Facilitator – Stacey Wilson: Welcome, everyone, and thank you for taking the time to attend today's webinar on AUSkey Decommission. My name's Stacey Wilson, I'm from the Digital Partnership Office, and I'll be facilitating today's webinar. This webinar is part of an ongoing series of information sessions facilitated by the Digital Partnership Office.

I have a few points to note before I introduce today's speakers. All attendees are on mute, with the exception of the presenters, to ensure minimal interruption, however we would like to address any questions that you have in regard to the presentation. We have a number of subject matter experts on standby to answer questions via the Q&A box located at the bottom right of your screen. Please ensure that you submit your questions to all panellists to ensure the appropriate subject matter expert is able to respond. Any questions that we're unable to answer throughout the session will be covered in a Q&A document that will be published on the software developer website, along with a recording of the webinar.

Our presenters today are Paul Stasinowsky and Ben Avery from the Digital Communications and Identity Services Team, and Roger Obbes from the Digital Partnership Office. Before I hand over to Paul I would like to respectfully acknowledge the traditional owners and custodians of country throughout Australia and their continuing connection to land, waters and community. I would like to pay my respect to them and their cultures, and Elders past and present.

I'll now hand over to Paul. Thank you.

Paul Stasinowsky: Thank you, Stacey. I hope everyone can hear me okay. My name's Paul Stasinowsky and I've been working on various elements of the Digital ID Program for several years now. Most recently I've been working on the Machine to Machine solution which I'm expecting many of you will be quite interested in as part of this webinar.

I'd like to welcome everyone to this DSP webinar. I just want to start off by saying we're now really advanced with the implementation of the Digital ID Program. So in the past you will have heard probably a lot about what's coming. This one will focus really on what's here. So what we've introduced as part of the Digital ID Program is a new whole-of-government individual credential, which is myGovID, not to be confused with myGov, and we've also introduced a whole-of-government Relationship and Authorisation Manager called RAM, and together these replace AUSkey for user authentication, and then we are replacing Device AUSkeys and user AUSkeys used with software with a new machine credential available from RAM.

So by way of update, we're just sort of I guess setting the context and showing you what is available right now. So as I indicated earlier, the majority of the elements of the Digital ID Program are live and in production right now, and we're focusing our efforts on engagement with the various audience segments affected by the retirement of AUSkey. Our aim is to ensure you are ready and that your clients are ready, regardless of their AUSkey use case. So just quickly, myGovID app is available for Apple and Android smartphones via their respective stores or their app stores.

RAM is available right now. Businesses can be linked by eligible associates in the ABR, authorisations can be granted to other uses via RAM, and a user with a myGovID credential and a business authorisation RAM can now use that to access the ATO Business Portal, Access Manager, the ABR and Online Services for Agents. In addition to that we've got one external or non-ATO service which is currently accepting that credential as well, which is the USI Office, or the USI Portal, or unique student identifier, and you'll see a number of other

agencies offering myGovID and RAM business authorisations for user authentication very, very soon.

And in addition to that we've got the ability to import AUSkey users, so that's been released in RAM, so you can import those AUSkey authorisations, which we're hoping will assist greatly in the transition space. The advantage of that is that it will actually bring the permissions in Access Manager for those AUSkeys into the RAM business authorisation, and I'll be speaking a little bit more about that throughout the presentation.

Okay, we've got in addition the new machine credential, so it's available in production, it can be installed on a computer or a server, enables users to interact directly with Government online services through business software. So it just continues that functionality that's currently available within software. So currently where uses us an admin or standard AUSkey, or a Device AUSkey, they would use a machine credential in future. We've got support material available on the myGovID and RAM websites, and we have a range of how to guides for checking your records on the ABR and cleaning up your AUSkey data. They've also been made available. What you'll see, sorry, what you'll see is a lot more information becoming available very soon, so we've been working hard to develop information to support users and assist you through that transition period.

What have we got coming up? As I said, more online Government services. As I said before, we're working with 28 AUSkey relying agencies to transition their services. There's a lot of work involved in doing that, but we're working very hard with those agencies to ensure that they will be able to continue to provide those portals to their users with a myGovID and a RAM business authorisation. We're also working hard on some solutions to address exception cases, including those cases where an individual is unable to obtain a myGovID with a suitable identity strength. And my colleague, Ben Avery, will be talking about that later on in the presentation.

So this is a functionality matrix. It's kind of designed to give you an idea of what users will be able to do based on their level of authorisation in RAM. So you can see here we've got principal authority. Now principal authority is the associate of the business in the ABR, they will be the ones who begin the process of authorising others in RAM, so they'll need to link their business in RAM, and once they've done that they can then start authorising others. Now what we really wanted to illustrate here is that the principal authority has all permissions, right, so that everything they are able to do. Now you'll see here, claim business, obviously a principal authority is the only one who can claim that role for a business, and they have to be listed as an associate for the business in the ABR. You can see they can undertake all these actions, they can log in to portals on behalf of the business, they can view machine credentials, they can create and manage machine credentials, they can authorise others on behalf of the business, they can use machine credentials, and they can edit permissions of machine credentials in Access Manager.

So then we've kind of tried to step it out a little bit. So there's an authorised user, so a principal authority can authorise someone else in RAM and just give them an authorised user, or just make them an authorised user, and if they give them no other roles, that authorised user, that person will be able to log in to portals on behalf of the business, and they'll be able to use machine credentials, but they won't be able to undertake any of the other functions. In addition to that, an authorised user can be given a machine credential administrator role. What this role enables them to do is in addition to logging on to portals on behalf of business,

they'll be able to view machine credentials, they'll be able to create and manage them, and of course they'll be able to use them.

In addition to that we've got another role in RAM called authorisation administrator, and an authorisation administrator will be able to log on to portals, they'll be to view machine credentials, they'll be able to authorise others on behalf of the business. And that's the really important distinction for authorisation administrator users, or users with that authorisation administrator role. In addition they'll be able to edit permissions of machine credentials in Access Manager. So I'll be talking a little bit more about the ongoing connection between authorisations and the management of permissions in Access Manager. Of course an authorisation administrator will be able to use machine credentials as well.

Now an authorised user will be able to be given both the authorisation administrator and machine credential administrator roles in RAM for a business. Where that's the case you can see they can do all, they can perform all of these functions. Obviously the only thing they can't do is claim the business, because they're not an associate, but they'll be able to do everything else.

The other thing I wanted to point out with this matrix is that a user with no authorisation RAM will still be able to use machine credentials. So if I am required to use software that interacts directly via SBR, I can use that software without the need to get a myGovID or a RAM business authorisation, so I won't necessarily need that to be able to continue using that software to interact with Government services.

Okay, so the next slide here is the AUSkey Transition Release Plan. So as you can see, and what I really wanted to demonstrate is we are here, so we're very well advanced on the plan for the AUSkey transition, or the transition away from AUSkey. So you can see we're currently in the public beta for machine credential use, so they're available now live. We're delivering a few things in December for IP1 options, for manual creation for RAM relationships, a few other bits and pieces. We've got some things we're delivering in March. But most of the pieces are now in place to support AUSkey being decommissioned in March 2020, and so that's kind of what we're trying to illustrate with this slide here. So there's a lot of work we've undertaken to get us to this point.

Okay, so I just wanted to focus a bit on the Machine to Machine solution, which I would imagine would be of particular interest to this group. So as part of the work we're doing on the Digital ID Program, it includes a Machine to Machine solution, and so basically that's designed to enable business and tax professionals to continue to interact with ATO digital services through software.

So as you'd well be aware, a Device AUSkey allows software to communicate with ATO systems. A machine credential will replace the Device AUSkey, but will also replace user AUSkeys used in software. So for a lot of desktop or locally hosted software solutions users currently use an admin or standard AUSkey to interact, in future those users will need a machine credential instead, they won't be able to use an individual credential to be able to authenticate into that software product. So the machine credentials, I'm sure you'd be well aware, is installed on a device.

Now the machine credential administrator role will only be required if the business is using software, and by that we mean desktop or locally hosted software. So businesses that use Cloud software, they won't need to appoint an MCA, so if they have no need to actually get a machine credential themselves, they can continue doing what they do without the MCA role

or without a machine credential. And then the business representative with the MCA role, or the machine credential administrator role, can create and manage machine credentials on behalf of the business. And so, and I guess this is kind of a pretty broad overview, so Cloud software, so we've been working with software providers on what they need to do to transition, and we'll be talking a little bit more about that in detail later on in the webinar, and we've been giving guidance, and we've been working with DSPs to go through what's required in terms of updating Cloud software products to consume the new machine credential. But the important thing to note is that for end users who are using existing Cloud software products, there won't really be a change for them, so they will just continue using the product and they'll be really unaware that anything's changed in the background.

Desktop or locally hosted software on the other hand, that will present more of a change management challenge for us as an organisation, and also yourselves as digital service providers. So the Digital Partnership Office is working with digital service providers, and so they will do things like they'll let us know once the software's been updated, or sorry, they'll let users know, I should say, when their software's been updated, and users will need to get an updated version of that software.

Now the software, I guess broadly speaking, would really just need to be configured so that it points to a new end point, so currently obviously software, to get an access token, points to the VANguard STS service. As part of the Machine to Machine solution we're deploying or delivered a different service we call MAS-ST or Machine Authentication Service–Security Token, so it's very similar to the VANguard STS service, but software will need to point to that new end point. And so in the desktop version users will need to obtain a machine credential and then users will need to download and install that machine credential where it's available to the software, and then they'll need to install the software and direct the software to the machine credential keystore. And that depends on how the software is configured in that setup process. I understand there's a number of different ways that's done, but broadly speaking that's what will need to happen to support those desktop users to receive the new product.

So as I said before, we've developed a security token service which we call MAS-ST, so replacing the existing VANguard STS. At a high level the software product will be able to consume the new Machine to Machine solution if it is pointed to the new, or if it is pointed to a new machine credential, so if it's directed to the keystore that stores the machine credential, and it's directed to the MAS-ST end point instead of VANguard STS. So just incidentally as well, MAS-ST is compatible with Device AUSkeys, but obviously it will not be so, it won't obviously still be compatible with them once those AUSkeys expire in March 2020. So between now and March 2020 you can use a Device AUSkey, point software at the MAS-ST service, and you should still be able to get the access token that the software usually receives. I just want to note as well that MAS-ST is not compatible with user AUSkey, so admin or standard, so as such we're encouraging users of desktop software to appoint machine credential administrators and get machine credentials in anticipation of receiving the software update.

So just a couple of other things by way of background. So we've only just really released the M2M solution into production. We've run an EVTE trial for some time, I think we began that in April this year, and we've got some certainly very useful feedback through that EVTE trial and we've had to make some changes to the service from things that came out of that. So as part of that production release of the M2M solution there's the ability to get machine credentials via RAM. So in addition to that the M2M solution remains available on EVTE and

we'll continue to make that available on EVTE so developers can test existing, or updated, or new software products against the M2M solution in EVTE to ensure that they meet the requirements before they obviously deploy those live to users. And I've previously mentioned that desktop software will require a machine credential in order to access the MAS-ST service.

So one of the things I want to touch on is Access Manager integration, and so I guess it's one of the things that we might have taken a bit for granted, but it's an important principle of the Digital Identity Program that Access Manager still maintains the functions that it maintains now. And the way it does that is that currently say if you have an AUSkey, like a standard AUSkey, it's given some permissions, you can add or remove those permissions, and the same thing applies for Device AUSkeys. Access Manager will continue to do that, but it will do that for RAM business authorisations, and it will also enable you to do that for machine credentials. So machine credentials will be treated almost the same in Access Manager as Device AUSkeys, okay, so that like Device AUSkeys, machine credentials receive full permissions by default. Important to note, and this is for Cloud software providers, a new credential will not appear in Access Manager until after the first use, or until the credential's primed. And we're exploring options for displaying machine credentials in RAM as soon as they are created, without the need to prime, and we expect to be able to deliver that as part of our March deployment. So it's just something to note when you're providing Cloud software services because the machine credential will need to be applied to the Cloud software role in Access Manager.

Permissions can be amended as required and can be changed in bulk using the copy permissions function in Access Manager, and they can also be given access to act on behalf of another business in the ATO through the business appointments functionality. So that functionality won't be changing, and the existing business appointments will remain in Access Manager as we move to the Digital Identity Platform. Machine credentials for Cloud hosted SBR services can be enabled in Access Manager in the same way that Device AUSkeys are currently enabled. So that's another important consideration.

Another thing I wanted to outline is if a user is given, when a user is given authorisation in RAM for a business, if they're given full access for ATO on behalf of that business this is the equivalent of an admin AUSkey, in so much that they will get full permissions in Access Manager to access ATO services with their myGovID credential on behalf of that business. If the user, however, is given custom access for ATO on behalf of the business in RAM, this is the equivalent of a standard AUSkey, so they'll receive basic limited permissions, and those are the same basic permissions given to a standard AUSkey user, and these can be amended. And so as mentioned earlier, RAM gives the ability to import AUSkeys. The advantage to this is that when an AUSkey is migrated the permissions associated with that AUSkey in Access Manager are immediately reflected in the RAM business authorisation. So in other words, if I have a business and I have 10 standard AUSkeys with some permissions set up in Access Manager, I can import all those 10, I can assign those to users who have a myGovID credential, they can then accept those authorisations, when they do those authorisations will have the same permissions in Access Manager that the AUSkeys had prior to migration.

One thing you may want to note is that access administrator role in AM is not reflected in the RAM business authorisation when the user with a migrated AUSkey requires the ability to change permissions in Access Manager. So in other words, if you have a standard AUSkey and you have the access administrator role in Access Manager, when that's migrated that role

won't be brought across unfortunately, so that authorisation will need to be amended and have the authorisation administrator role in RAM added to that authorisation once migrated.

Okay, so here we're going to run through some use cases on what needs to be done by different, different players I guess in the Machine to Machine space. So this year's case is around DSPs providing desktop software. So kind of at a high level there's four main steps required from the DSPs in creating the desktop software products which consume the new M2M solution. The first one is update the desktop software, so the DSP will be required to update the software to point to the new end point, and those end points are available in the document that's currently published on sbr.gov.au, so it's in the physical end points document, and so it's in, we've had it published there for some time, that includes the end point in EVTE to access the MAS-ST service, and the end point in production to hit that same service.

Next the DSP will be required to package and deploy the update, so they'll need to package up the software that is amended to consume the machine credential with the MAS-ST end point, and they'll need to deploy their updated product and provide that update to their users. Now I guess there's a number of different ways that DSPs do that, and I understand that that may present some challenges, but in any event the new desktop or locally hosted software product will need to be deployed to users, and it will probably need some instructions accompanying that. And we're actually working on providing some guidance for you as DSPs that you can provide to your clients to assist them to get a machine credential, and how to set that up.

Here we've got a possible channel of communication, so we've envisaged sending an email or the DSP sending an email to subscribed software users advising that an update's available and providing the installation instructions, and that could also include information that we've provided to assist them through that process of getting machine credentials and working through that particular process.

In addition to that we'll be providing our own messaging. We're also working through our different audience groups to talk to impacted business across different segments to help them understand what they're required to do in order to be able to continue using desktop software after AUSkey's decommissioned in March 2020. So really our aim is that users of desktop software products will be able to be well supported through this process, both through yourselves, and we'll assist you in that, and through information that we provide. So they'll be able to come to us for information if they require it, and they'll be able to get information from yourselves as their DSP.

So we've got a quick overview for the business using desktop software. So I've gone through this pretty quickly. The end user impact, so they need to get a machine credential or get machine credentials which support their business setup. So there's not really a one size fits all for this. They may want to have a machine credential on every desktop, they may want to have their machine credential administrator create all the credentials centrally and distribute that to users via a thumb drive or via the IT network or IT infrastructure that's existing. So how they do that is kind of up to them, and we're not really being prescriptive about that, but the point is that a desktop software product will need to have a machine credential that it can access in order to request that access token from a MAS-ST service.

So they'll need to get the machine credential and then set that up, and then they'll need to point their software to that machine credential, and then they can continue using that, or they can use that updated desktop software product. And as I said, we're working hard to provide

support material, both through our audience channels, and also through the DSP community, to be able to provide comprehensive material to users that will enable them to transition as easily as possible.

So the next thing I want to touch on was DSPs providing Cloud software. Okay, so DSPs providing Cloud software, so with Cloud software the bulk of the change will be handled by the DSP, so basically what you'll need to do, like desktop software, you'll need to update the software to point to the new end point, you'll need to create a machine credential and store it in a similar location or a location that your Cloud software can point to. You'll then need to apply that Cloud software or point your Cloud software to that machine credential and then package and deploy the update to the Cloud, and then users will continue using that without really any impact. So just to demonstrate that here, a business using Cloud software will continue to use their software, they really won't be aware that there's been a change, and they'll just continue using that without interruption. So I guess in a nutshell, desktop software update will require effort from DSP and effort from the end user, Cloud software will require effort from the DSP, but no real effort from the end user.

Now I just want to touch on sending service providers. So sending service providers will basically have a pretty similar experience in terms of their software, so they'll need to either create or receive an updated software product if they have someone else produce that software, but they will need, so whereas sending software providers currently have an AUSkey and they're able to send on behalf of others with that AUSkey, they'll need a machine credential and they'll continue to be able to lodge information on behalf of others using that machine credential, instead of their Device AUSkey.

The reason for that is their sending service provider role is recognised in Access Manager, as with they, or as they transition to the new digital service platform or the Digital ID Platform they will continue to have that sending service provider role in Access Manager, and therefore we will still expect to receive SBR lodgements from them on behalf of other users, okay. So that won't really change. But they'll need to either update their software or receive an updated software product and get a machine credential, and then they'll be able to continue to send SBR lodgements on behalf of other users as they have done previously. So a business using a sending service provider, once again they won't really see any kind of significant impact, they won't really be affected by the change at all, so the changes will be undertaken by their sending service provider.

Now trying to run through some of the things we've noticed. Oh actually, just before I do, what I wanted to be really clear on here, and it's probably the easiest way to think through these changes, because there are some quite complicated use cases that are currently out there in the software Machine to Machine space, the important thing to think of is whoever has an AUSkey now in the SBR space, so whoever, whatever entity or the business, the ABN that holds the AUSkey now, will need to get a machine credential and use the machine credential in the same way that they're using the AUSkey now. That's the easiest way to think of it, okay. So if a business, like a sending service provider, they have an AUSkey right now, they'll need a machine credential to continue doing what they're doing, okay. So that's probably on a philosophical level or at a very high level, that's the easiest way to think through how this change will impact users, okay. So if you have an AUSkey now you'll need a machine credential to continue using software in the way that you do it now. If you don't need an AUSkey now, you'll be right to keep doing what you're doing.

Okay, I just wanted to come up with some common issues that we've encountered during EVTE testing. So we've had a number of DSPs come in and do EVTE testing, so our external vendor test environment, and we've gotten a lot of feedback through that, we've gotten a lot of valuable feedback through that, and we've actually made changes to our, actually made changes to our system and to our service as a result of that feedback that we've received. But some of the common issues that we've uncovered through that EVTE testing, which you may want to keep in mind, is use of the incorrect end point, so some DSPs have used an incorrect end point. As we've said throughout the pack, the end point is available from the SBR physical end point's document, which is currently housed on sbr.gov.au.

We've had some instances of using an incorrect applies to value, so the correct applies to value is test.sbr.gov.au/services. So, yeah, just make sure of that one. We've seen some issues come up with firewalls, firewalls may block interaction. The other thing is using an old and unsupported Software Developer Kit, SDK. So the new Machine to Machine solution supports the latest SDK, so if you're using an older SDK or you're not using the SDK in your software products, there may be more configuration changes required, so in that instance we'd encourage you to begin testing as soon as possible in EVTE and work through any issues you encounter. We can assist you as best we're able to in that transition space and in that EVTE test cycle, but just bear in mind that the Machine to Machine solution was I guess developed to support the latest SDK.

Okay, so with that I'll now hand over to my colleague, Ben Avery, and he'll run through some of the client group exceptions.

Benjamin Avery: Thanks, Paul, for that. Thank you for that, and thanks, everyone, for having us today. So as Paul mentioned, I'm just going to go into some of the exceptions where we've discovered as a part of the AUSkey transition. So obviously with the AUSkey transition we're focused on developing myGovID and RAM as that alternate credential to AUSkey, but there are a number of sort of exception cases where we're looking to provide solutions, and I'll go through those details now.

Now I'll just, so I'll just touch on, so that the ones we're going to discuss today are individuals who do not have the required identity documents to verify their myGovID to a standard identity strength. So with the way obviously myGovID works, a user will need to set up their myGovID to what we call an IP2 or standard identity strength, which requires two of three documents, so they either require an Australian passport, an Australian driver's licence or learner's permit, or a Medicare card. The birth certificate will be available in our next release, so as an option as well, from next weekend.

Now recognising that, you know, we do deal with users that are overseas, or even Australian residents that don't have those identity documents, and therefore may not be able to get their myGovID to an IP2, what we are looking at is introducing an IP1 option in RAM. So when you set up an authorisation you can elect to set up an authorisation for an IP1 user, so we're actually calling those users basic authorisations. Now with the IP1 authorisation, because the credential strength, and I guess the whole solution is, you know relies on that strong security in credential strength, so with consultation with other agencies and internal and everything in the ATO, as part of that IP1 solution, you know, the user cannot be an admin for the business, they won't be able to be an MCA for the business, and they'll be restricted in terms of the Government services that they can actually access. We've consulted with Government agencies, and those agencies that have confirmed, have advised what, you know whether they're willing to accept an IP1 user or not.

So we do actually have, and I might just touch on the other agencies first for that first exception case. So as part of our next release we are supporting the IP1 option for other agencies as they onboard, so recognising not all agencies have onboarded yet, but as they onboard those agencies that have requested an IP1 solution will be able to sort of implement that as they onboard from December. So that'll be available from December. I will touch on what the ATO's doing in relation to the IP1 users, and I guess the authorisations that can be established with that. I've got that on the next slide, so I won't sort of go into too much more detail with that at the moment.

So the other two exception cases we've got there, the second one is about individuals that cannot link their business in RAM. Now what RAM relies on at the moment, when you go and link your business RAM relies on the Australian Business Register, and it relies on an associate listed against that ABN. Now that's the current process which is automated through RAM, so if anyone's gone through that process you obviously provide your address details, you're presented with a list of businesses that have you linked as that associate on the ABR, and you're able to link those businesses.

Now we do recognise that there are a number of entities, and I think we actually had a question in the Q&A there, that are unable to link a business at the moment purely because we don't have any associates listed against those ABNs on the ABR. So they include entities such as Government departments, so Government departments won't have an associate listed. They may have an authorised contact, but they don't have an associate. It also includes entities such as not-for-profits. And a big one that comes through is corporate trustees, so which we refer to as non-direct associates. So that's where they may, the ABN may be linked to another ABN as part of that trustee relationship, but they won't actually have an individual link to that. Other examples of that are public schools and deceased estates, and things like that.

So from December we are actually introducing functionality to allow an authorisation to be established for that type of entity. Now it is a manual process, so it does require the right person, so they need to be an authorised contact against that entity, to call up the ATO over the phone and they'll verify who they are, and then telephony or one of our frontline staff will actually go in and add that particular user to that ABN. As part of that process they still need to accept the request, which they do so by logging in to RAM with a myGovID and accepting that request. So that essentially for those entity types that don't have current listed associates on the ABR, there is that option from December for them to call up and have them manually linked, and that essentially creates the authorisation chain to allow them to manage the authorisations for those entities.

The third I guess exception case there is that where users have been unable to set up their myGovID due to faulty documents or name mismatches and things like that, so with that one, so with myGovID, it does rely on the document verification service to allow users to link their documents, which is called upon as they're linking. So if there's any sort of faulty documents or any mismatches and things like that, it's obviously not going to allow them to link those documents or set up their identity to the required strength. What we, what we are suggesting, it sort of is a little bit out of the control of myGovID, but it is a requirement for the user to make sure their documents are up to date. If they've got faulty documents or any issues with it, we are recommending to call the issuing document provider to confirm that it is up to date and correct. So that one there sort of is relying on sort of obviously a user making sure their documents are correct and up to date.

Now I might just move on to the next slide. Now I did, as part of that first exception case, I spoke about creating the basic authorisation for an IP1 user. Now what the ATO is doing in relation to that, recognising, you know, we do have users that are offshore, you know, they may be on temporary work Visas or just can't get the right identity documents to set up their myGovID to the required strength, so in the middle of March we are releasing functionality to allow a basic authorisation to be created for ATO services.

Now again we have reviewed, in terms of getting access to ATO services, you know, we do rely on Access Manager to define the permissions, and we have reviewed the permissions aligned to a basic user in Access Manager. You know, we're quite conscious, you know, these users, you know, it isn't a verified identity, so you know they won't have permissions that allow them to essentially change bank details or change business registration details, but they will be able to do other functions for the business.

So with the IP1 for the ATO, again they can set up an authorisation in RAM for a basic user. Now the ATO, we do require some additional proofing of that individual, so once they set up an authorisation they can accept the authorisation, but before they actually get in to, they're able to access ATO services they will need to provide some additional identity documents just to verify that they are who they say they are, to allow them to transact with the ATO. So that solution will be available mid-March, and we will be providing information on our website on that to help businesses prepare for that solution and what they need to tell their users in terms of setting it up. But essentially, you know, recognising the need that we, you know there is users out there that may not be able to get the right identity strength, and we are developing solutions to allow those users to interact and proceed, recognising that, yeah, they will be restricted in terms of what they can do, but will be providing information on that.

So essentially they're the, I guess the three major use cases we're looking at, at the moment. I guess the good thing is, the second one I mentioned, the manual authorisation, will be available from December. So look out for that if you are in that situation where your business structure is set up like a corporate trustee, or there was that question about being a Government representative, there are those options available from December to allow those type of entities to be linked in RAM and to essentially initiate that authorisation chain.

I'll move on, I think, Roger, you're going to be discussing the next component.

[Pause on audio]

Roger Obbes: Can you hear me?

Paul Stasinowsky: Yes. We can hear you, Roger, we can hear you now.

Roger Obbes: Oh sorry, yeah, I had some technical issues here. For Online Services for DSPs, we have the AUSkey decommissioning, that's going to impact on the authentication of Online Services for DSPs, and so we're moving away from the AUSkey and we're going to be using the myGovID. So that we've got the new authentication of Online Services for DSPs and it will be available from 13 January 2020. That's the date we've been able to lock in at this time, and we're hoping to achieve that date.

Prior to that date, the 13th of January, we will continue to use your AUSkeys to use Online Services for DSPs, but from the 13th of January 2020 you'll only be able to use your myGovID. So to assist in that transition the principal authority or authorised administrator should be importing the AUSkey, import the AUSkeys via using RAM. Now that may have

already been done through the linking of the business and setting up in RAM, so that may have already been done. This will allow the ATO to match your existing profile, so when you get to view your previous records, when you log on like to Online Services for DSPs with your myGovID you should be able to see that history there.

If you have not been able to import prior to the authentication using the new myGovID approach for online services, that we will not be able to link you automatically to your old file, you will not be able to see your contact registration tickets, and you won't be able to access any of your previous requests. So actually as a mitigation for that we have created a ticket to allow you to inform us if you've got that issue, and you'll be able to lodge a ticket with us through online services to actually be able to have that received from our team here, who'll be able to action that, so that will be able to create that link again and get you working again. We're going to have some more information available shortly, which we'll be sending out to the different users of the Online Services for DSPs.

So I'll throw over to Paul. I think you're finishing off.

Paul Stasinowsky: Thanks, Roger. Yeah, so I guess what we're talking about now is next steps, what do we do from here, what do we need you to do, what do you need to do to ensure that the transition is smooth, that things are done in enough time, and we bear in mind that it is a tight timeframe obviously between now and March 2020 when AUSkey is formally retired. So there's a few things we're asking business to do, there's a few things that we're asking business broadly to do, and we're also asking DSPs to do the same.

So first thing is if you haven't tested your product in EVTE yet, get in contact with us, get in contact with the DPO. So you can do that either through Online Services for DSPs, so you can log in to that using your AUSkey, you can request to be a part of that EVTE trial, but you will need to be in order to ensure that your products are compatible with the M2M solution, right. So I can't stress that enough, make sure you take part in the EVTE trials. So get in contact with us. If you don't have access to Online Services for DSPs, send an email to dpo@ato.gov.au, and then request to be included in the EVTE trial for the M2M solution, okay. So that's one of the big things we need to stress.

Next, get a myGovID now. And I'd hope that many of you already have it, right. So go to the app store, go to your platform's app store, iOS or Android, and search for myGovID, download the app. If you have the Australian Government issued documents, so have your driver's licence, passport or Medicare card, prove your identity, okay. So get your app set up, get that ready to go, prove your identity. If you're an associate, go in to RAM, so log in to RAM at authorisationmanager.gov.au with your myGovID, okay, and then go through the steps to claim it. So in order to claim your business you'll need to provide an address for tax purposes, and then RAM will present you with a list of businesses for which you are an associate or listed as an associate in the ABR.

If you're not an associate, but you're obviously working for a DSP, take steps to notify the associates, right. So depending on the size of the business, some associates, obviously they're busy in the work that they do in running the organisation, they may not have seen these messages, right, so they may not be aware that this stuff's coming up, so get in contact with them if you're able to, get them to get a myGovID credential, get them to claim the business. Once they claim the business they can just authorise one other person, give that person the auth admin role, and then that person can go ahead and import AUSkey users, set up authorisations, and then everything's in place and everything's prepared, okay. So that can't

stress that enough, so an associate will need to claim the business, right, so it's a really, really important step.

In preparation for that, go into abr.gov.au and you can authenticate with your AUSkey to do that, check on the associates now, so make sure that for the business the associates, the listing of the associates is correct. If they're incorrect and you have the appropriate permission, change the associates, right, so update them, make sure those records are up to date. You don't want someone who's not an associate being able to claim a business, okay. We're treating the ABR as the source of truth in terms of the connection between businesses and individuals who are legally responsible for those businesses, so please make sure that that information is up to date and current, right. So you can log in to abr.gov.au with your AUSkey and you can update those details.

Get rid of any AUSkeys you don't need, right. So if you've got AUSkeys in your business that have been around for a long time, or you know the user of that AUSkey has moved on, log in to AUSkey Manager and get rid of them, right, because when you go to import your AUSkeys they'll all come up. So if you've got a hundred standard, but only 20 of them are currently used, when you go to import you'll see a hundred standard, and you'll have wade through those to figure out whose are whose, who you want to allocate them to. So just get rid of those ones that you don't need anymore in AUSkey Manager, right, so you can log in to AUSkey Manager with your AUSkey and get rid of those AUSkeys. It'll make that transition period just a whole lot easier.

Get machine credentials, right, so they're available now. So if you have the machine credential administrator role or if you're a principal authority, log in to RAM, place the business in focus, and then you select the manage credentials tab, which is on the top bar, it's one of the tabs, you'll need to download a browser extension, so we've got a browser extension that's available from our RAM website, our RAM information website, which is info.authorisationmanager.gov.au, so those browser extensions are available there, right, and you can download and install those now. So the operating systems that we accommodate with those browser extensions are macOS, Windows and Linux, okay, and we support Firefox and Chrome based browsers, okay. So you'll need to do that in order to get a machine credential, but I just want to stress you don't need that in order to use a machine credential, and you won't need that for any user authentication exercise, given that user authentication will occur in future with a myGovID credential. It won't be a, like an AUSkey style authentication where you've got a credential sitting on your device. You know, so for a user authentication you'll be using your key, your myGovID on your personal device, and then the machine credential, the Software Developer Kit incorporate, the elements of the Software Developer Kit incorporated into the software consume that machine credential, okay.

So you'll need the browser extension. So if you work for a large business in a controlled IT environment you may need to liaise with your IT department to enable or to allow the browser extension software to be installed and loaded onto your browser, so just bear that in mind as well. As I said, they're available right now on the RAM information website. And then so once you've got the browser extension and you've got the MCA role or you're a principal authority, you can create and download machine credentials and then you can start using them, you can start doing what you need to do with them. Also you may hear from your clients, so your clients who have desktop software may have heard some messages, and they may be getting in contact with you. You can direct them to some information that we can direct you to, or we can give you some links to some information you can direct them to. Also we'll be providing resources that you can provide to assist them in that transition space.

So we're not only having these sessions with yourself, we're having these sessions with larger groups with different audience segments across business, to make sure that they are prepared and they are ready to onboard to the digital identity solution, the Digital Identity Program, and that they're ready to transition off AUSkey.

I guess that concludes the, I guess the presentation portion of the webinar, so that's the information that we've prepared for you today. I'll just throw back to Stacey to conclude the webinar, and thank you all for your time and attention.

Facilitator – Stacey Wilson: Thanks, Paul. I'd like to thank everyone for attending today. And I'd also like to thank Paul, Ben and Roger for their presentation. Hopefully they've given you some really valuable insight into the Digital Identity Program and current key issues and developments that are underway.

Just a reminder that the webinar was recorded and will be published on the software developer website. Questions raised at the Q&A box will also be published on the site, including responses to any questions that we were unable to respond to today. So I noticed there were quite a few technical questions coming through that we may need to escalate to our technical team for accurate responses, so we'll make sure that we include those in that document that we publish on the website.

If you have any further questions you can submit them via online services or send an email to the DPO mailbox. You'll also note on the screen in front of you there is information available on various public websites. myGovID has it's own website, as does RAM, Relationship Authorisation Manager, we've got our software developers website of course, and the ATO website has some information, and ABR also. So if you're interested in further information you can read on those websites at your leisure. Otherwise of course, as I said, submit a query via online service or send an email to the DPO mailbox.

Thank you everyone for your attendance. Appreciate your time today.