## Authentication Overview

Authentication is based on a public and private key being generated. The public key is placed on the server, while the private key remains in a secure location on the client computer. These public/private keys use asymmetric cryptography to establish the clients identity.


Step 1:
Initiate initial connection with username
Step 2:
Generate a challenge message using public key
Step 3:
Send challenge message to client
Step 4:
Prompt for passphrase to access private key and decrypt challenge message (response message)
Private Key
Public Key
Step 5:
Send response message to server
Step 6:
Validate response message with original challenge message and allow access if same

Summary of ssh key based authentication.

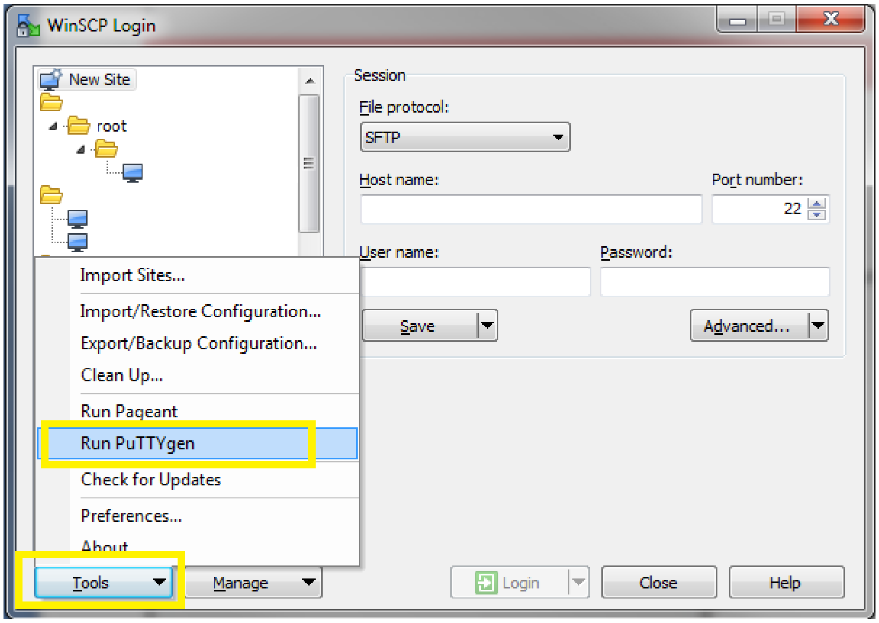
When using Key based Authentication the following occurs:

- An initial connection is made by the client providing the username and request to authenticate using keys.
- The sftp server (sshd) takes the public key for that user and constructs a message based on the public key. This message (or challenge) is returned to the sftp client.
- The client locates the local private key and prompts for a passphrase to access to local key (when necessary).
- The client then generates a response to the challenge message using the private key. This response is sent to the sever.
- The server takes the message response and validates it using the public key and grants access.

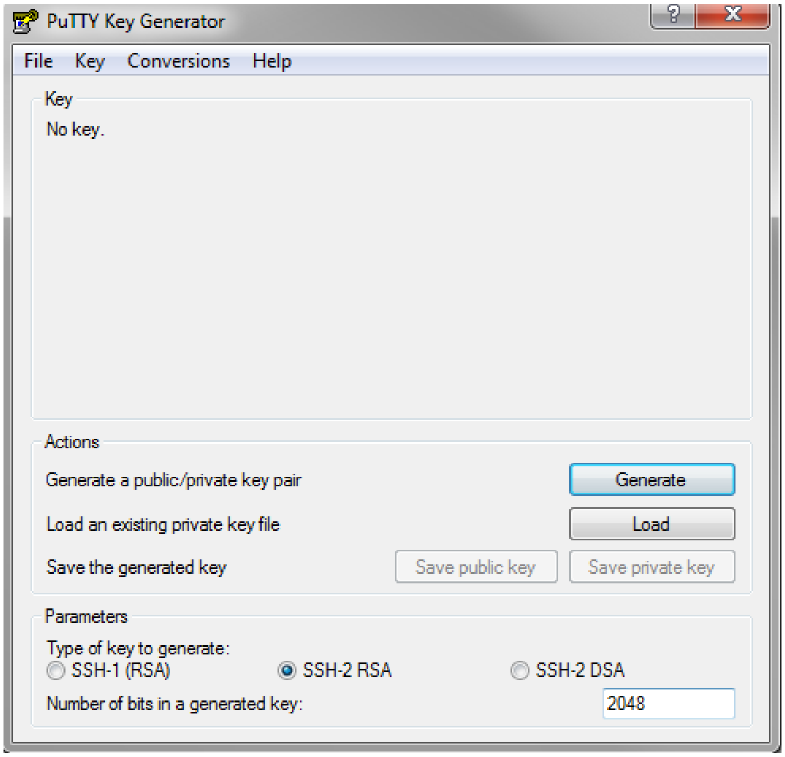
# Establishing Authentication

## Generate Public/Private Key Pair

Use puttygen.exe to generate the public private key pair. From WinSCP there is a menu item to for PuttyGen under the Tools menu as shown here:



**Step 1 – open puttygen.exe**



Key

No key.

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

Parameters

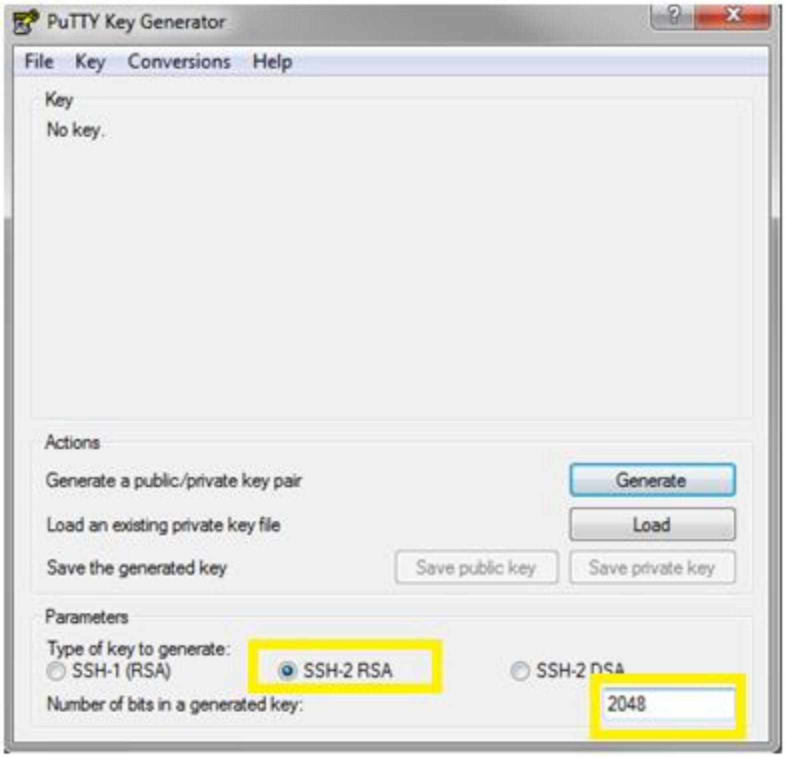
Type of key to generate:

○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 2048

Select options

- Type of key generate : SSH-2 RSA
- Number of bits in a generated key: 2048



Key: No key.

Type of key to generate: ○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 2048

**Step 2: Generate keys.**

Click on the Generate button and move the mouse as directed until the keys are generated.

Assign a comment to the key so that it can be identified.

**Step 3: Save private key**

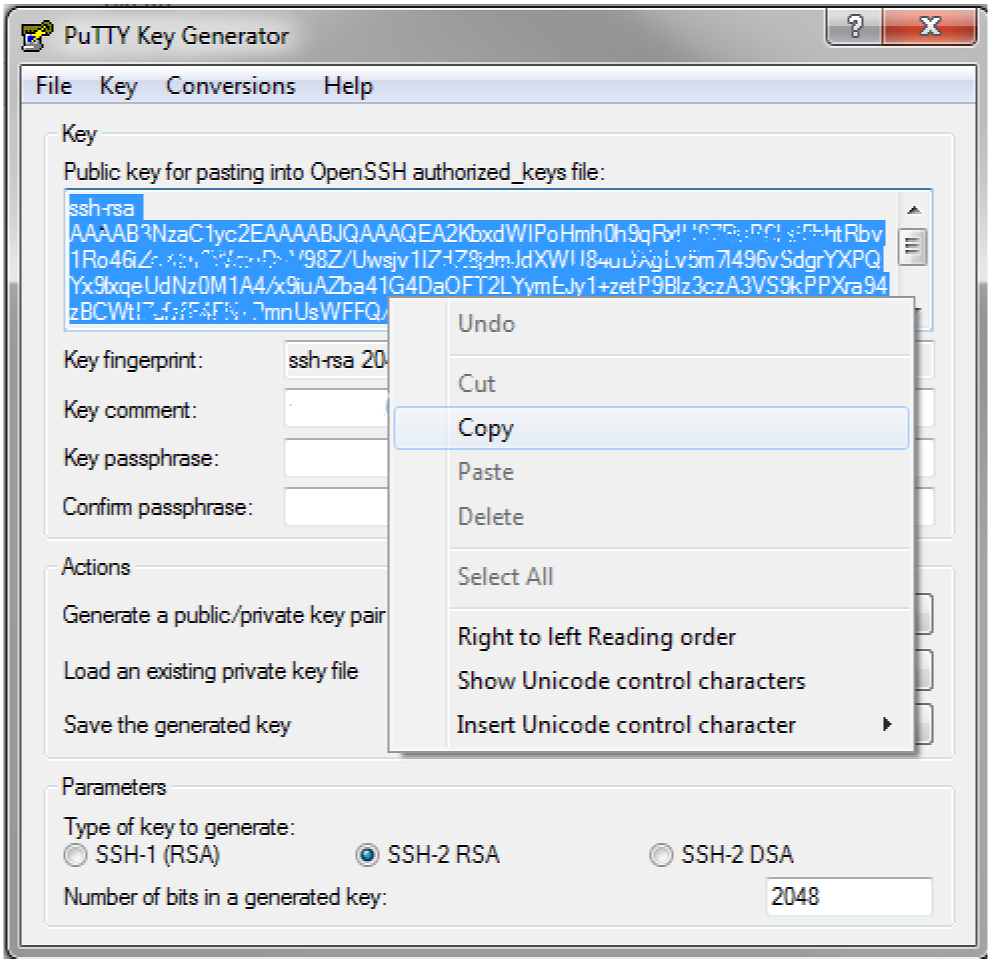
Once the keys are generated – save the private key to a secure location, assigning a pass phrase. While assigning a passphrase is not required it is strongly recommended. This passphrase will be required to subsequently access the private key.

***Important:*** *It is critically important that the private key file is secured and protected at all times.*

**Step 4: Save public key to text file**

Using the button “Save public key” saves the key in the incorrect format, a better way is to copy the public key text and from the puttygen screen and paste it into a text file to save it.

Specifically copy text from the top of the puttygen screen:



Public key for pasting into OpenSSH authorized_keys file:

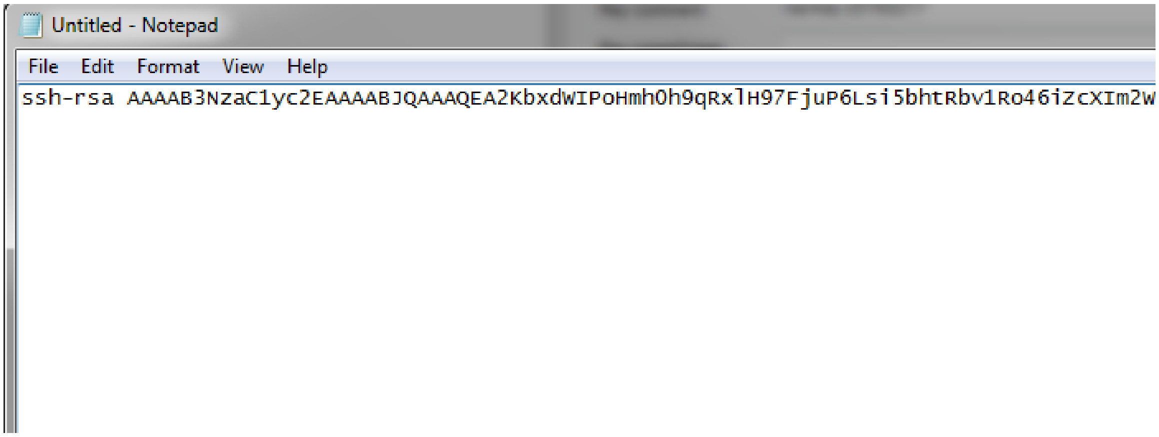
```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEA2KbxdWIPoHmh0h9qRx[illegible]htRbv
1Ro46i[illegible]98Z/Uwsjv1IZ[illegible]dmJdXW[illegible]gLv5m7I496vSdgrYXPQ
Yx9bxqeUdNz0M1A4/x9iuAZba41G4DaOFT2LYymEJy1+zetP9BIz3czA3VS9kPPXra94
zBCWt[illegible]mnUsWFFQ
```

Key fingerprint: ssh-rsa 20

Type of key to generate: ○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 2048

And paste it in a text file.



```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEA2KbxdWIPoHmh0h9qRxlH97FjuP6Lsi5bhtRbv1Ro46iZcXIm2W
```

Save this text file containing the public key.

*Tip: You may save the file with any extension, but “**.pub**” is a useful convention to indicate that this is a public key.*

Once finished you should have two files, a file containing the private key and a file containing the public key.

The private key remains in your possession, and the public key is sent to Oracle so that it can use it for authentication of the sftp service.

## Submit public key to Oracle

Raise a service request with Oracle Global Support and attach the public key file **only**. Identify both the user and environment you would like to use this public key to establish an authenticated session. The user should already have been created by Oracle and a temporary password provided. This key pair will replace the password authentication.

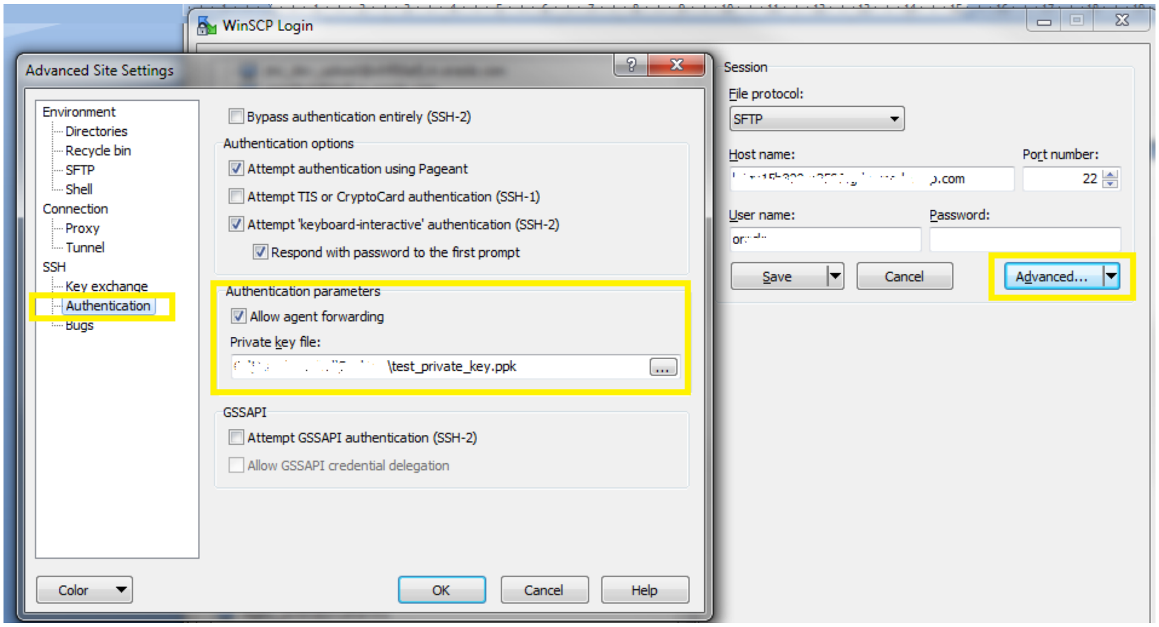
Oracle will take the public key and associate it with the relevant user on the relevant environment, updating the service request when done.

## Logging on with Key Based Authentication

### Windows - WinSCP

There are multiple sftp clients available and you will need to consult the documentation of the sftp client you are using to understand the syntax of how to refer to the private key when connecting.

As an example – using WinSCP, create a new site – entering the hostname and port. Then under Advanced>Authentication set path and filename of the private key as shown in screen shot.



WinSCP Login

Advanced Site Settings [redacted]

- Environment
  - Directories
  - Recycle bin
  - SFTP
  - Shell
- Connection
  - Proxy
  - Tunnel
- SSH
  - Key exchange
  - Authentication
  - Bugs

☐ Bypass authentication entirely (SSH-2)

Authentication options

☑ Attempt authentication using Pageant

☐ Attempt TIS or CryptoCard authentication (SSH-1)

☑ Attempt 'keyboard-interactive' authentication (SSH-2)

☑ Respond with password to the first prompt

Authentication parameters

☑ Allow agent forwarding

Private key file: [redacted]\test_private_key.ppk

GSSAPI

☐ Attempt GSSAPI authentication (SSH-2)

☐ Allow GSSAPI credential delegation

Session

File protocol: SFTP

Host name: [redacted].com

Port number: 22

User name: or[redacted]

Password:

Finally enter the User name – which is the same username you requested the public key to be associated with when sending the public key to Oracle, and leave the password blank.

Click Save, then Login and an authenticated session should be established.

If you put a pass phrase on your local private key, you will be prompted to enter that so that WinSCP can open the private key file.

## References

https://docs.oracle.com/cloud/latest/dbcs_dbaas/CSDBI/GUID-4285B8CF-A228-4B89-9552-FE6446B5A673.htm#CSDBI3349

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

- blogs.oracle.com/oracle
- facebook.com/oracle
- twitter.com/oracle
- oracle.com

Integrated Cloud Applications & Platform Services

sftp Autentication Overview
January 2016
Author: FSGBU