SDI

Setting up SSL connection to
1 - OpenPages
And
2 - GSA

Eddie Hartman – GBS Senior Consultant & SDI/TDI Storyteller

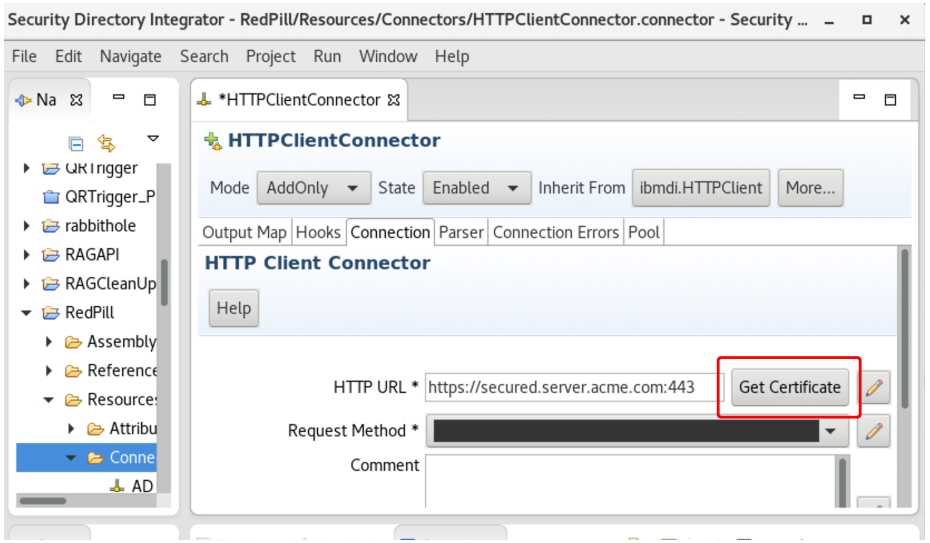
- May 20 2020

1 Setup SSL Connectivity to OpenPages

In order for SDI to make an SSL connection to OpenPages, it must have the necessary certificates in its keystore.

These include the client certificate and any other certs that trust of this one depends on.

Some servers and services provide for easy request of client certificates. With these you can simply set up an HTTP Client Connector in the SDI CE (Config Editor), configure the URL to the server (https://...) and press the **Get Certificate** button.

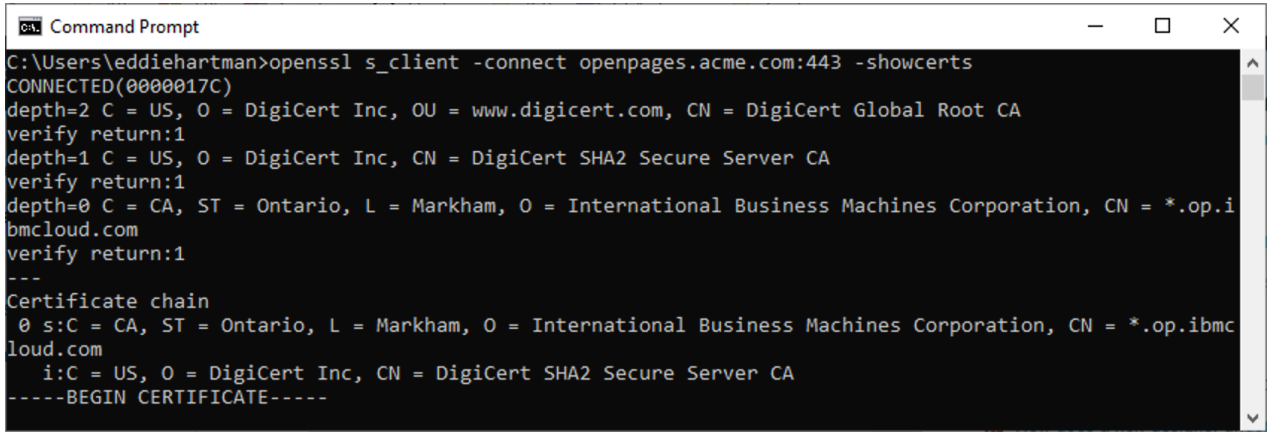


Unfortunately, OpenPages does not respond to this type of request.

1.a Requesting Certificates with openssl

Fortunately the **openssl** commandline utility provides functionality to return certificates from all kinds of services. This tool is available on various Linux distros, as well as on modern Windows 10 installations*.

Simply open a command window and fire up the **openssl** utility with the **–connect** argument followed by the hostname of the server, and including **–showcerts** to display certificates.

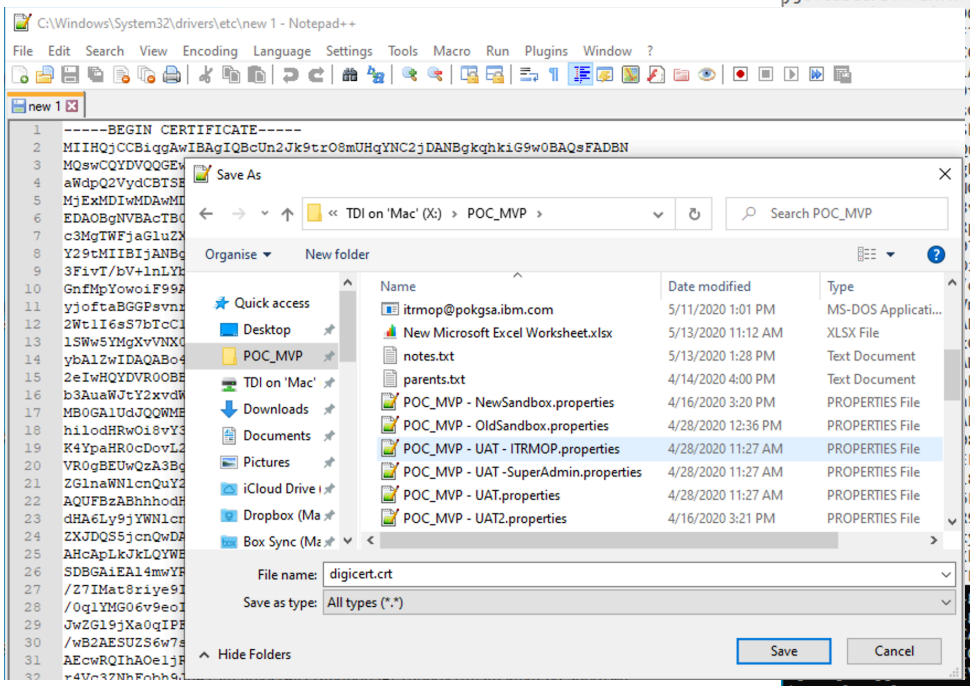


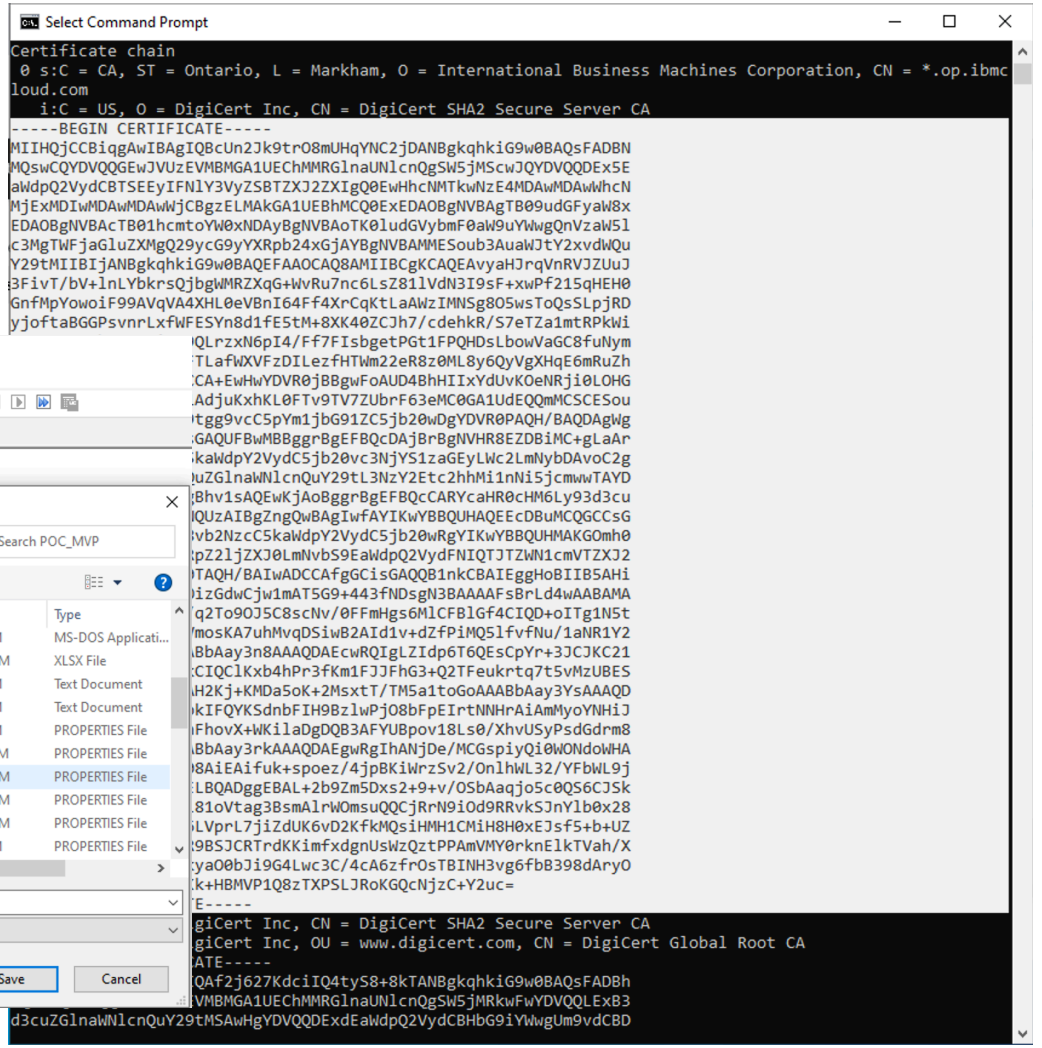
This will result in a lot of output to the terminal window, including all certificates needed for a secure client connection. These will be in order from top-down starting with the client cert, possibly including an intermediate one, and ending with the root cert.

* For earlier versions of Windows, install Git Bash

1.b Saving Certificates to Files

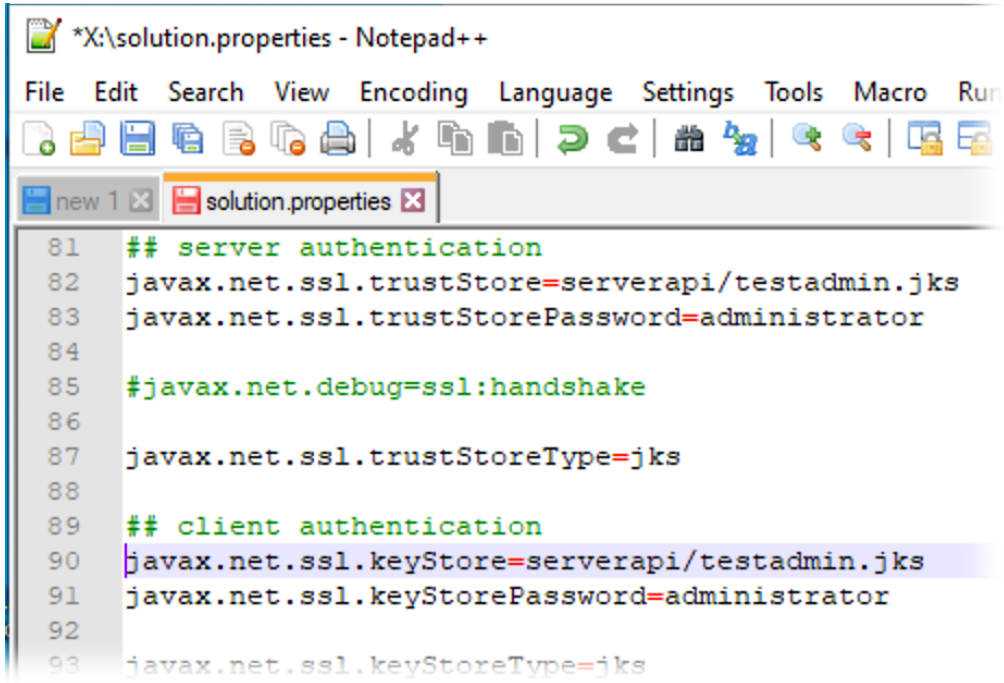
Each certificate must be copied, including the 'BEGIN' and 'END' lines, and saved to files labeled suitably and legibly.





1.c Destination = The SDI Keystore

The SDI Keystore is defined in the **solution.properties** file found in the *Solution Directory* of the SDI installation.

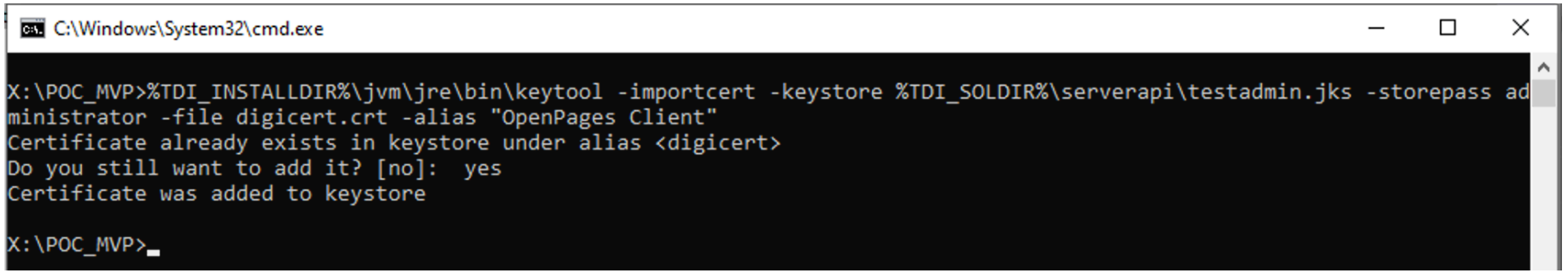


By default this is the *testadmin.jks* file in the *serverapi* sub-folder of the *Solution Directory*, and with the password 'administrator'.

NOTE: To locate your *Solution Directory,* examine the **defaultSolDir** batchfile/script in the *bin* sub-folder of the SDI installation directory (V7.2).

1.d Importing Certificates using keytool

Use the **keytool** utility found in a Java JVM installation to install the certificates. You can use your default Java installation, or the one in the *jvm/jre/bin* sub-folder of your SDI installation.



Execute the **keytool** utility with the following arguments:

-importcert	*command to import certificate*
-keystore	*filepath to the keystore*
-storepass	*password for the keystore*
-file	*certificate file to import*
-alias	*descriptive alias for this cert*

1.e Last Step: Restart SDI

Whenever you make changes to you keystore or truststore – which by default are the same file (testadmin.jks) – you must restart SDI for the changes to take effect.

Once restarted you can test connectivity to ensure an encrypted connection can be established.

2 Enabling Password-less File Transfer To GSA

To enable password-less file transfer using the **scp** utility requires two steps:

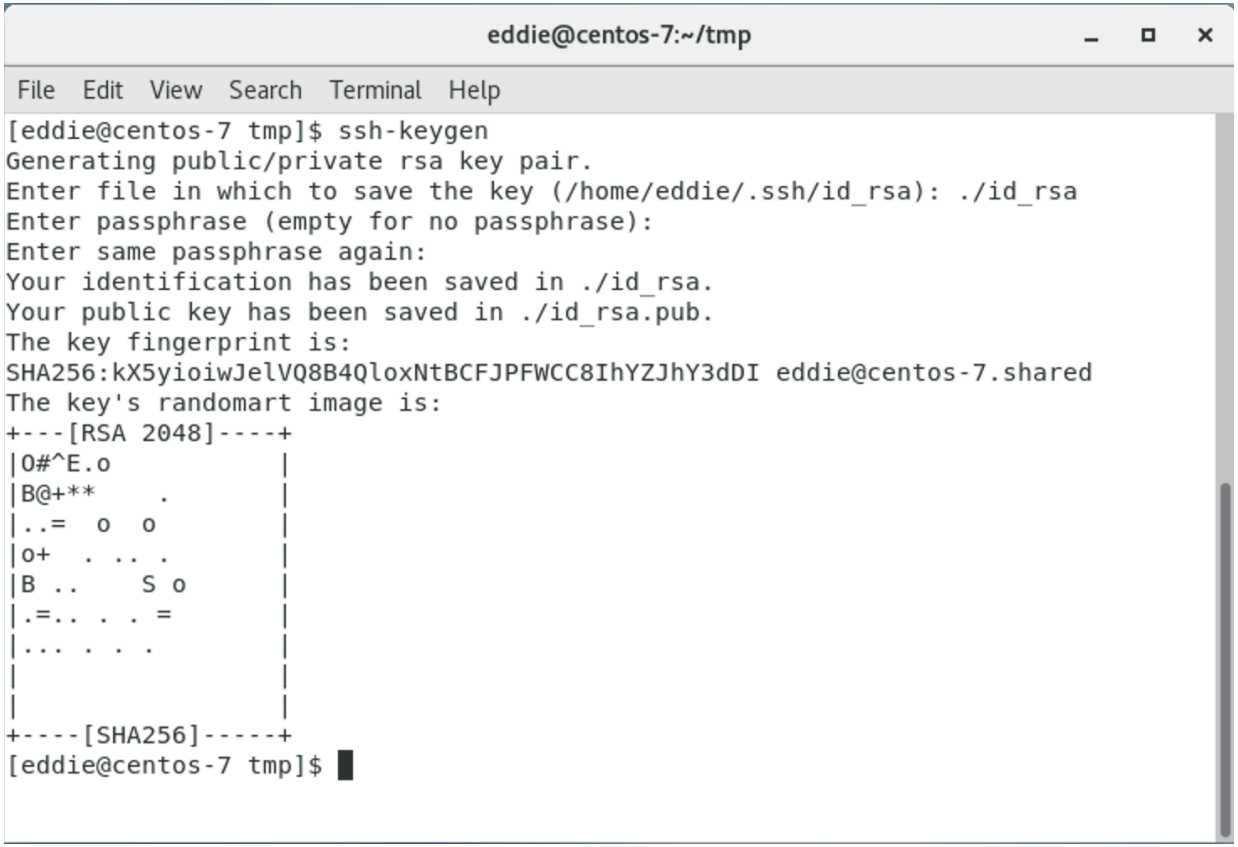
1. The generation of a public/private keypair
   This we do using a utility like **ssh-keygen**

2. Configuring the target GSA account with the public key
   This means updating a file in the *.ssh* sub-folder of the GSA account's home folder and ensuring the *ACLs* of the folder and files are correct.

NOTE: These instructions work for Centos, which is the OS of the servers operated by Cloud Ops. The approach will likely work for other Linux distros as well, since the **scp** utility is available for all. However, achieving password-less file transfer using **winscp** on Windows has eluded me (so far).

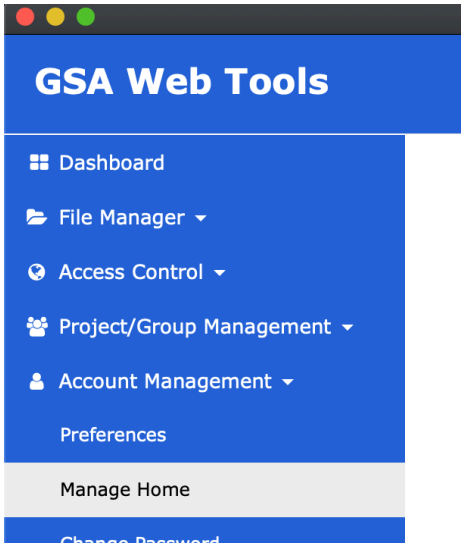
2.a Using ssh-keygen To Generate Keychain

The **ssh-keygen** utility lets you easily create the public/private keypair you need. Simply run the commandline from a terminal. If you do not specify a filepath it will update the keychain of the current user (i.e. ~/.ssh/id_rsa & ~/.ssh/id_rsa.pub).



2.b GSA Account Must Have A Home Folder

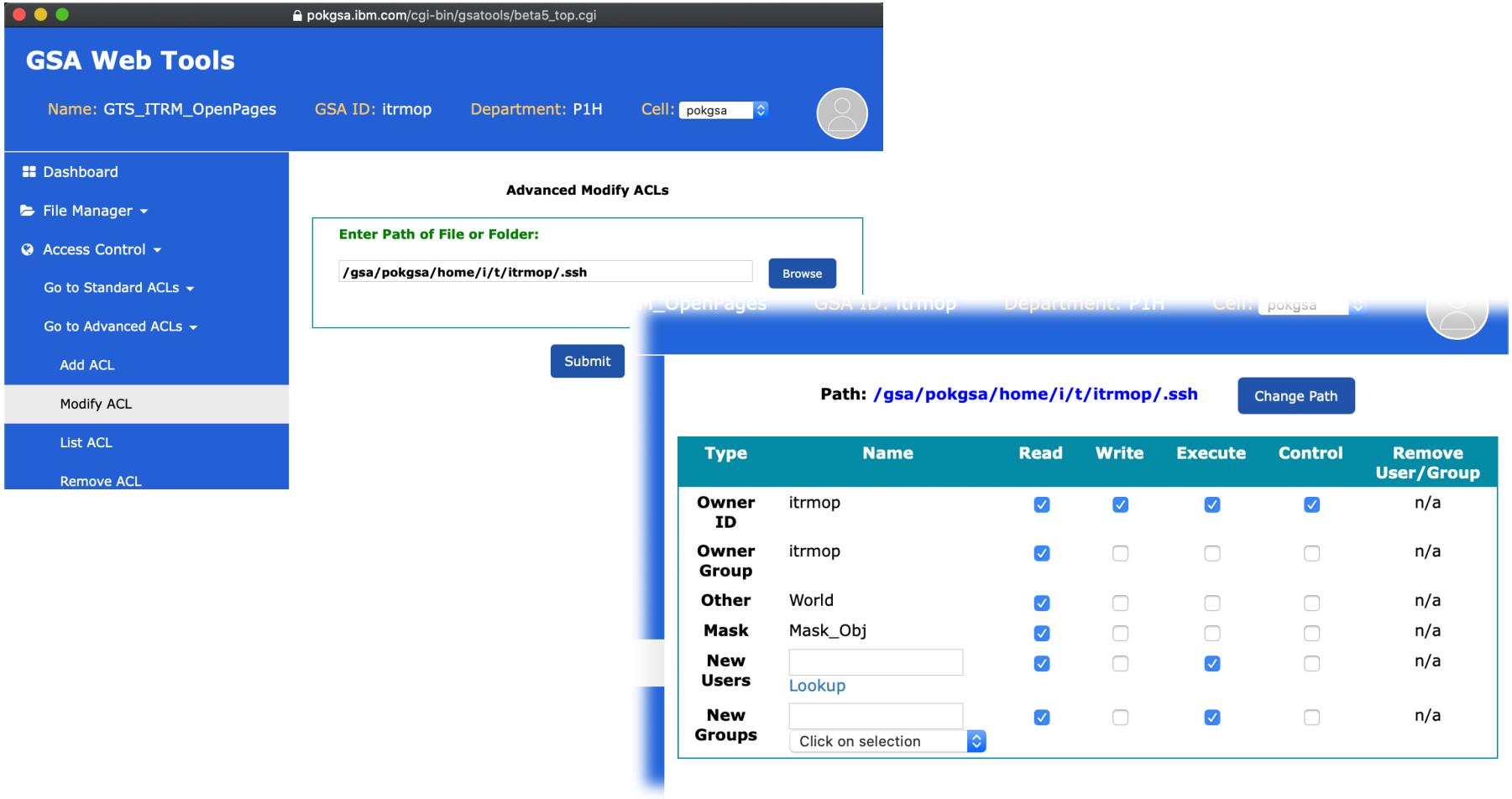
The **id_rsa.pub** file contains the public key. Copy the contents of this file to your copy buffer. It must be appended to the end of a file named **authorized_keys** which is located in the *.ssh* sub-folder of the home directory of the GSA account being used.



For example, if the GSA account is 'itrmop' then you can use the appropriate GSA Web Tools to authenticate and configure the the home directory for your account (for example, this one for POKGSA: https://itrmop@pokgsa.ibm.com/gsadoc/ - the Web Tools link is at the top left).

2.c Home Folder Must Have .ssh Sub-Folder

Once the Home folder is in place then the next step is to ensure it has the *.ssh* sub-folder with the correct ACLs set. You can set these using the GSA Web Tools. Access should be *User*: all, *Group*: R, *World*: R

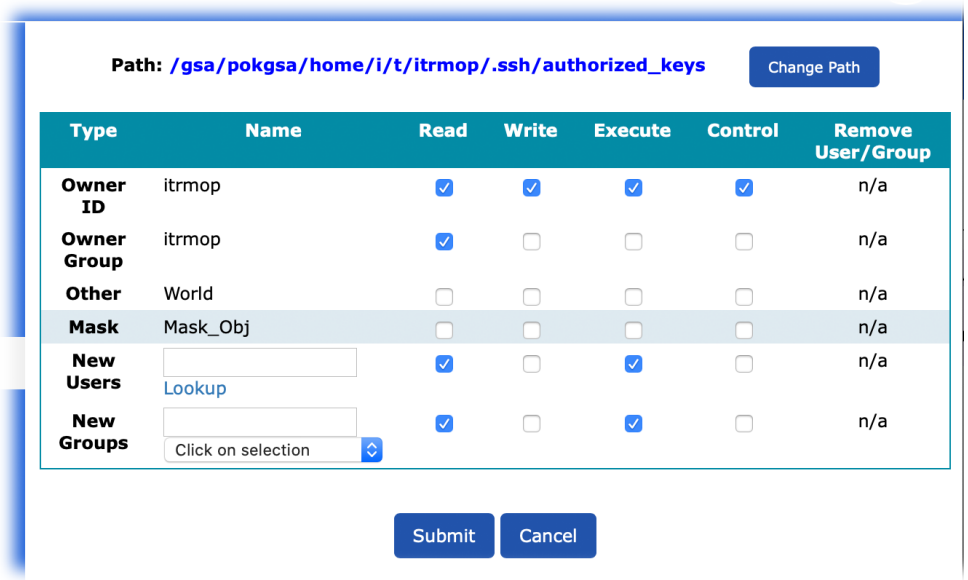


2.d Inside .ssh Must Be The File **authorized_keys**

For a server to accept SSH connections, it must a list of all accepted client keys. This is the **authorized_keys** file found in the *.ssh* sub-folder of the home directory.

Append this file with the contents of the **id_rsa.pub** file created in step **b** above. The single line of test should start with: *ssh-rsa*

Ensure this file has similar ACLs as the *ssh* sub-folder itself, except None for *World*.



2.e Test Password-Less File Transfer

To test if setup is complete, try to transfer a file from your local system to the home folder of the GSA account using the **scp** utility.

```
eddie@centos-7:/media/psf/Home/My_Documents/TDI/POC_MVP
File  Edit  View  Search  Terminal  Help
[eddie@centos-7 POC_MVP]$ scp -i id_rsa test.csv itrmop@pokgsa.ibm.com:/pokgsa-h
3/06/itrmop/
test.csv                                      100%   16     0.1KB/s   00:00
[eddie@centos-7 POC_MVP]$
```

Use the **–i** argument to indicate where the key files are located. The above example is run from a directory containing these key files. Then use a tool like **FileZilla** or **sftp** to list files in that directory and confirm that the file was successfully transferred.

```
eddie@centos-7:/media/psf/Home/My_Documents/TDI/POC_MVP
File  Edit  View  Search  Terminal  Help
[eddie@centos-7 POC_MVP]$ sftp itrmop@pokgsa.ibm.com:/pokgsa-h3/06/itrmop
Connected to pokgsa.ibm.com.
Changing to: /pokgsa-h3/06/itrmop
sftp> ls
test.csv  web
sftp>
```