INSTRUCTIONS

D2A and Extranet are replacing AUSkey with MyGovID and RAM

February 2020

Disclaimer and Copyright

While APRA endeavours to ensure the quality of this publication, it does not accept any responsibility for the accuracy, completeness or currency of the material included in this publication and will not be liable for any loss or damage arising out of any use of, or reliance on, this publication.

© Australian Prudential Regulation Authority (APRA)

This work is licensed under the Creative Commons Attribution 3.0 Australia Licence (CCBY 3.0). This licence allows you to copy, distribute and adapt this work, provided you attribute the work and do not suggest that APRA endorses you or your work. To view a full copy of the terms of this licence, visit https://creativecommons.org/licenses/by/3.0/au/

Contents

Instructions to update D2A to replace AUSkey with myGovID and RAM **4**

Prerequisites – Before you start 4

Steps to update D2A to replace AUSkey with machine credentials **5**

Step 1: Check your D2A client version 5

Step 2: Backup the existing file 6

Step 3: Save the JAR File 7

Step 4: Replace credentials 8

Step 5: Verification of the JAR file replacement 9

Step 6: Verify that the machine credential works 10

In the event of issues 13

Glossary **14**

References and support **15**

References 15

myGovID, RAM & machine credential help 15

D2A and Extranet technical help 15

Instructions to update D2A to replace AUSkey with myGovID and RAM

This document provides the content which can be found on the APRA website at https://www.apra.gov.au/instructions-to-update-d2a-to-replace-auskey-mygovid-and-ram

Prerequisites – Before you start

Users and administrators **must first complete the following steps** using ATO published materials, as a prerequisite to complete the relevant APRA system update (D2A or Extranet).

1. D2A administrators (Principal Authority and Machine Credential Administrator), and Extranet users should set up their digital identity and obtain a myGovID

2. Entities should ensure that their business ABN is linked and administrators are authorised in RAM

3. Entities need to create machine credentials for D2A and store these in a different file to the current D2A credential. Take note of the password you create and where you have saved this file, as you will need to access it later. More information about installing a machine credential can be found here.

Note: Please contact the ATO and/or refer to the ATO website for specific enquires relating to the above steps.

Steps to update D2A to replace AUSkey with machine credentials

Entities will need to repeat these steps for each instance of D2A.

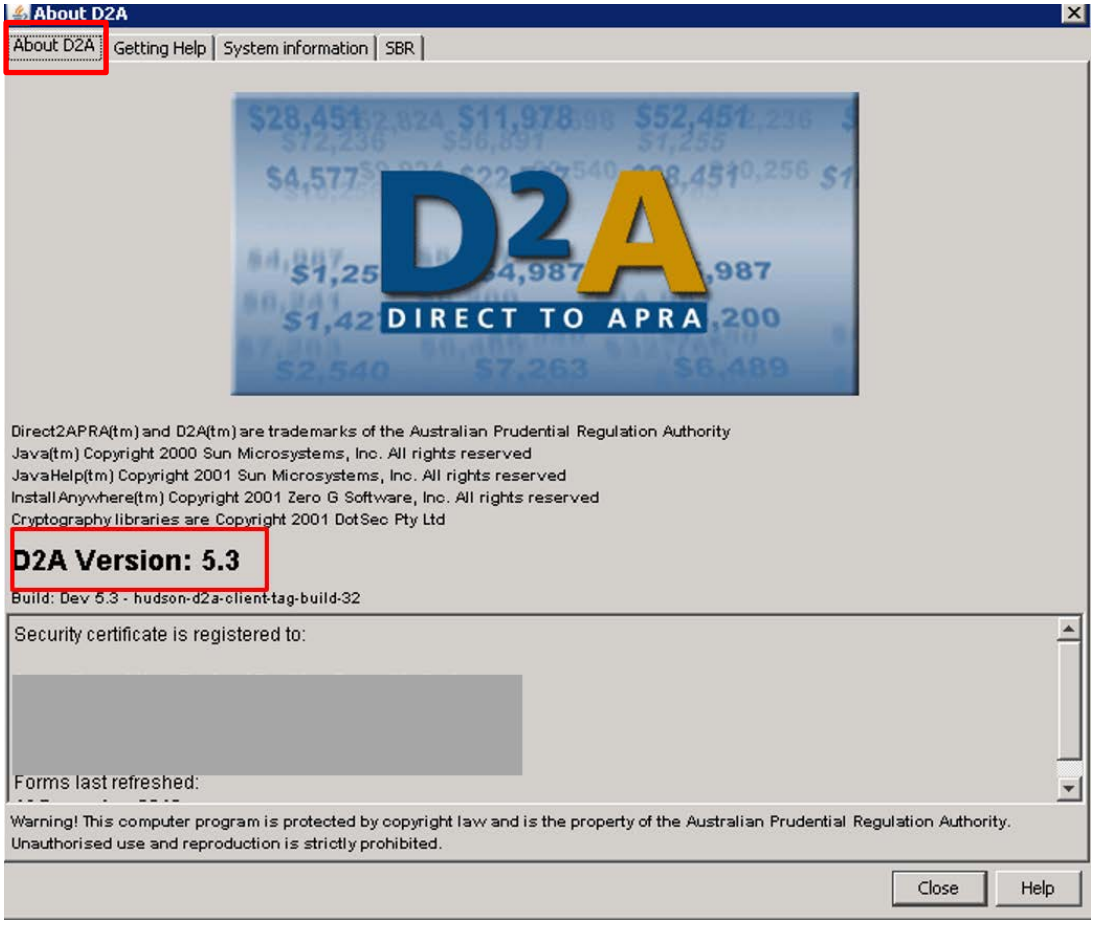
Note: Once an instance of D2A has been transitioned to the new authentication credential that instance will no longer be able to authenticate using AUSkey. If you use this same computer to access the APRA Extranet, you will also need to update the link for the Extranet. Please contact the D2A Help Desk for details.

Step 1: Check your D2A client version

APRA currently supports two versions of D2A (version 5.3 and 5.3.1).

In order to determine which version you are running:

1. Open **D2A client**, and select **Help**
2. Select the **About D2A** tab (refer to screenshot below)
3. Your version number will appear. Make a note of your version number



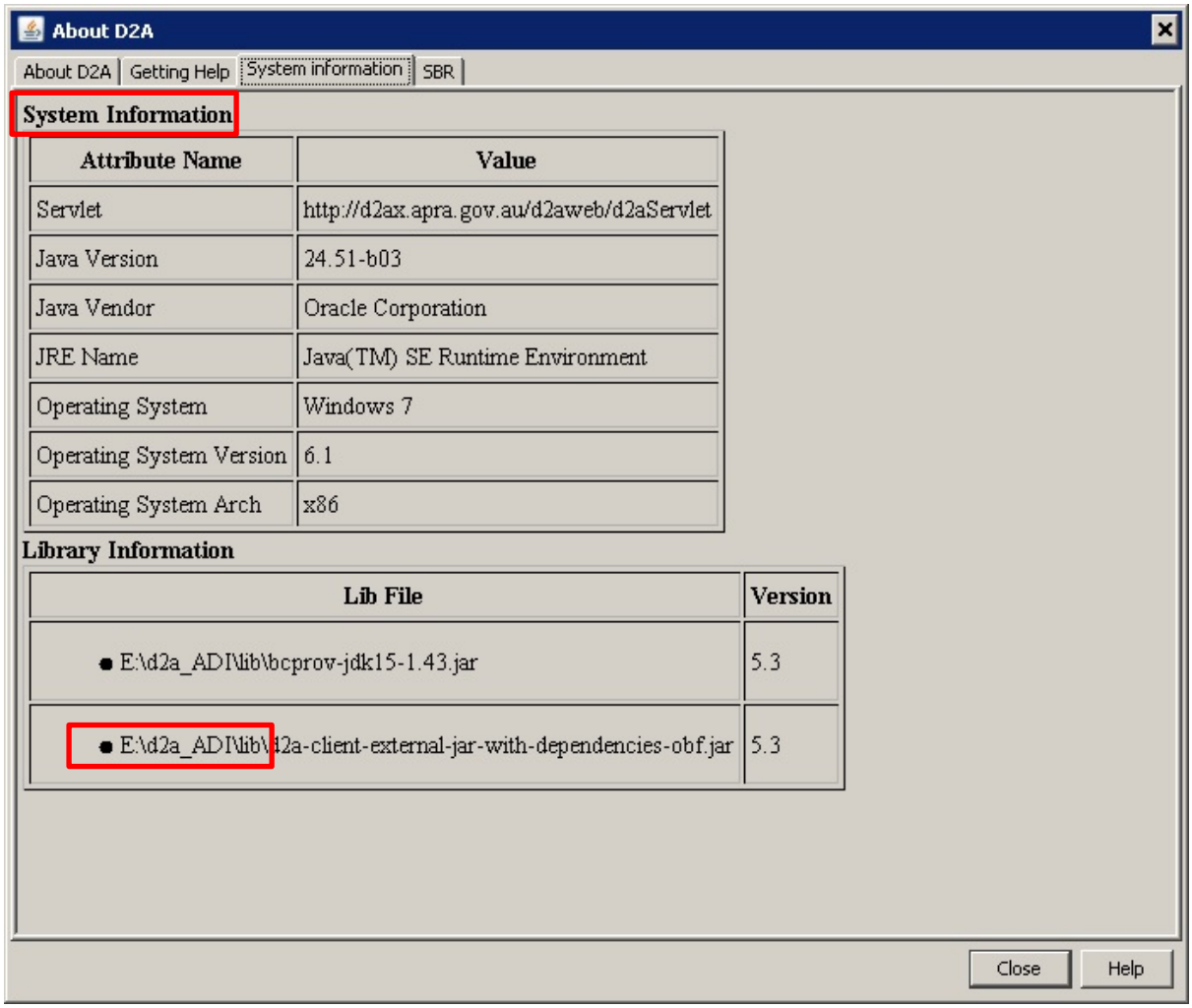
Step 2: Backup the existing file

It is important to back up your existing file, in the event the upgrade process fails. You can do this by accessing your D2A installation folder, which may differ from machine to machine.

To locate your D2A installation folder:

1. Go to the **D2A Client** menu bar and select **Help**

2. Select the **System information** tab



In the screenshot above, the highlighted location is where the D2A client is installed.

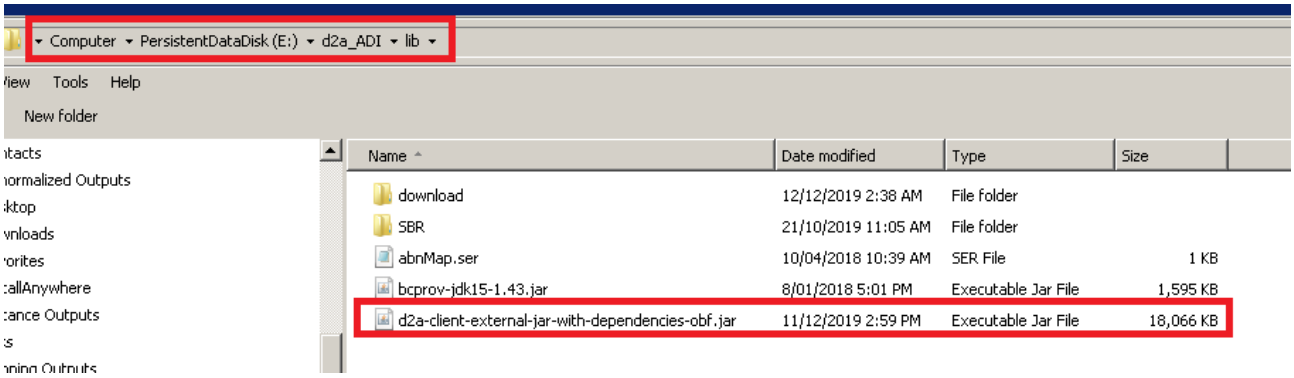
Within this location there will be a folder called **lib**, where you will see a reference to the relevant **.jar file**. For this example, we will refer to this folder location **E:\d2a_ADI**

3. **Close** your D2A client

To back up the JAR file :

4. Use **File Explorer**, and go to the folder location identified in Step 2.2 (i.e.: E:\d2a_ADI\lib)

5. Find the file called **d2a-client-external-jar-with-dependencies-obf.jar** (illustrated in the screenshot below)



6. **Rename this file** (e.g. add " _AUSkey" to the existing file name so that it becomes **d2a-client-external-jar-with-dependencies-obf_AUSkey.jar**) and keep this copy in this location

7. **Close** your file explorer

Step 3: Save the JAR File

To update the D2A client to use the new machine credential, you will need to download and save the JAR file in the location identified above.

1. **Download the relevant JAR file for your version of D2A** identified in Step 1 above
   JAR file for D2A version 5.3 ZIP 15.81 MB

   JAR file for D2A version 5.3.1 ZIP 19.61 MB

2. You will need **to extract the JAR file from the zip file**

3. **Save the JAR file to the same folder** as the screenshot above

Step 4: Replace credentials

To replace the AUSkey credential with the new machine credential, you will need to access your Roaming folder. This should be the default folder where your AUSkey was installed.

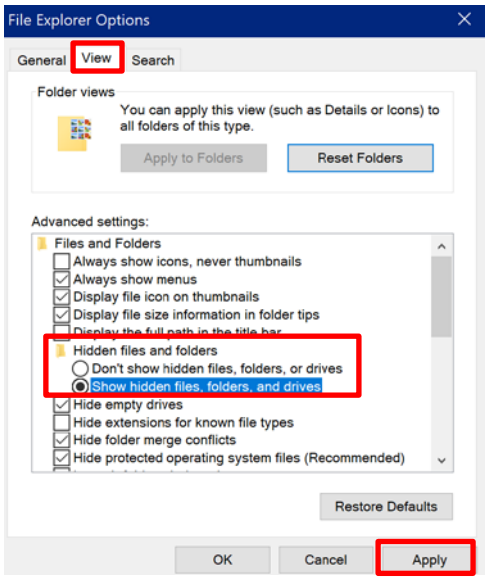
To locate your Roaming folder and the file which needs to be replaced:

1. Ensure D2A client is closed

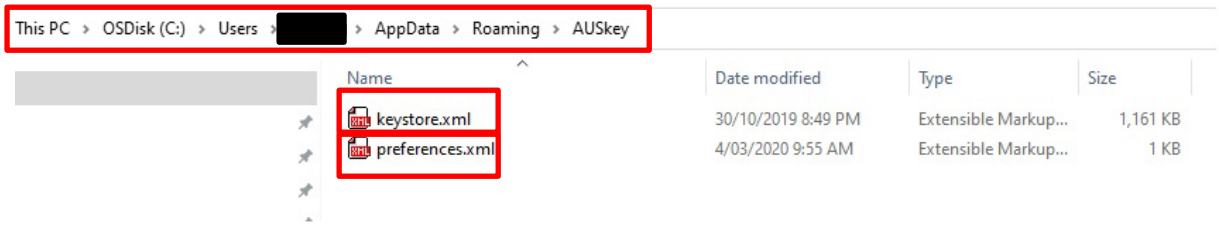
2. Use **File explorer** and in the quick access bar, type the following file location (ensure that you replace the yellow highlighted text with your corporate userID)

   C:\Users\<<enter your userID>>\AppData\Roaming\AUSkey

Note: The AppData folder may be hidden for some entities. To unhide and view the AppData folder; within **File Explorer Options**, go to **View** tab, select "Show hidden files, folders, and drives" and click **Apply** (as illustrated in the screenshot below).



3. **Locate the keystore.xml file**, which will appear in your Roaming folder (refer to screenshot below)



Note: If your AUSkey was not installed in the default location, you will need to search for it and/or speak to your IT department.

To create a backup of the old file:

4. **Rename the file** (e.g. add " _AUSkey" to the existing file name so that it becomes **keystore_AUSkey.xml**) and keep this copy in this location

To save the new machine credential:

5. **Locate** the new machine credential that was created in RAM (you would have completed this as part of your prerequisite)

6. **Save** as **keystore.xml** in your Roaming folder (e.g.: C:\Users**<<enter your userID>>**\AppData\Roaming\AUSkey)

Note: There should only be two files within the Roaming folder, the keystore.xml and the keystore_AUSkey.xml file. Some users may find that within the Roaming folder there is another file called preferences.xml (as illustrated in the screenshot above). If this file exists, you will need to save a backup of this file to another location and delete it from the Roaming folder.

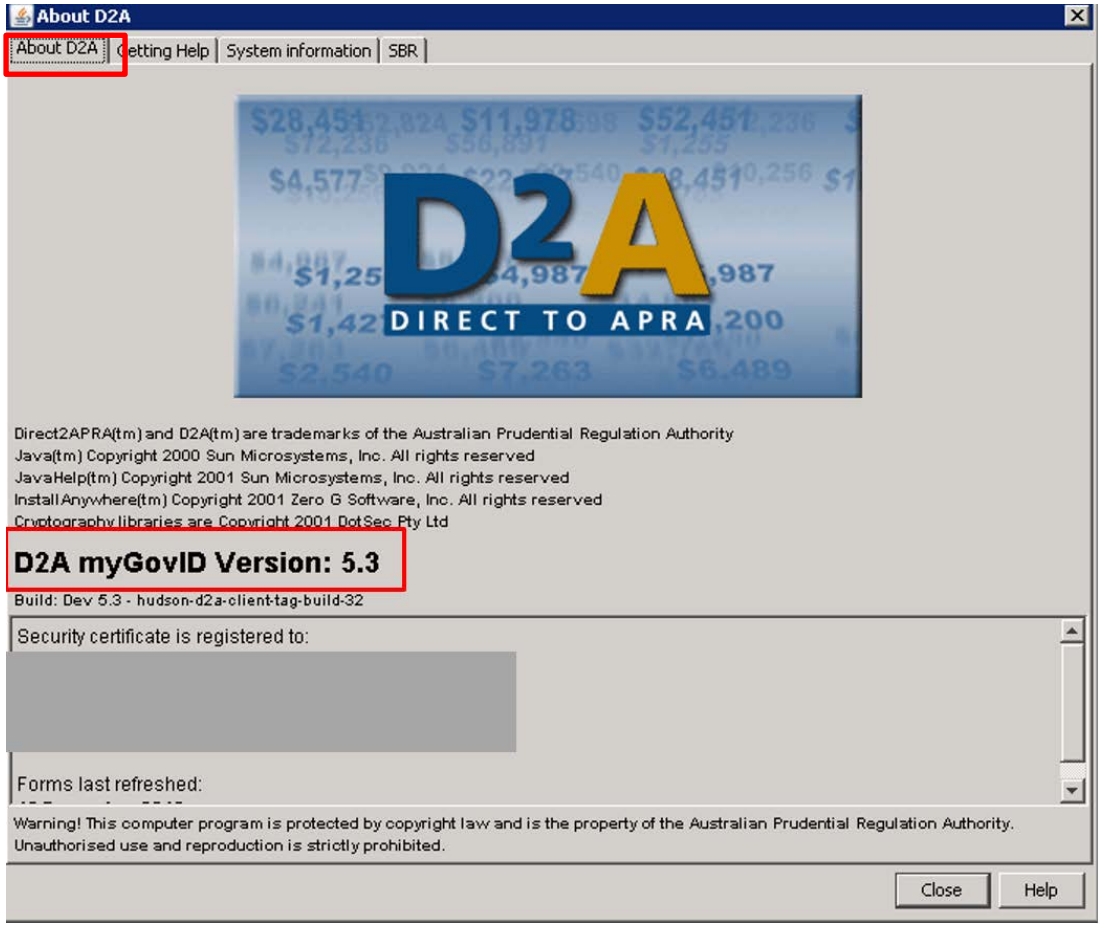
Step 5: Verification of the JAR file replacement

In order to verify that you have successfully replaced the JAR file:

1. Open **D2A** on your machine and select **Help**

2. Select the **About D2A** tab (refer to screenshot below)

3. You should see a "D2A myGovID Version XX". This confirms that you have successfully replaced the JAR file



Note: If D2A fails to open, this indicates that you have not successfully replaced the JAR file. Check that you have completed all the above steps successfully. You may need to refer to the steps outlined in the section below "In the event of issues" to reverse any changes made.

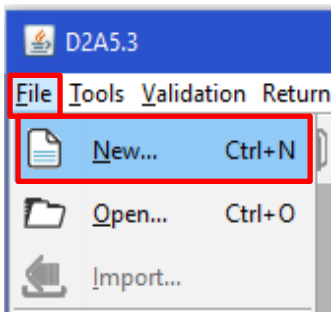
Step 6: Verify that the machine credential works

In order to verify that the machine credential works, you are required to complete and submit a new D2A form CONFIRM: D2A update for myGovID completed.

Note: This submission is for verification purposes only. APRA is not recording or reporting on the data submitted. The return will show as due 29 February 2020, however you will not receive late notices and the return will be available during February and March.

1. Open D2A and select Tools from the top menu

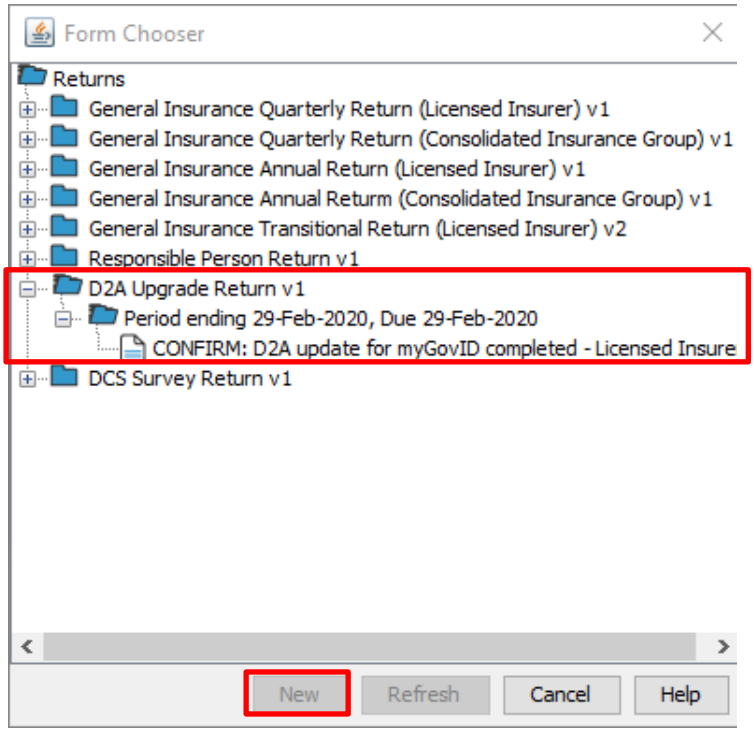
2. Select File and then New menu option



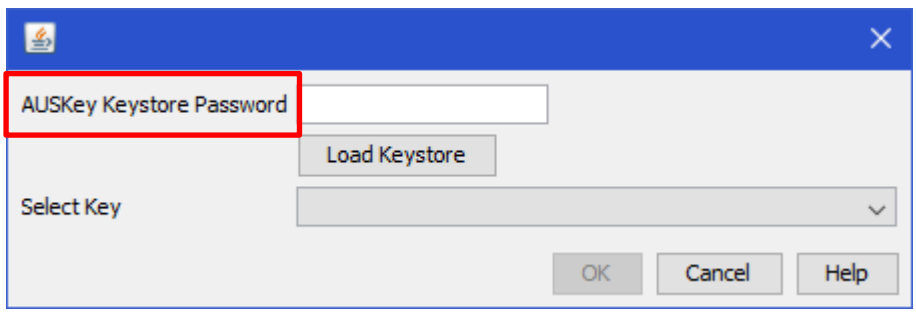
This will open the Form Chooser:

3. Select the **D2A Upgrade Return v1** folder, choose **Period ending 29-Feb-2020** and select the **CONFIRM: D2A update for myGovID** completed form

4. Press the **New** button (as shown in the screenshot below):



You will be prompted to enter a password (as shown in screenshot below)

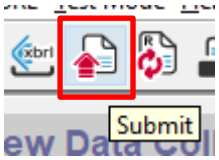


Note: D2A will still refer to "AUSkey" on the screen and commands (as shown in the screenshot above) even once successfully updated.

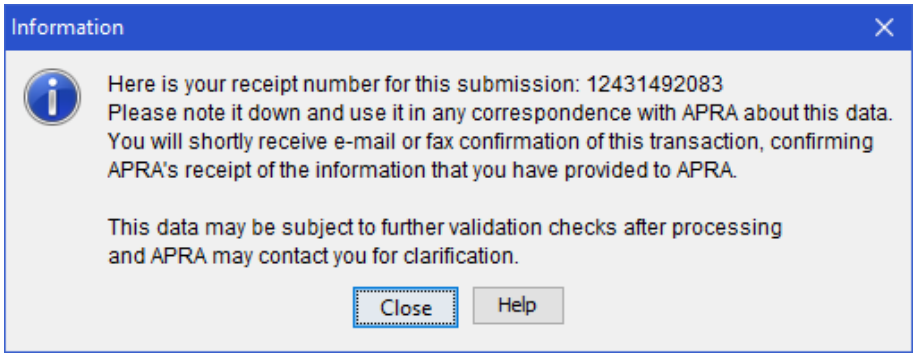
5. Enter the **password** that you created for the new machine credential, and click **Load Keystore**

6. Click on the **Select Key** drop down menu and choose a key from the available list, then click **OK**

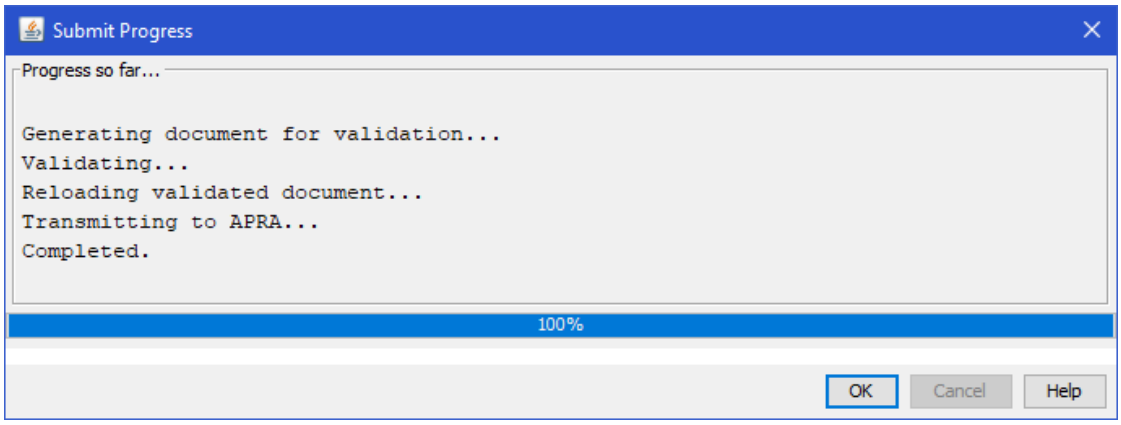
7. This will open the confirmation form. Complete the return by answering the question and then **Submit** the form to APRA, as shown below:



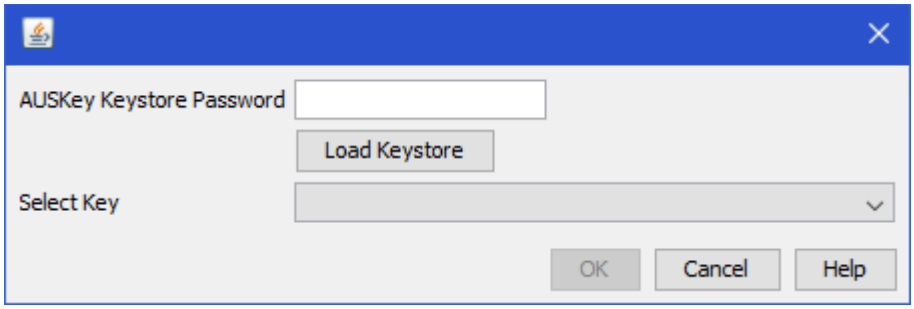
8. You will get an onscreen confirmation (like the one shown below) that confirms that the submission was successful.



Behind that confirmation, D2A will also show details of the submission process:



If you receive these confirmations you have successfully used the new machine credential to submit data to APRA. APRA will have a record that the new machine credential has been used for that installation of D2A.



Note: If Keystore fails to load and hangs on the following screen (refer to above screenshot), this indicates that you have not successfully saved the new machine credential. Check that you have completed all the above steps successfully. You may need to refer to the steps outlined in the section below "In the event of issues" to reverse any changes made.

In the event of issues

If you experience issues, (D2A may not launch or Keystore does not load) you will need to first close your D2A client, then reverse Steps 2 and 4 to restore the original files and delete any new files you have added.

Glossary

AUSkey	AUSkey is a secure login that identifies you when you use participating government online services on behalf of a business. AUSkey and Manage ABN Connections will be decommissioned in March 2020
D2A Client	Software used by entities to submit their data to APRA
Instance of D2A	A machine that has the D2A Client software installed on it
JAR file	JAR files are archive files that include a java-specific manifest file
M2M	The Machine to Machine (M2M) solution supports users getting a machine credential to enable them to use software to interact directly with government services. The M2M solution includes a machine credential to replace device AUSkey.
Machine credential	Replacement for device AUSkey
MyGovID	The Australian Government's digital identity provider that allows you to prove who you are when using government online services
Relationship Authorisation Manager (RAM)	A whole of government relationship and authorisation manager. RAM lets you control who can act on behalf of your business across eligible government services.

References and support

References

1. myGovID and Relationship Authorisation Manager (RAM)
2. Machine credentials
3. AUSkey

myGovID, RAM & machine credential help

The D2A Help Desk cannot assist with specific enquires relating to myGovID. Please refer to the ATO website for technical support.

D2A and Extranet technical help

If this document does not assist with your enquiry or you are experiencing technical difficulties with the D2A application, please contact the D2A Help Desk on 02 9210 3400 between 9am and 5pm (Eastern Standard Time) Monday to Friday, or email support@apra.gov.au.

APRA