FREQUENTLY ASKED QUESTIONS

Using the Machine Credentials for D2A - Entity

March 2020

Disclaimer and Copyright

These FAQs are not legal advice and users are encouraged to obtain professional advice about the application of any legislation or terms relevant to their particular circumstances and to exercise their own skill and care in relation to any material contained in these FAQs. APRA recommends users visit the ATO website for further information on machine credentials.

APRA disclaims any liability for any loss or damage arising out of any reliance or use of the information in these FAQs.

1. What is a machine credential?

A machine credential is essentially a cryptographic asymmetric key-pair – a private key and a public key - that can be used for authentication purposes, to digitally sign and verify documents and to encrypt communications. They are issued by the ATO who are an accredited Certificate Authority within the Australian Government's Public Key Infrastructure program called Gatekeeper.

They replace AUSkeys, specifically, the device Auskey, but they are also similar to the User AUSkeys that D2A used previously, but provide a higher level of security. They are also easier to create.

Although they are termed 'machine' credential, and are often used to authenticate a device – a machine or an application - they are quite flexible and can be used in a variety of ways.

APRA uses them to authenticate each instance of the Direct to APRA (D2A) client application, but because the D2A client can only be 'operated' by a person, and not autonomously (by a machine), we also recommend that each credential is given a name – an identifier - which can be linked to the person who is 'operating' the client. It is a 'hybrid' authentication method, where the user submitting data, the machine and the application can be authenticated simultaneously.

The credentials themselves are held in a "keystore", an XML file with an ATO proprietary format that is protected by a password.

They are often referred to as certificates, although a certificate is more accurately described as the public part of a credential – the public key plus a 'trust chain' that is used to 'guarantee' the authenticity of the public key.

Refer to ATO website here for further information on machine credentials.

See DTA website here for information on Gatekeeper

2. How are machine credentials used with D2A?

D2A uses the machine credential for authentication and to encrypt and digitally sign the data sent to APRA in exactly the same way User Auskeys were used previously. They are also stored in a credential file (aka keystore) which has the same name as the keystore used by D2A for AUSkeys.

Note that that the keystore is actually installed in a D2A user's roaming folder, and so it is not 'tied' to a specific machine. It is tied more to the D2A client (by virtue of the ABN value) and the user of the D2A client. It is the user who provides the credential to the D2A client (by knowing the password of the keystore). So the keystore would 'accompany' a user if they signed into another machine or virtual device that hosted a D2A client.

See APRA website for further details

3. How do I create a machine credential?

Only Machine Credential Administrators (MCA) or Principal Authorities can create machine credentials.

The conditions and the processes necessary to create the credentials are described on the ATO website and the Terms of use.

Currently, only Firefox and Chrome browsers are compatible with the browser extension that is used to create the machine credential.

4. Who should be an MCA?

An MCA needs to be a myGovID standard user (Identity proofing level of IDP2) and should be a trusted member of your organisation who is familiar with the Australian Government's recommended security principles and practices.

An MCA is authorised to create and administer credentials by an authorised representative of the business that has a reporting obligation to APRA. The authorised representative can be the Principal Authority of that business or their authorised delegate.

If your organisation administers regulatory returns on behalf of other reporting entities, and a machine credential is needed for the reporting entity, the MCA can create the credential using the ATOs Relationship Authorisation Manager (RAM).

The MCA and their organisation have certain responsibilities with regard to machine credentials so they should be familiar with the terms of use of myGovID Machine Credentials and usage policies surrounding them.

See MyGovid Terms of use - Machine.

5. How many machine credentials can an MCA create?

There is no limit. It depends on how many entities your company submits D2A data on behalf of and how many people are involved in that process.

Remember the MCA is the custodian of any machine credential they create and is responsible for the management of those credentials (including revoking them) so they should minimise the number of credentials they create and provide them only to the users of D2A who need them for their role. In other words they control the distribution and should follow recommended security practices with regard to cryptographic materials.

6. How many machine credentials does my organisation need?

It depends on how many businesses your organisation submits D2A data on behalf of, how many people normally take part in that process and, to a lesser extent the number of machines used to submit D2A data.

Our operational statistics show that over 50% of our regulated entities have two or more people using AUSkeys and 65% have two or more machines used to submit D2A data.

A significant proportion (16%) have five or more AUSkeys, and of all the user AUSkeys in operation about 40% are used on more than one machine.

7. How many keystores should a MCA create?

There is no limit but it is generally good security practice to limit the distribution of credentials and keystores and to control access to those keystores.

Some organisations find that grouping together all the credentials a particular person uses in one keystore is an efficient way of managing their distribution, with the name of each credential linked to, or associated with, that individual. That way if a user of a credential leaves the organisation, or no longer has responsibility to submit data, the credential can be identified and revoked easily. Because there can be many credentials and keystores it is also a good idea to store the passwords for the keystores in a password manager or vault.

8. Can the machine credentials created for D2A be used for other purposes?

Yes, as long as they are used only for other government services and according to the terms of use and policy documents.

See myGovID Terms of use - Machine *and* ATO PKI Policies

9. Do I need a myGovID to use a machine credential with D2A?

No. The credential and keystore is provided by the MCA (who does need a myGovID) and it is their responsibility that the files are issued only to the nominated users of D2A.

The "Manage Credential" page in RAM records the ABN, the names of the credentials, and the MCA who issued them but does not record to whom the credentials have been issued. That is the responsibility of the MCA.

The use of the credentials is recorded by D2A, which ensures that only current, valid and active credentials issued by the myGovID system can be used for D2A submissions.

10. Can I share machine credentials or keystores with other people?

The ATO's terms of use are quite clear on this. It is poor security practice and not recommended. However because the MCA generates the credentials and provides them to D2A users in a keystore that is protected by a single password it is inevitable that passwords are shared. So the MCA's organisation and the MCA should have secure and robust standards and practices in place to ensure that the credentials and keystores are not used

inappropriately.

11. My company has many people who have AUSkeys they have used for D2A and Extranet – should we replace all of them with machine credentials?

Not necessarily. Extranet does not use machine credentials. And only those individuals who use D2A need a credential.

12. My company has many instances of D2A on many machines – should we create a single keystore for all of them?

Sharing files amongst a group of people or machines it is not a good idea. It may seem to involve less administration by the MCA, but it is not a good security practice because it would mean that credentials/passwords are shared with a large number of people (see policy restrictions on ATO sites referred to above).

13. Can an MCA create machine credentials for multiple entities?

Yes they can. Assuming the MCA has been authorised to do so by an authorised administrator or the principal authority of the reporting entity.

14. Should the MCA give the same password to all keystores?

No. Although possible, it may violate the principle of least privilege which requires access only to information necessary for a particular role. It is poor security practice.

15. Should the MCA put each credential in a separate keystore?

This is up to the individual business, based on their own requirements

For organisations with a large number of people and/or machines involved with D2A submissions a password manager or vault might offer a more robust and secure solution since a MCA has to record who they distribute credentials to. This is the recommended approach by the Australian Government Information Systems Manual for password storage.

Additional information such as credential name, installed machine, D2A client instance, issued to, date, serial number etc. would also provide further control and audit capability.

The MCA can obtain this information from the keystore by using a browser to view the contents.

16. How do I change the password on the keystore?

You can't. Once the keystore is created the password is fixed.

17. What happens if I forget or loose the password of the keystore?

You can't use that keystore again unless the password can be recovered.

18. How do I revoke a credential?

Normally the MCA would revoke a credential. The option is provided on the "Manage Credentials" page in RAM.

See 4.9 Certificate Revocation and Suspension in the CPS.

19. When should the MCA revoke a credential?

If they think that the credential's integrity or security has been compromised, or may be in the future. For instance, if a D2A user leaves the organisation or changes role.

For more examples see 4.9 Certificate Revocation and Suspension in the CPS.

20. How can I replace a credential?

You can replace a credential with one of the same name in a keystore using the "Create Credential" function in RAM. The new credential will have the same name but a different private key, public certificate, serial number and validity dates.

If it has been revoked, it cannot be replaced or renewed.

21. What name should I give the credential?

The name should be unique and meaningful. Although the ATO web pages and Certificate Policy (CP) suggest only a machine name or IP address, it is sensible to include the name or identifier or some reference to the actual user of the credential so if the credential needs to be revoked, it is easily identified on the "Credentials Management" page in RAM.

The credential name is character string - freeform text, containing upper and lower case alphabetic, numeric and special characters '-.:"

22. What name should I give the keystore file(s)?

When a keystore is installed in the user's roaming folder it must conform to the D2A standard *C:\Users\<<userID>>\AppData\Roaming\AUSkey\keystore.xml*[1]

The keystore is initially created on the machine that hosts the Chrome or Firefox browser used by the MCA and doesn't need to be the machine where the D2A client is finally installed. The "Create Machine Credential' page in RAM provides a default value. This can be typed over with a more meaningful name – perhaps with some reference to the intended destination and/or recipient.

23. What happens if I create a credential with the same name as one in a different keystore?

This is essentially a 're-key' of a credential, and as long as your intent is to replace the credential in the second keystore, it is perfectly acceptable practice. For instance, if the original credential was close to its expiry date then this is the only way (currently) they can be replaced or renewed.

It is also acceptable for two credentials to have the same name if they are created for different ABNs. They are differentiated by the 'Subject name ID' which is comprised of the ABN and name.

24. Do credentials get renewed automatically?

Not at the moment. APRA intends to work with the ATO to provide the capability in the near future.

Renewal in this context means a re-key, with different private and public keys, rather than extending the validity period of the credential but keeping the same key values. It is not possible to simply extent the expiry date on a credential.

Machine credentials are valid for two years.

25. How do I back up a credential?

Copying a keystore file backs up all credentials in that file.

[1] note: we will remove the Auskey element in a future release

26. My company has more than one instance of D2A on a single machine, how many credentials and keystores do I need?

It depends on how many people use that machine.

If a single user normally uses that machine and runs the different D2A Clients themselves, then their best option would be to have all the credentials in one keystore file. So there would be multiple credentials, for different ABNs, in the single file and that file would be copied to the roaming folder of that user e.g.
C:\Users\<<userID>>\AppData\Roaming\AUSkey\keystore.xml[2]

For multiple users of the same machine, it may be sensible to have all the credentials for each user in a single keystore in their roaming folders.

As mentioned elsewhere, the MCA would normally create each keystore containing credentials for different ABNs that a user of D2A would normally need for their role. And give each credential a name that may include the user's name and/or other identifying information (the ABN isn't needed because that gets automatically added to the subject name ID) so that each credential is uniquely defined and can be traced. Then that keystore could be copied (and perhaps renamed) to the appropriate roaming folder.

27. Does D2A work with Citrix?

Yes, it works in the same way as user AUSkeys worked with Citrix.

Generally, the best approach is to treat the new credential as if it were a user AUSkey.

Although it is called a machine credential and the ATO's generic advice is to give the credential the name of the machine it is installed on –this practice is less applicable in virtualised environments like Citrix, where 'machines' are virtual devices or instances of virtual images and their names are ephemeral.

The new credentials are portable – so they can 'accompany' the user to whatever machine or virtual desktop or device they are using.

Remember that D2A expects to find the keystore in a fixed location which cannot be modified. So the MCA (or other authorised staff) should install the credential file (the keystore) in the user's roaming directory at:

C:\Users\<<userID>>\AppData\Roaming\AUSkey\keystore.xml

And of course, the ABN associated with the D2A instance running on a virtual machine must match the ABN in the credential itself.

[2] note: we will remove the Auskey element in a future release

So if a user normally uses a number of different D2A instances, submitting data for organisations with different ABNs it makes sense to put all the credentials they need in a single keystore. And if all those credentials are linked in some way to the user – by the user's name or another identifier for instance – they will be instantly recognisable and are easily traced by the MCA who created them.

28. Can D2A use a centralised keystore shared by many D2A instances?

No – this is not possible for D2A. The D2A client expects the keystore to be in the current user's roaming folder – not on a network storage device shared by many users or machines. And if the location or name of the keystore used by the D2A client is changed, D2A will fail to load. This is a security measure.

29. Are there any additional special security requirements for machine credentials?

It depends on the security policy and standards of your organisation

APRA