

Provider Registration and International Student Management System (PRISMS)

PRISMS Get Started User Guide for Relationship Authorisation Manager

This guide shows how Principal Authorities and Authorisation Administrators can use the Australian Government’s Relationship Authorisation Manager (RAM) to authorise others to act online on behalf of a business. This guide should be used along with the RAM website: [Get started | Relationship Authorisation Manager](https://info.authorisationmanager.gov.au/get-started). It also outlines the steps to obtain a public and private certificate using OpenSSL and how to install a machine credential.

# Installing a machine credential

|  |  |
| --- | --- |
| **1** | **Requirements to install a machine credential** |
| 1.1 | 1. Ensure you have a digital identity such as [Home | myGovID](https://www.mygovid.gov.au/) 2. A compatible internet browser (i.e. Google Chrome version 39+, Mozilla Firefox version 30+, Apple Safari version 5+) |
| 1.2 | 1. Link your myGovID to the business’s Australian business number (ABN) in RAM, starting with the **Principal Authority**, then others can be authorised to act on behalf of the business, such as Authorised User & Administrator and Business Software User or Provider. 2. [Login | myGovID](https://mygovid.gov.au/AuthSpa.UI/index.html#login) (Select Link my Business and continue steps as per [Principal authority | Relationship Authorisation Manager](https://info.authorisationmanager.gov.au/principal-authority). |
| 1.3 | 1. To start using government online services on behalf of a business, **a principal authority or authorisation administrator needs to authorise you** to act on behalf of a business. 2. You will receive an email with an authorisation request to become an Authorised administrator, Authorised user, Machine credential administrator or Basic user with Full access, Custom access or No access. |
| 1.4 | 1. If you use Standard Business Reporting-enabled software or if you are a digital service provider, **you can use Relationship Authorisation Manager to create machine credentials** and notify the Office of the Student Identifiers Registrar, Department of Education about the software you’ll be using to interact with them through My Cloud software services. [Business software user or provider | Relationship Authorisation Manager](https://info.authorisationmanager.gov.au/business-software-user-or-provider) (Please follow link details) |
| **2** | **How to install a machine credential** |
| 2.1 | 1. Using Chrome or Firefox, go to <http://info.authorisationmanager.gov.au/>. 2. Click the Login with myGovID button or the Login button in the top right-hand corner. |
| 2.2 | 1. Enter the email address you used to set up your myGovID. 2. A code will appear on your smart device, enter the 4-digit code and click **Accept**. 3. If you have selected the ‘Remember me’ option, you will only need to click **Accept** in your app.   Screenshot showing an example 4 digit code generated by the myGovID website. |
| 2.3 | 1. Click **View or manage authorisations, machine credentials and cloud software** notifications. You will be directed to a view of all the entities you can act for. 2. Select the entity you would like to create a machine credential for.   Screen showing an example of where you can select the entities you can act on behalf of. |
| 2.4 | 1. The entity homepage will be displayed with a list of all the authorisations for the entity. 2. Click the **Manage Credentials** tab in the toolbar.   Screen showing a list of all authorisations for the entity. |
| 2.5 | 1. The Manage Credentials page is displayed.   Screen showing the notification that software is required.   1. If you have already installed the required browser extension, go to the next step. 2. If you have not yet installed the required browser extension, you'll receive a message that browser extension software is required. 3. Click **Machine credential downloads** or see the [Installing a browser extension](https://info.authorisationmanager.gov.au/guide-how-to-install-a-machine-credential#Installingabrowserextension) section. 4. Select, install and enable the browser extension link for your operating system. 5. Close your browser, then reopen it and follow Steps 1-6. |
| 2.6 | 1. Select **Create machine credential**   Screen of Create a machine credential page with create a machine credential button in the top right hand corner. |
| 2.7 | 1. Enter the following information:  * **Keystore path** – this is where the machine credential will be created and stored, the information will be pre-filled but can be changed if required. * **Keystore password** – choose a password that is at least 10 characters (with no space) including an upper-case letter, a lower-case letter, a number and a special character. You’ll provide this password within your software either when setting up or authenticating. You should not use your myGovID password for the ‘Keystore password’. * **Verify** **your keystore password** – re-enter your chosen password. * **Credential name** – create a name that will help you to easily identify the machine credential. If you’re creating a new machine credential to prevent expiry of an existing one, use the **same** credential name. * **Identify the machine credential custodian** – this will be pre-filled with your name and cannot be changed.  1. If you’re creating a new machine credential to prevent expiry of an existing one, a message will display confirming the new credential will share the same permissions. You’ll need to [revoke](https://info.authorisationmanager.gov.au/business-software-user-or-provider#How%20to%20revoke%20a%20machine%20credential) the existing machine credential if it hasn’t expired yet. 2. When creating a machine credential, you can store it in:  * an existing keystore by using the initial keystore path and password * a new keystore by changing the keystore path and password * a new keystore each time you create one - you will need to change the keystore path each time you create a new machine credential to do this.   The machine credential keystore is generated in Extensible Markup Language (XML).   1. If your software requires the keystore to be stored in an alternative format, you’ll need to follow the guidance provided by your digital service provider to convert and install the keystore. 2. Tick the box to confirm you understand and accept the machine credential details. 3. Click **Download**.   Screen showing fields for the Keystore path, Keystore password and Credential name. |
| 2.8 | 1. Once downloaded you will receive a message confirming that the machine credential has been installed.   Screen showing the message that a machine credential has been installed successfully. |
| 2.9 | 1. From the **Manage Credentials** page you can create, edit, revoke and claim unassigned machine credentials for the entity.   Screen showing the newly created machine credential listed on the Create a machine credential page. |
| 3.0 | Continue onto the next section: Generate public x509 certificate from RAM Machine Credential |
|  |  |

# Generate public x509 certificate from RAM Machine Credential

The following information describes how to extract the public certificate and private key using OpenSSL from your M2M credential keystore. This is used as an example. Other software or methods can be used to extract the public certificate and private key.

|  |  |
| --- | --- |
| **1** | **Extracting the Public certificate** |
| 1.1 | 1. Download and install OpenSSL <https://slproweb.com/products/Win32OpenSSL.html>.   A screenshot of a computer  Description automatically generated   1. Open the keystore xxxx.xml in a text editor. 2. Copy the public x.509 certificate and convert into xxx.cer by:  * copying **<publicCertificate>** base 64 encoded content into a new text editor * adding a line -----BEGIN CERTIFICATE----- to the top * adding a line -----END CERTIFICATE----- to the end * saving the file as xxx.p7b * opening the command prompt and \*cd to the directory * running the command: openssl pkcs7 -print\_certs -in xxx.p7b -out xxx.cer * opening the xxx.cer file using a text editor to view the public x.509 certificate (the first certificate in the list). |
| **2** | **Extracting the private key** |
| 2..1 | 1. Copy the private key into an encrypted PKCS8 file xxx.key by    * copying the **<protectedPrivateKey>** base 64 encoded content into a text editor    * adding the line -----BEGIN ENCRYPTED PRIVATE KEY----- to the top    * adding the line -----END ENCRYPTED PRIVATE KEY----- to the end    * saving the file as xxx.key. |
| 2.2 | 1. Convert xxx.cer and xxx.key into PKCS12 by    * opening the command prompt and \*cd to the directory    * running the command openssl pkcs12 -export -in xxx.cer -inkey xxx.key -out xxx.p12 -passin pass:<password> -passout pass:<password>. |
| 2.3 | 1. Extract the private key from the PPKCS12 file xxx.p12 by    * running the command openssl pkcs12 -info -in xxx.p12 -nodes -nocerts    * entering the keystore password    * viewing the private key, which will be shown between 'begin private key' and 'end private key'. |