DRAFT

Cloud Software Authentication & Authorisation

(replaces 'AUSkey in the Cloud')

Software developer information kit

DRAFT ONLY - *This document has been developed to collect feedback from SWDs and government agencies*

Australian Government
Australian Taxation Office

DRAFT

Contents

1 Executive summary

2 Context

3 Policy advice

4 What is the 'Cloud'?

5 High level solution

6 Set up and authorisation process

7 Cloud Software Authentication & Authorisation requirements

8 Transition assistance

Appendix A - Cloud Software Authentication & Authorisation - Detailed Design

Appendix B - Cloud Software Authentication & Authorisation agreement

Appendix C - Setting up your device AUSKey

Appendix D - How your client will nominate an Online Software Provider via Access Manager

Appendix E - How your client will nominate an Online Software Provider via Phone

Appendix F - Frequently Asked Questions (FAQ)

DRAFT

1. Executive Summary

As businesses update their processes and technology to adapt to the current digital environment, there is an increased demand for the use of business management software in the cloud (online).

Taking into consideration the feedback received from the software developer (SWD) community on the use of AUSkeys in the cloud, the ATO have been working with agencies across government to develop a solution that would streamline the client experience, support a move toward Digital by Default and be compatible with future directions (e.g. WofG authorisation and Single Touch Payroll).

The ATO will implement changes to support a Cloud Software Authentication & Authorisation solution that:

- enables approved SWDs to setup a dedicated Device AUSkey for the purposes of securing transmissions to the ATO made by businesses through online (cloud enabled) software,
- allows businesses to nominate and authorise a SWD's dedicated Device AUSkey for the purposes of securing transmissions made by the business from within their online (cloud enabled) software,
- eliminates the need for businesses to obtain, upload or use an AUSkey to secure transmissions when interacting with the ATO via online (cloud enabled) software,
- applies to both businesses and tax agents, and
- co-exists with existing compliant SWD solutions until transitioned to the new model.

The targeted deployment date for the Cloud Software Authentication & Authorisation solution (initially for ATO lodgements only) will be 30 June 2015 with the ability for SWD to begin transitioning from 1 July 2015.

It is expected that SWDs satisfy requirements that address legal and technical aspects of the solution and develop on-boarding processes for new clients by **31 December 2015**. Additional time will be provided to transition existing clients to the new solution. It is expected that existing clients are transitioned by **31st of March 2016.** The ATO will work with SWDs and assist with transitioning their products and their clients to the new solution.

If you would like to provide feedback or arrange a meeting to discuss your individual circumstances/scenarios please contact the ATO Software Industry Liaison Unit (SILU) via email or phone 1300 139 052.

2. Context

Registering for and maintaining credentials across government?

Registering for and maintaining credentials across government in order to interact digitally is difficult for businesses today. This is impacting the take-up rate of digital services offered by government. Recent ATO consultation activities with small businesses have highlighted the frustration faced with applying for and using an AUSkey.

There were approximately 2 million actively trading businesses in Australia at June 2013. Currently there are approximately 1 million active AUSkeys, of which belong to approximately 500,000 unique businesses. Approximately 300,000 unique businesses are actively lodging (based on activity statement lodgements).

As businesses become more mobile, based on changes to technology, credentials used to access government services also need to evolve and meet the needs of businesses.

The future of digital identity across Government?

The ATO is progressing digital as the default way to interact and driving whole of government initiatives such as Single Touch Payroll that leverages off a business's natural systems to streamline interactions with government. Addressing digital identity across government is key to enabling these and other transformational initiatives.

With the establishment of the Digital Transformation Office (DTO), government is committed to streamlining access to government services, making it simpler, clearer and faster for individuals and businesses. The DTO will be responsible for improving digital identity across government, leveraging myGov and the Australian Business Register to transform the way services are delivered to both individuals and business. This will mean myGov and the use of other credentials (e.g. voice biometrics) will become the future of credentials for individuals and businesses.

3. Policy Advice

The current AUSkey conditions-of-use (abr.gov.au/AUSkey/Help-and-support/AUSkey-terms-and-conditions/Conditions-of-use---AUSkey) outlines the responsibilities placed upon AUSkey holders. Failure to uphold these responsibilities will result in the cancellation of the AUSkey.

Policy advice received from the Department of Finance on the use of AUSkeys indicates that software developers remotely storing their client's AUSKeys and in some cases their associated passwords, in cloud based solutions are in breach of the AUSKey terms and conditions of use.

Responsibilities in relation to the AUSkey Standard Certificate

4.1 The Certificate Holder and the Business must not: • disclose the password for the AUSkey Standard Certificate to any other ***person*** • store the AUSkey Standard Certificate in a keystore to which any other ***person*** has access • otherwise allow, grant, permit or enable any ***person*** other than the Certificate Holder to use the AUSkey Standard Certificate.	There is no definition of ***'person'*** in the policy. We have received legal advice stating that 'person' includes computers, systems and software.
4.2 The Certificate Holder and the Business must promptly advise the ABR CA if: • the Certificate Holder is no longer authorised to use the AUSkey Standard Certificate on the Business' behalf • it becomes aware of any unauthorised use of the AUSkey Standard Certificate • the security of the AUSkey Standard Certificate or its password has been ***compromised***.	There is no definition of ***'compromised'*** in the policy. We have received policy advice from AGIMO (who accredit the AUSkey system) that any transfer of an AUSkey off the computer that it was generated on, onto another computer via the internet (i.e. uploading to any form of cloud storage) , constitutes a breach of the terms and conditions.

Responsibilities in relation to the AUSkey Device Certificate

4.1.1 Who can submit an application for a Device Certificate? An application for an AUSkey Device Certificate (to be held for a Business Entity): • can only be made by an Administrator for that same Business Entity, and • can only be made online through the AUSkey Manager, and • must nominate an individual ***who holds a valid AUSkey Standard Certificate*** (for that same Business Entity) as the Device Custodian to be associated with that Device Certificate.	Device custodians must hold pre-existing Standard AUSkeys for the business, thus typically aren't the Cloud provider. The Device Custodian creates the password, which cannot be disclosed to any other ***'person'*** **(**as per previous slide), and ensures the Device AUSkey is only used on the intended device, presumably requiring physical access to installed sites, or some other form of assurance.

4.4.1 Device Custodian responsibilities
 	
The Device Custodian for an AUSkey Device Certificate is responsible for:
 	
• downloading the Device Certificate when it is issued, following registration
 	
• creating the password that protects the Device Certificate and its associated Keys, and changing that password at recommended intervals
 	
• ensuring the Device Certificate is ***attached to the correct Device***, for example by ensuring a match between the IP address of the Device and the subject of the Certificate
 	
• safely transferring the Device Certificate from the download location to the server location, if required for example because:
 	
  • email access is not available on that server, so that the download link that is used to install the Device Certificate cannot be accessed from that location, or
 	
  • ***the Business Entity has an IT Outsourcing, SaaS or similar arrangement with another entity, and needs to transfer its Device Certificate to that other entity's hosting location.***
	The Device AUSkey conditions-of-use do not expressly forbid Cloud use, however given the definition of ***'compromised'*** (as per previous slide) Device Custodians cannot send the Device AUSkey across the internet, or by any other comprisable means.
	Cloud providers aren't allowed to have the password 'disclosed' to them, their systems or software.

4. What is the 'Cloud'

The Department of Finance have released the Australian Government Cloud Computing Policy. The definition below can be found in this policy.

http://www.finance.gov.au/sites/default/files/australian-government-cloud-computing-policy-3.pdf

Australian Government definition of cloud computing

The Australian Government has adopted the US Government's National Institute of Standards and Technology (NIST) Definition of Cloud Computing[8].

The following is an excerpt from the current NIST Definition of Cloud Computing, Special Publication 800-145 September 2011.

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Service Models

Software as a Service (SaaS). *The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure[10]. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.*

Platform as a Service (PaaS). *The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.*

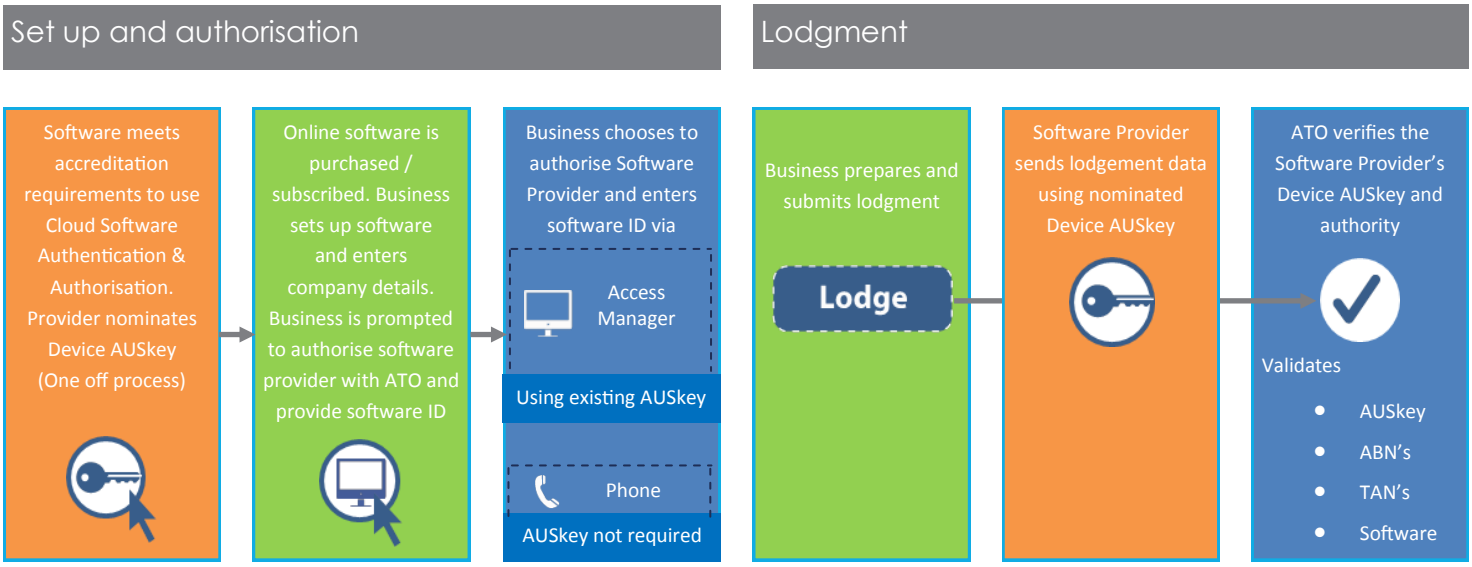
Infrastructure as a Service (IaaS). *The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).*

5. High Level Solution

The proposed Cloud Software Authentication & Authorisation solution allows a business to authorise a Software Provider's dedicated Device AUSkey for the purposes of securing a transmission/lodgement to the ATO via online 'cloud' software.

How does it work?

1. The SWD meets accreditation requirements to use Cloud Software Authentication & Authorisation
2. The SWD nominates a dedicated Device AUSkey which is used to secure transmissions initiated by their business clients via online (cloud enabled) software.
3. The SWD's clients are asked to contact the ATO and authorise the SWD (via Access Manager using their current Admin AUSkey or over the phone (Must be verified as a business associate to use the phone channel) and provide their 'Software ID'[1]
4. Once the business initiates a transmission (e.g. lodges), the lodgement data (including the Software ID) is sent to the ATO and secured using the SWD's dedicated Device AUSkey
5. Once the lodgement data is received, the ATO verifies that the authorisation between the SWD and the business exists and the Software ID matches the one provided by the business in Access Manager. For agents the relationship between their business and their client is also verified.



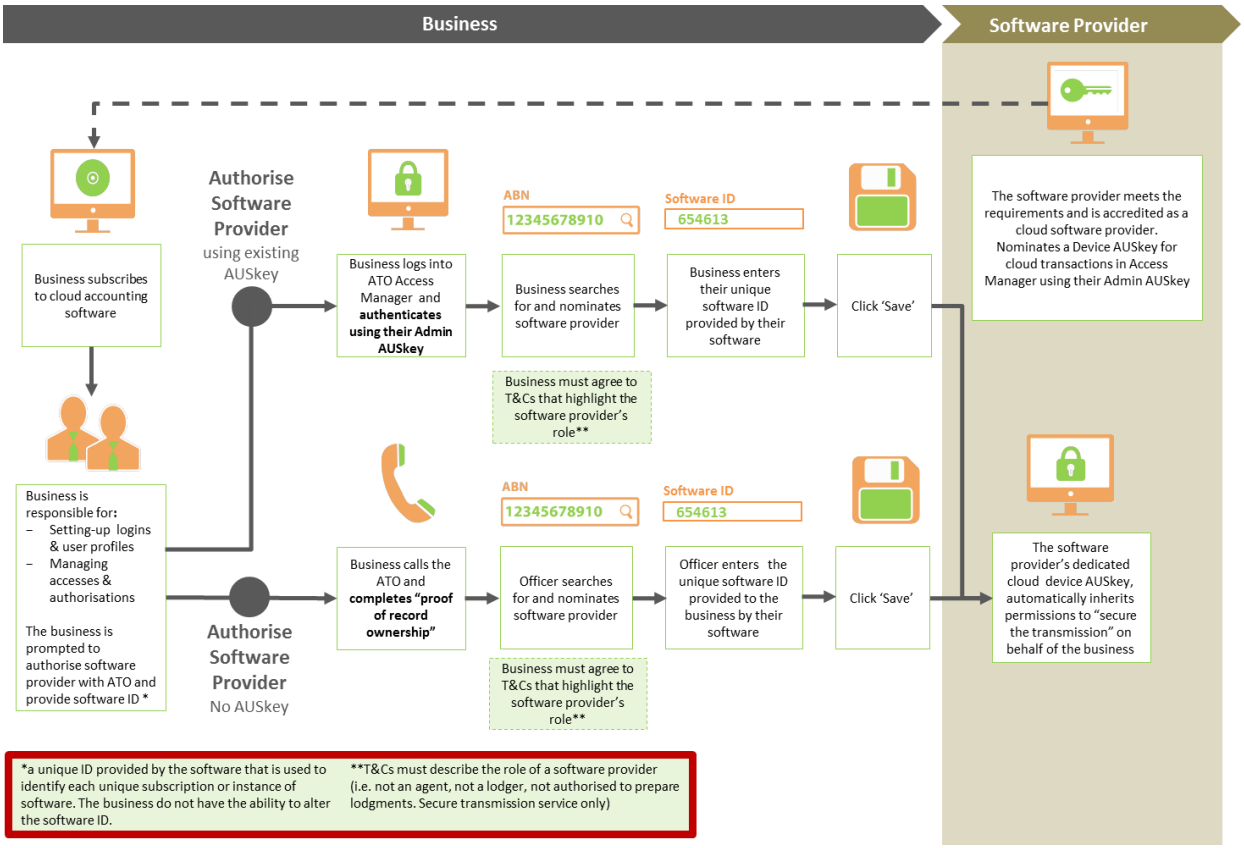
1 - 'SoftwareID' is a unique ID that is used to identify each unique subscription or instance of software

Benefits

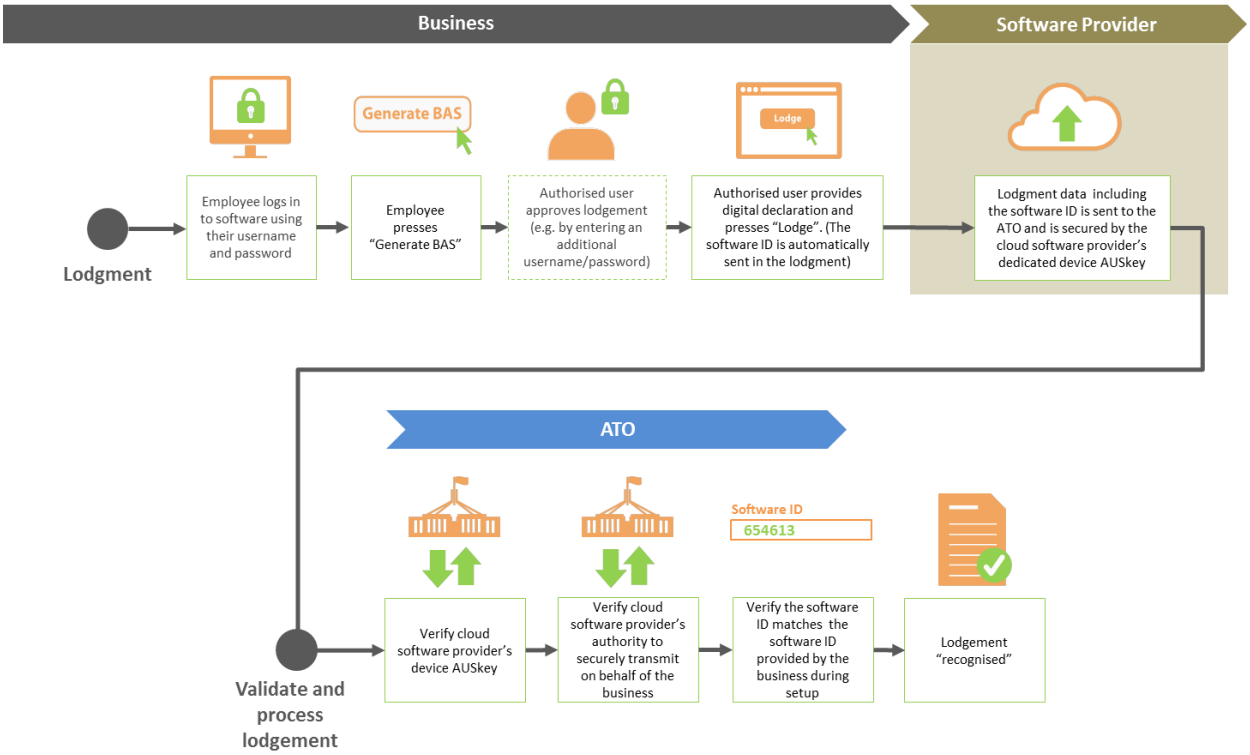
- Simplified on-boarding process for the business client offering them choice during transition/on-boarding on how to nominate a cloud Software Provider
- Businesses do not need to register for and obtain an AUSkey in order to authorise a Software Provider and transact in cloud, maximising take up of these services
- Device AUSkey nomination by the Software Provider is only required once using an existing Administrator AUSkey (in Access Manager)
- Software Providers can nominate multiple device AUSkeys if required
- Dedicated Device AUSkey limits the potential for fraudulent access by unauthorised individuals
- No concentration of AUSkeys in a single location

Detailed design aspects of the Cloud Software Authentication & Authorisation solution can be found in Appendix A – Cloud Software Authentication & Authorisation - Detailed Design .

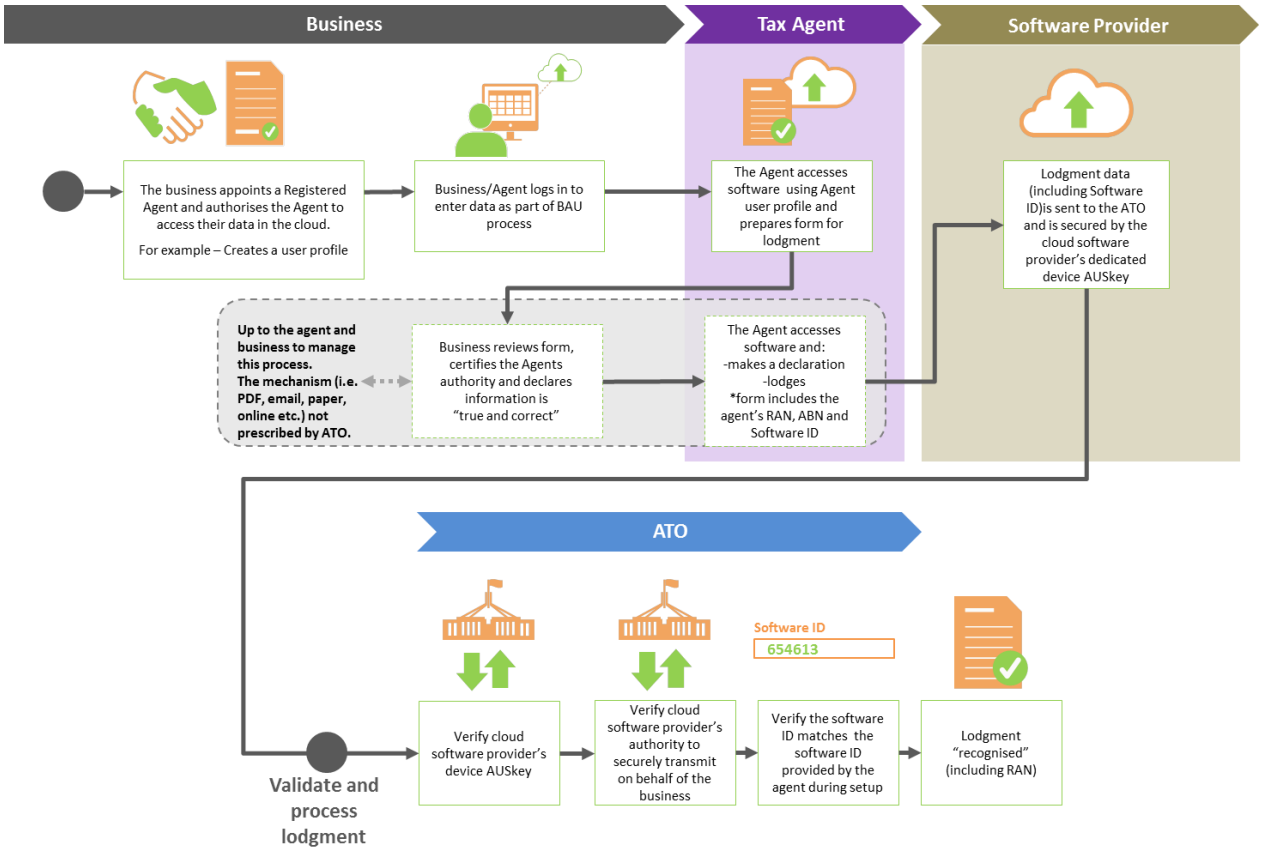
Cloud software set-up and appointment – ATO Only



Lodgement by "business" using cloud software



Lodgement by Registered Agent in the cloud



6. Set up and authorisation process

To provide services using the Cloud Software Authentication & Authorisation solution, software developers will be required to complete the following steps to on-board and become accredited. The steps below also outline what your client is required to do to on-board/transition. If you would like assistance with transitioning to Cloud Software Authentication & Authorisation , please contact the ATO Software Industry Liaison Unit (SILU).

Step 1
Register to become a SBR licenced Software developer

For information select the link below.
http://www.sbr.gov.au/software-developers/what-can-i-expect#register-intent-license

Step 2
Complete Cloud Software Authentication & Authorisation agreement

For a copy of the agreement select the link below.
Cloud Software Authentication & Authorisation agreement

Step 3
Set up your device AUSKey

To navigate to instructions on how to set up your device AUSKey select the link below.
Appendix B - Setting up your device AUSKey

Step 4
Design and build your system and messages

Ensure that Cloud Software Authentication & Authorisation requirements are met.

Step 5
Assess and test your product against the certification process via

- SBR 1 - Self Certification Process

For information select the link below.

http://www.sbr.gov.au/software-developers/what-can-i-expect#self-certification

- Or SBR 2 (ebMS3) - Certification Process

For information on how to certify for SBR 2 refer to the link below.
http://softwaredevelopers.ato.gov.au/ATO-ebMS3_subscription_to_EVTE

Step 6
Online software product is purchased / subscribed.

Step 7
Business sets up software and enters company details

Step 8
Business prompted to authorise software provider with ATO and records Software ID

Step 9
Business nominates an online software to make lodgments with the ATO via

- Access manager

To navigate to instructions on how to **nominate an online software provider** via Access Manager select the link below.
Appendix C - Nominate an online software provider via Access Manager

- Or phone

To navigate to instructions on how to **nominate an online software provider** via phone select the link below.
Appendix D - Nominate an online software provider via phone

7. Cloud Software Authentication & Authorisation Requirements

To become accredited as an online software provider you must ensure your software product meets the requirements outlined below. (Please note that these are Cloud Software Authentication & Authorisation specific requirements only, other existing SBR and AUSKey requirements and standards apply).

The following reinforces key requirements set out in the SBR Message Implementation Guide that must be adhered to for Cloud Software Authentication & Authorisation and include four new requirements that will also need to be incorporated into your software products. You will be required to declare that you have met these requirements to become accredited. *See Appendix B - Cloud Software Authentication & Authorisation Agreement*

Requirements

No	Description	Requirement
1	Declaration	Prior to lodging a form a user (business representative or authorised intermediary) must provide an appropriate declaration ***as outlined in the SBR Message Implementation Guide.***
2	Lodgement	Lodgements from a Registered Agent user must include the Registered Agent Number (RAN) ***as outlined in the SBR Message Implementation Guide.***
3	Software terms and conditions	Software terms and conditions must describe the role of a software provider (i.e. not an agent, lodger or authorised to prepare lodgements. Secure transmission service only). ***The ATO will provide instruction to support this (to be added to appendix).***
4	User authorisation	Upon authentication the software must recognise the role of the user (e.g. Authorised business representative or intermediary). This should determine what information the user is authorised to access and what functions they are able to undertake (for example must recognise the difference between an authorised representative and an intermediary).
5	Software ID	A unique (read only) Software ID must be provided to authorised users for each software subscription or instance of software. The online cloud software will ensure a unique software ID for each software account is automatically sent within the message of the transmission (Software ID not entered by client). *This Software ID will be recorded in Access Manager when an authorised business representative nominates their Software Provider.*

No	Description	Requirements
6	User authentication standards	We need to work with SWDs to develop minimum standards for user authentication. Software providers using passphrases as the sole method of authenticating a user must implement a passphrase policy the meets 'best practice' standards. Requirements should protect business information and maintain a positive user experience. **EXAMPLES** 1. Based on research conducted, the following common standards are used by many of the banks today: **Passphrase strength** A minimum length of between **6-8** characters, consisting of at least one alphabetic character and one numeric character. Some enforce the use of other character sets (e.g. uppercase alphabetic characters) **Failed authentication attempts** Users are generally locked out after 3 failed logon attempts to reduce the risk of brute force attacks. A temporary lock out is used by some before a complete lock out (e.g. locked out for the remainder of the day or 10 minutes). After a complete lock out the user is required to call a representative to get their password reset. 2. The Information Security Manual (ISM) is the standard which governs the security of government ICT systems. As such, AUSkey follows the below standards: **Passphrase strength** A minimum length of **10** characters, consisting of at least three of the following character sets: • lowercase alphabetic characters (a–z) • uppercase alphabetic characters (A–Z) • numeric characters (0–9) • special characters. **Failed authentication attempts** • Lock out user accounts after a maximum of **5** failed logon attempts to reduce the security risk of brute force attacks . (AUSkey = 3 failed logon attempts). • Have a system administrator reset locked accounts (For AUSkey the user is required to register for a new AUSkey) The ATO will work with software developers to come up with an agreed set of requirements addressing user authentication as part of the proposed Cloud Software Authentication & Authorisation solution.

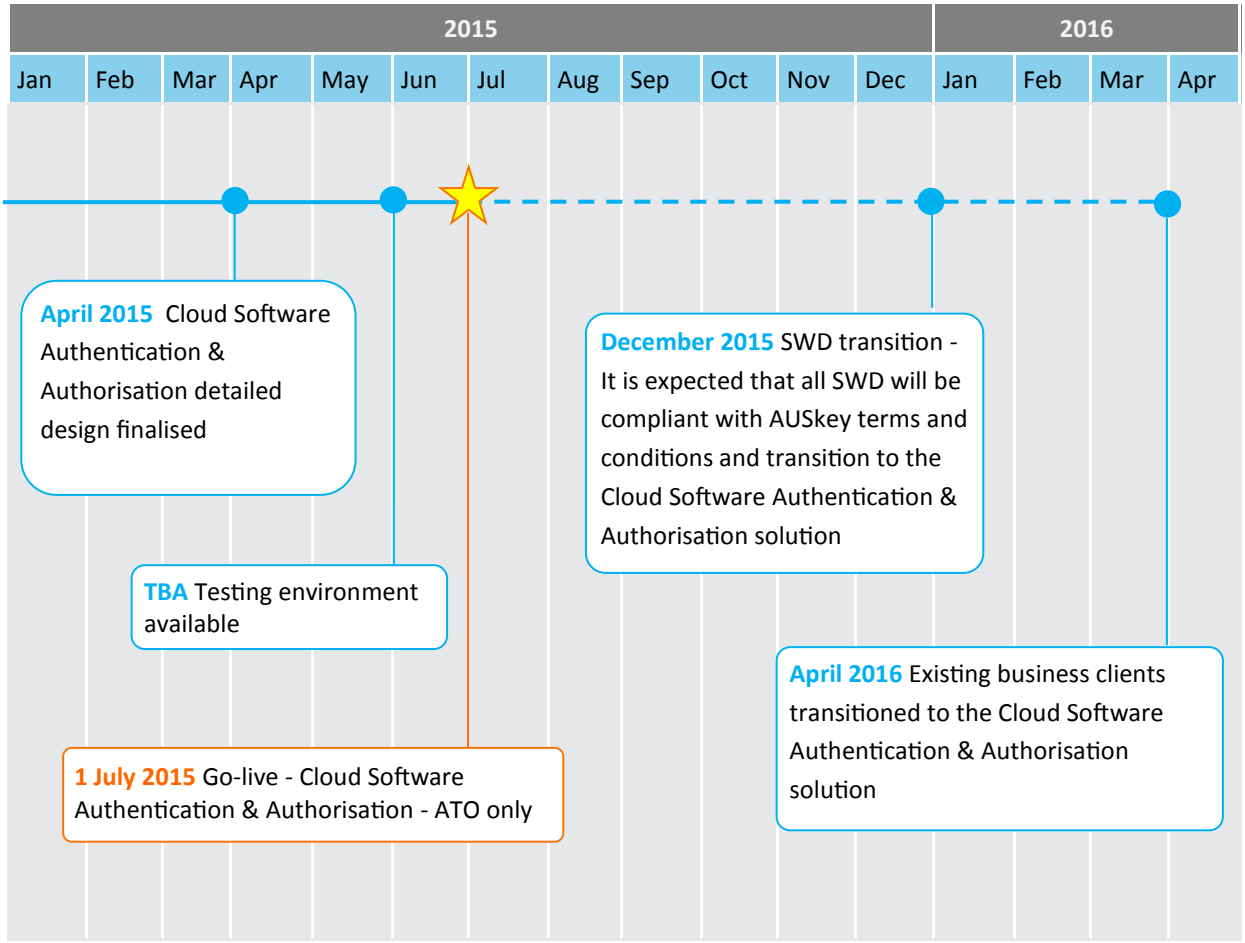
Adhering to the SBR taxonomy

For information on how to build SBR enabled software refer to the link below.
http://www.sbr.gov.au/software-developers/what-can-i-expect#design-build-test

8. Transition timeframes

The targeted deployment date for Cloud Software Authentication & Authorisation (initially for ATO lodgements only) will be 30 June 2015 with the ability for SWD to begin transitioning from 1 July 2015.

It is expected that SWDs satisfy requirements that address legal and technical aspects of the solution and develop on-boarding processes for new clients by **31 December 2015**. Additional time will be provided to transition existing clients to the new solution. It is expected that existing clients are transitioned by **31st of March 2016.** The ATO will work with SWDs and assist with transitioning their products and their clients to the new solution.



DRAFT

8. Transition assistance

ATO assistance to support your transition to Cloud Software Authentication & Authorisation

If you would like assistance with your transition to the Cloud Software Authentication & Authorisation solution please contact the ATO Software Industry Liaison Unit (SILU) via email or phone 1300 139 052 . The ATO will assist where possible regarding:

- the on boarding process (e.g. completing the Cloud Software Authentication & Authorisation agreement and setting up your device AUSKey),
- designing your software to requirements, and
- testing and certification processes.

ATO assistance to support your clients

If you would like assistance with transitioning and supporting your clients contact the ATO Software Industry Liaison Unit (SILU) via email or phone 1300 139 052. The ATO will assist where possible regarding:

- tailored processes to transition your clients (e.g. Bulk telephone callouts to nominate your software product with the ATO),
- user interface assistance manuals, and
- ongoing client support through existing channels.

Communications

Communication products/activities will be delivered through existing ATO channels to Australian businesses and Tax Agents. SWDs will continue to be engaged in communication, consultation and co-design activities throughout the detailed design and transition.

Key communication messages to businesses and tax practitioners

- Cloud Software Authentication & Authorisation will allow businesses and registered agents to lodge through their SBR-enabled software providers without an AUSkey
- Businesses and registered agents simply nominate a Software provider through Access Manager (existing administrator AUSkey required) or by calling the ATO (no AUSkey required)
- The nominated software provider uses their Device AUSkey to securely transmit the lodgement to the ATO.
- Software providers will need to meet minimum requirements to on board
- Software providers will not act as intermediaries. Their role is to simply transmit the data securely between their client and the ATO.

Appendix A

Cloud Software Authentication & Authorisation - Detailed Design

(Currently under development)

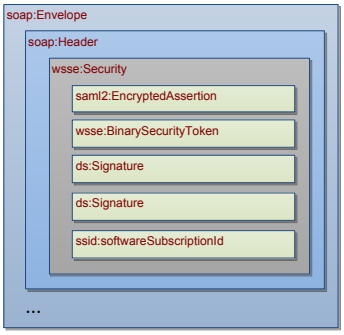
Characteristics of the Software ID

This section is currently under development and will be updated as we work through detailed design.

Passing of the software ID for;

SBR1 (SBR CORE)

The software ID will be passed in the message through an incorporated new element called "softwareSubscriptionId" in the namespace "http://sbr.gov.au/identifier/softwareSubscriptionId". This element is located in the web services security extension (wsse)-security header (see the diagram) and can be added into the message after the message generation process is completed (including singing) and it doesn't break the message integrity or any existing signatures. There will be very little impact on the Reference Client and/or SWDs software packages.



SBR 2 (EBMS)

The software ID will be passed in the soap:Header by using the new ebMS3 custom message property called "SoftwareSubscriptionId". For this purpose the API of the RequestUserMessage class setMessageProperty(String name, String value) of the embeddable client can be used. The method allows adding a new property with the specified value to the generated message. No modifications are required in the Software Developer Kit (SDK) and only SWD will need to modify their software packages.

Error messages returned by SBR as part of Authorisation checks

This section is currently under development and will be updated as we work through detailed design.

Appendix B

Cloud Software Authentication & Authorisation agreement *(DRAFT)*

To allow a business to authorise your dedicated Device AUSkey used for the purposes of securing transmissions/ lodgements to the ATO, you must first send an email to the ATO Software Industry Liaison Unit (SILU) with the heading 'Cloud Software Authentication & Authorisation agreement' containing the following Information:

- written agreement to the meet the Cloud Software Authentication & Authorisation requirements listed in this document,
- your software company's ABN number, and
- contact details.

Appendix C

Setting up your device AUSkey

The steps below outline the process of setting up your Device AUSkey as an Online Lodgement Provider and viewing a list of your clients who have nominated your business to secure transmissions online.

After you have registered SBR licenced Software developer and completed the Cloud Software Authentication & Authorisation agreement (See section 6. On-Boarding process for Software Developers), An ATO operator uses the internal Access Manager version to allocate your permissions as an online software provider. If you have registered for AUSKey in the cloud and you have not been allocated these permissions please contact the ATO Software Industry Liaison Unit (SILU).

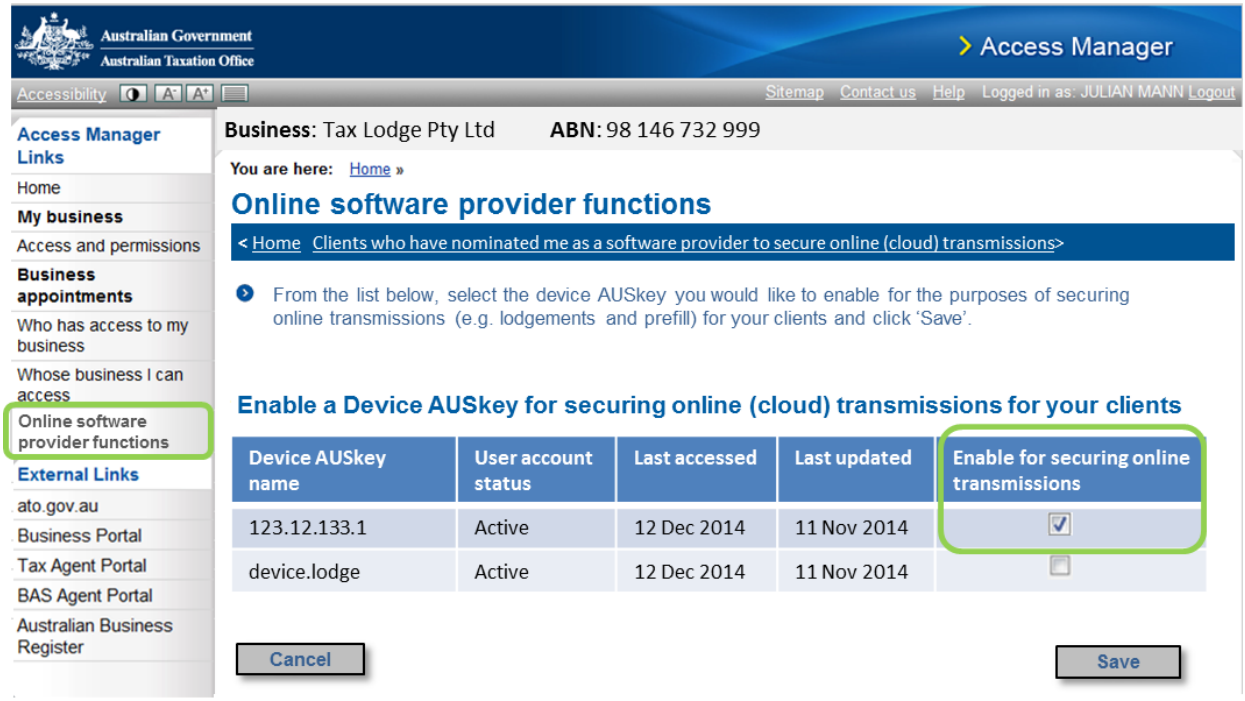
1 Provider enables a Device AUSkey for online (cloud) transmissions

Step 1 of 1 – The provider selects a tick-box next to the Device AUSkey and clicks 'Save'

To enable a Device AUSkey, the software provider will need to;

1. Click on 'Online Software provider functions' in the left hand menu,
2. Select the tick box next to the relevant Device AUSkey and click 'Save'

Note:
The 'Online software provider functions' screen will only be visible to software providers enabled as an 'Online Software Provider' as per ATO internal process described on slide 2



2 Provider views clients or removes a client's nomination

Step 1 of 2 – The provider views clients who have nominated them. The provider removes a client nomination.

To view clients who have nominated the online software provider;

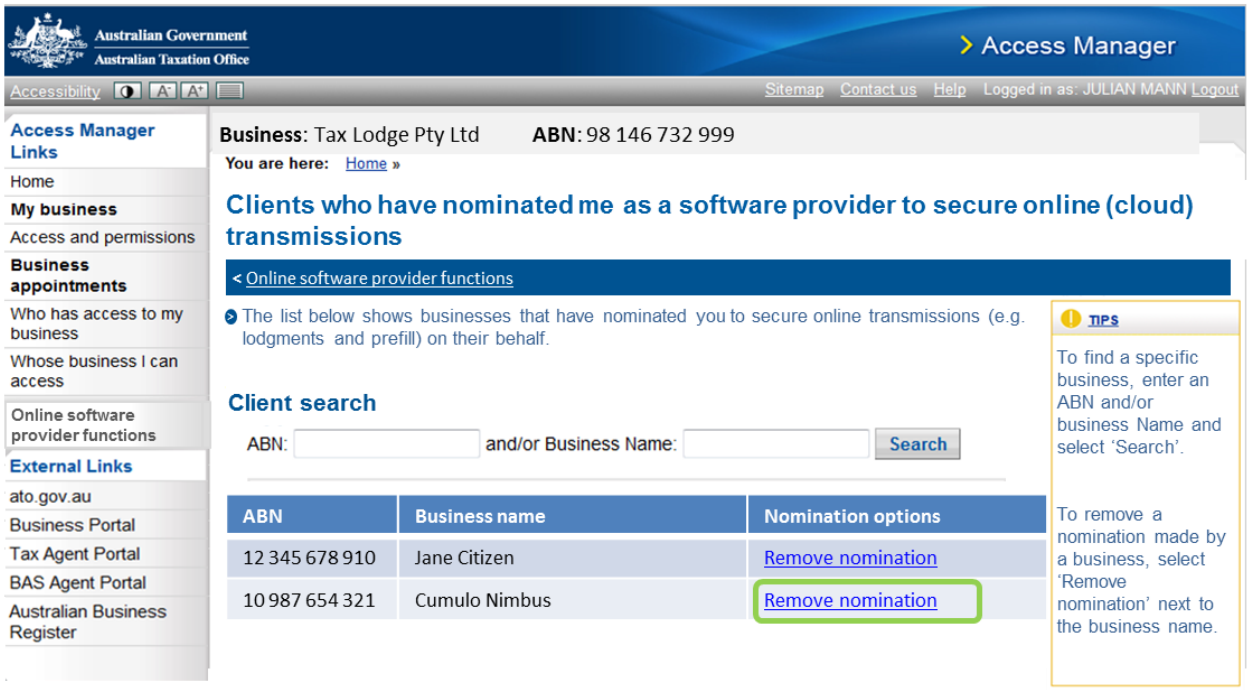
1. Search for clients using the ABN or Business name or scroll through the list.

To Remove a client's nomination;

1. Locate the client either through the search function or by scrolling through the list and
2. Click on 'Remove nomination'

Note:

- The 'Online software provider functions' screen will only be visible to software providers enabled as an 'Online Software Provider' as per the process on slide 2
- Software providers will only be able to view clients that have nominated them

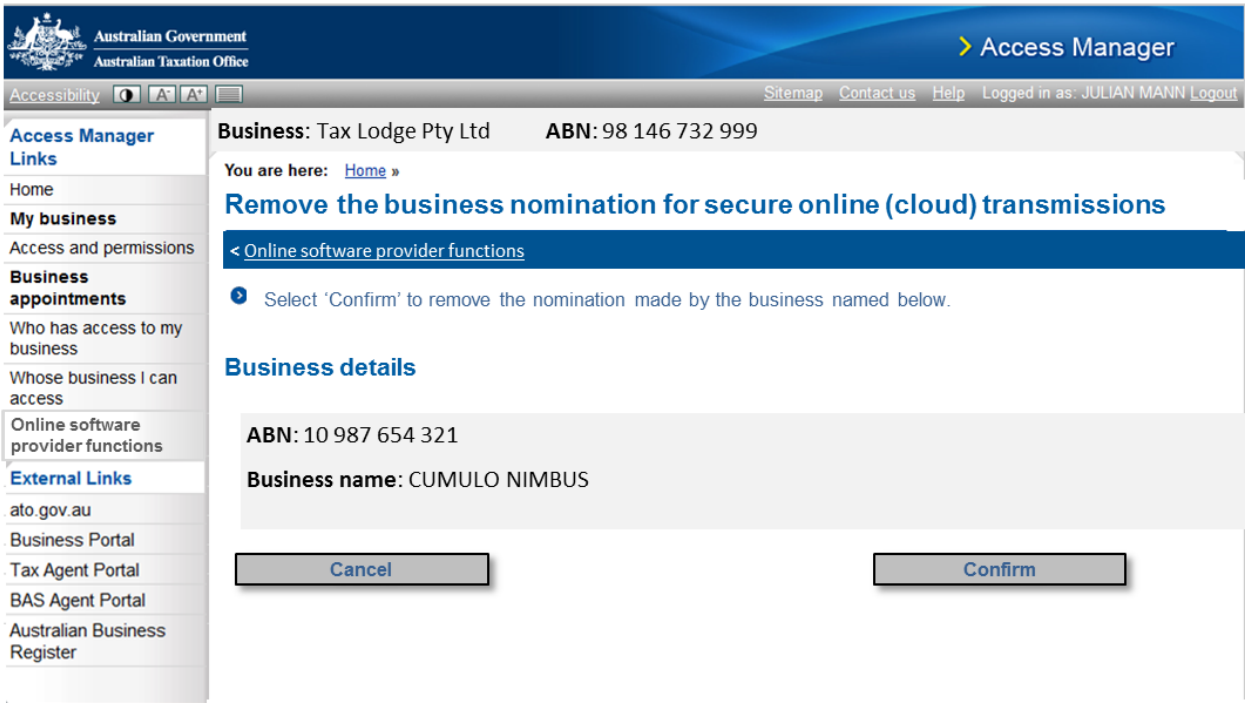


2 Provider views clients or removes a client's nomination

Step 2 of 2 – The provider confirms the nomination removal

1. To confirm the nomination removal, select Confirm .

Note:
The 'Online software provider functions' screen will only be visible to software providers enabled as an 'Online Software Provider' as per ATO internal process described on slide 2



Appendix D

How your client will nominate an Online Software Provider via Access Manager

After an online software product is purchased/subscribed, if a user chooses to use this software to lodge with the ATO, they will be prompted to nominate the SWD with the ATO and present a unique software ID.

'Subscription' – a unique account or single instance of software set up by business for a specific software product

'Software ID' - a unique ID that is used to identify each unique subscription or instance of software

There are two methods in which a business can nominate an Online Software Provider:

- **Online via Access Manager:** an existing administrator AUSkey is required
- **Over the phone:** AUSkey not required.

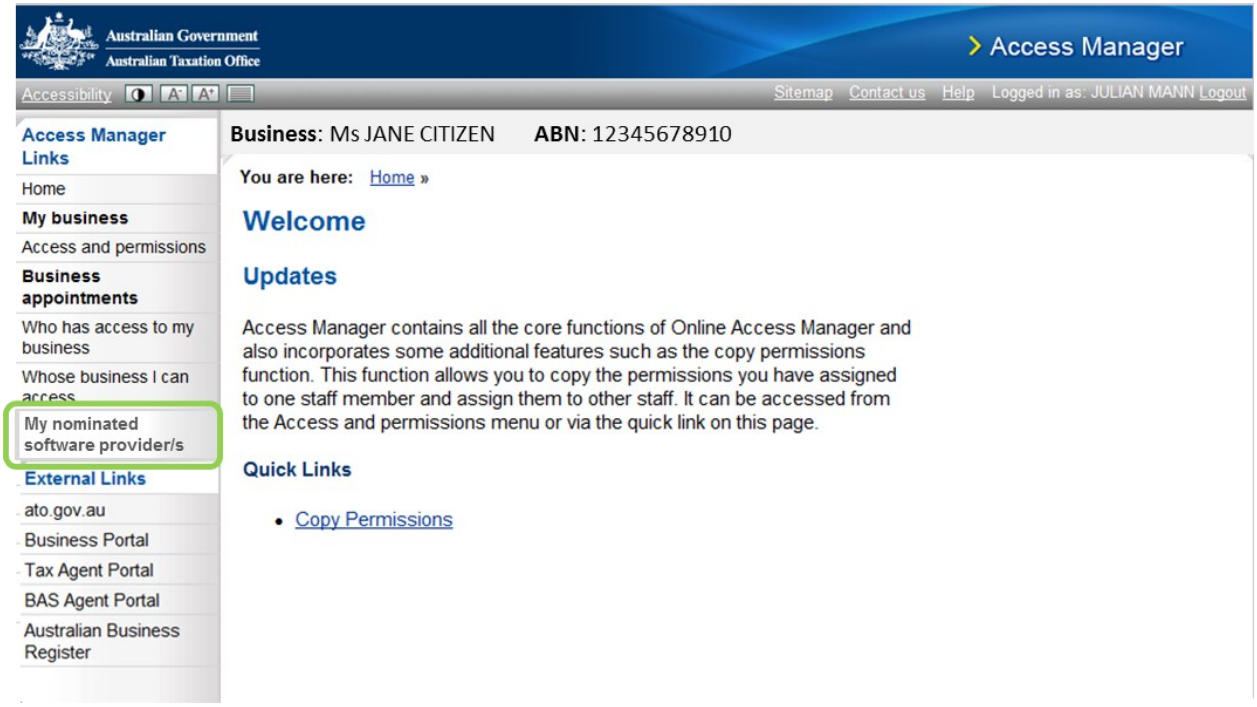
The steps below outline the process in which a business can use their Administrator AUSkey to nominate you as an Online Lodgement Provider through Access Manager.

1 Client nominates a provider

Step 1 of 6– The client logs into AM and selects 'My nominated software provider/s'

To nominate an online software provider, the client;

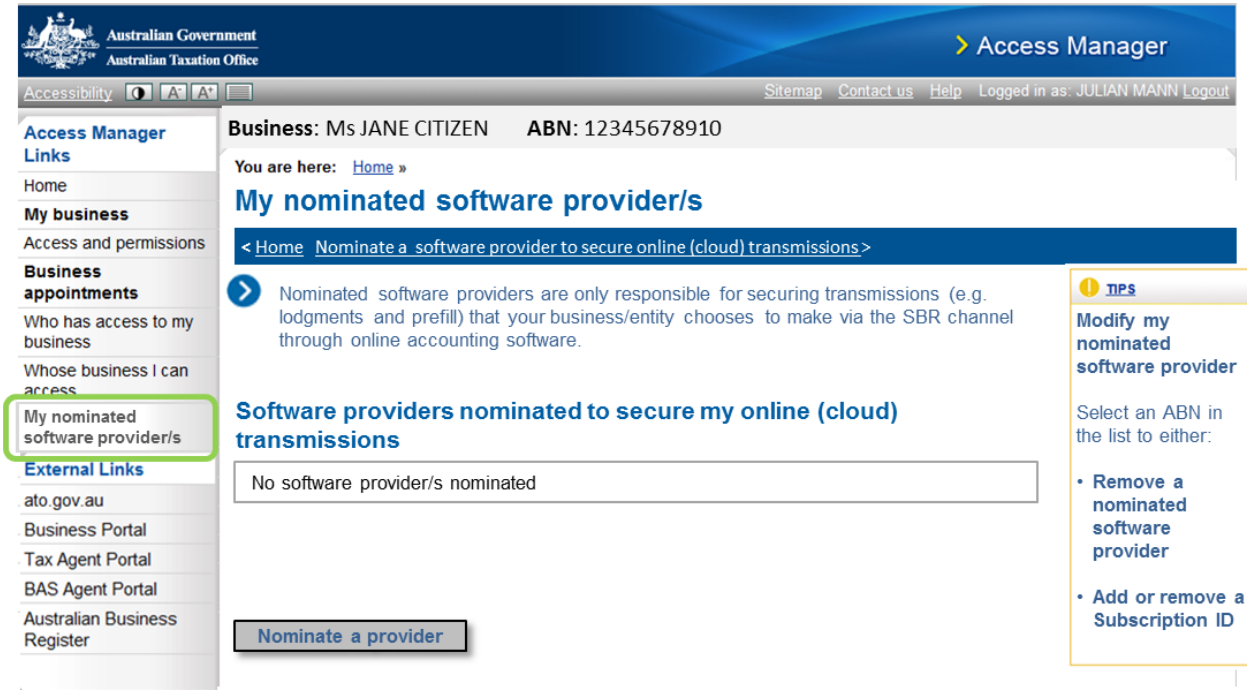
1. Clicks 'My nominated software provider/s' from the left hand menu



1 Client nominates a provider

Step 2 of 6 – Client selects 'Nominate a provider' (The client currently has no provider/s listed)

1. The client clicks 'Nominate a provider'



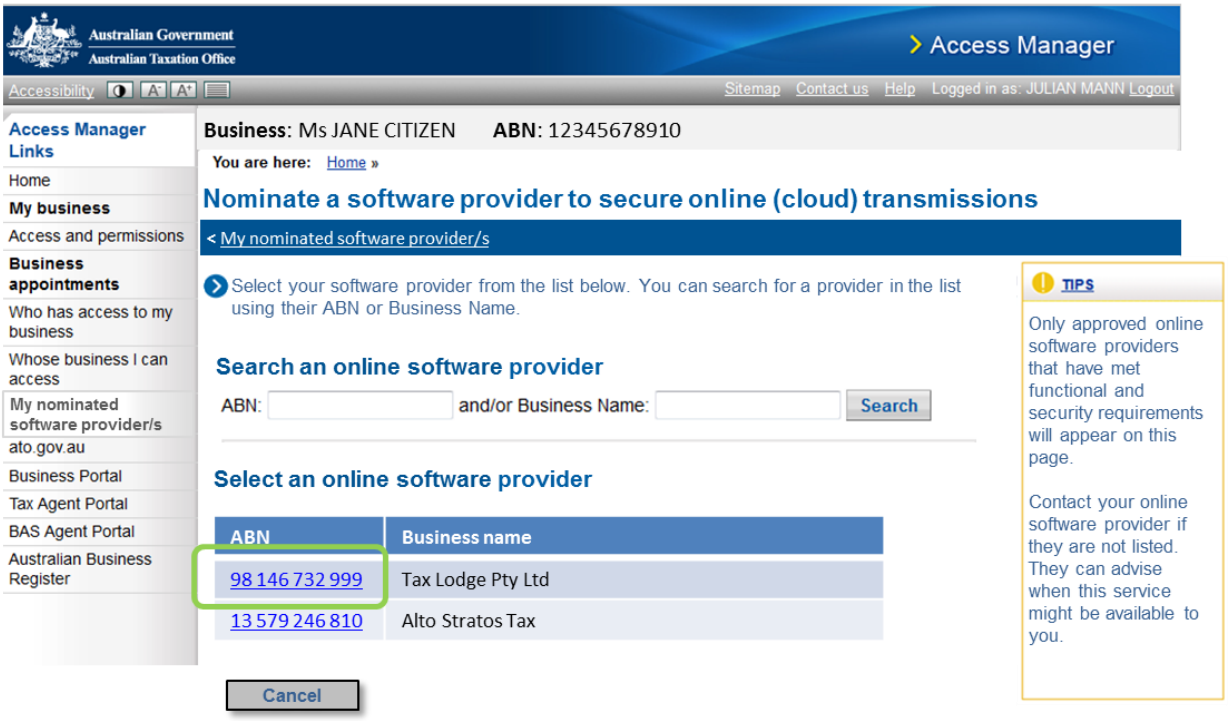
1 Client nominates a provider

Step 3 of 6 – The client searches for and selects an online software provider from the list

1. Scroll or search the list to select an online software provider.
2. Once located, the ABN is clicked to continue with the nomination process.

Note:

List Source - Only approved online software providers will appear in the software provider list below



1 Client nominates a provider

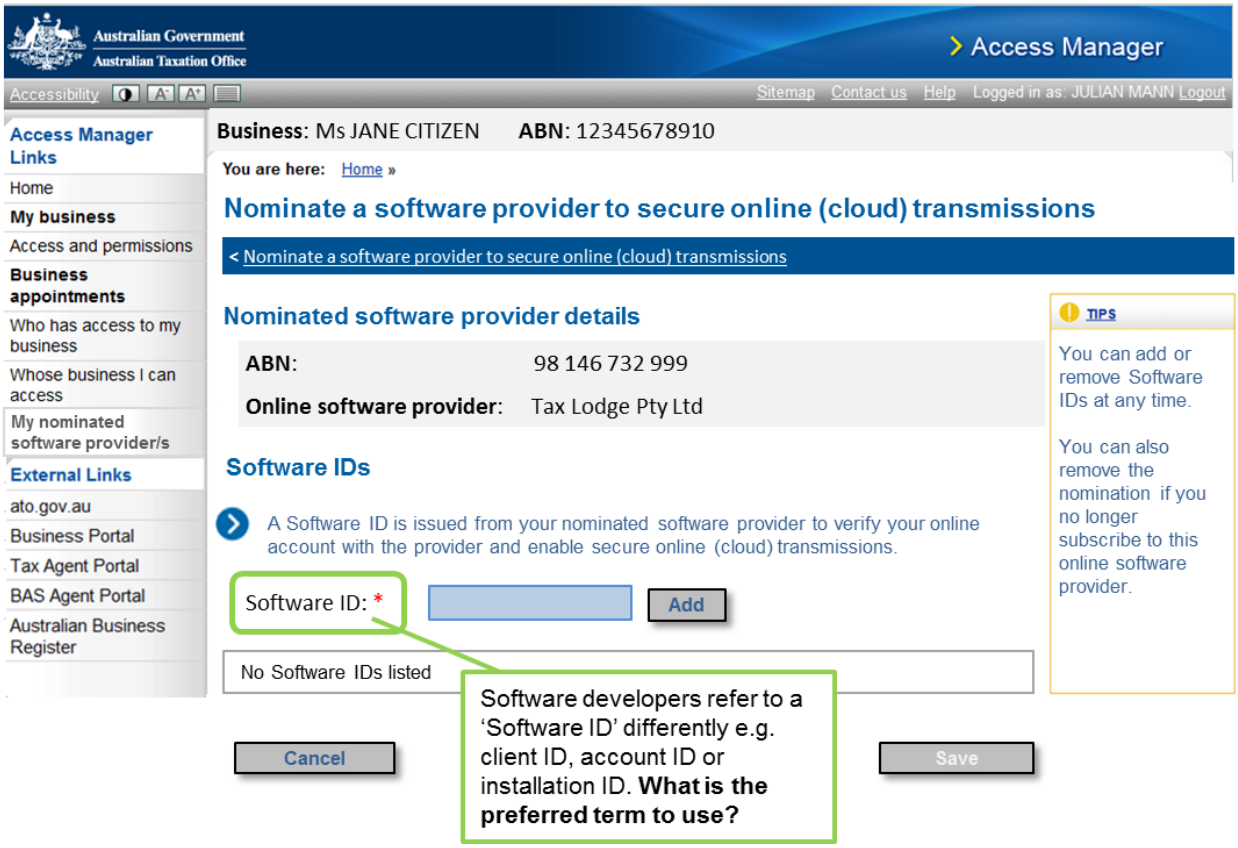
Step 4 of 6 – The client adds one or more Software IDs issued to them by their software provider

The client;

1. Enters the Software ID/s, provided by their online software provider
2. Clicks 'Add'

Note:

- The Software ID is entered as part of the initial nomination process (one-off process). Thereafter, this Software ID is automatically attached with each transmission (e.g. lodgement / prefill) by the software provider.



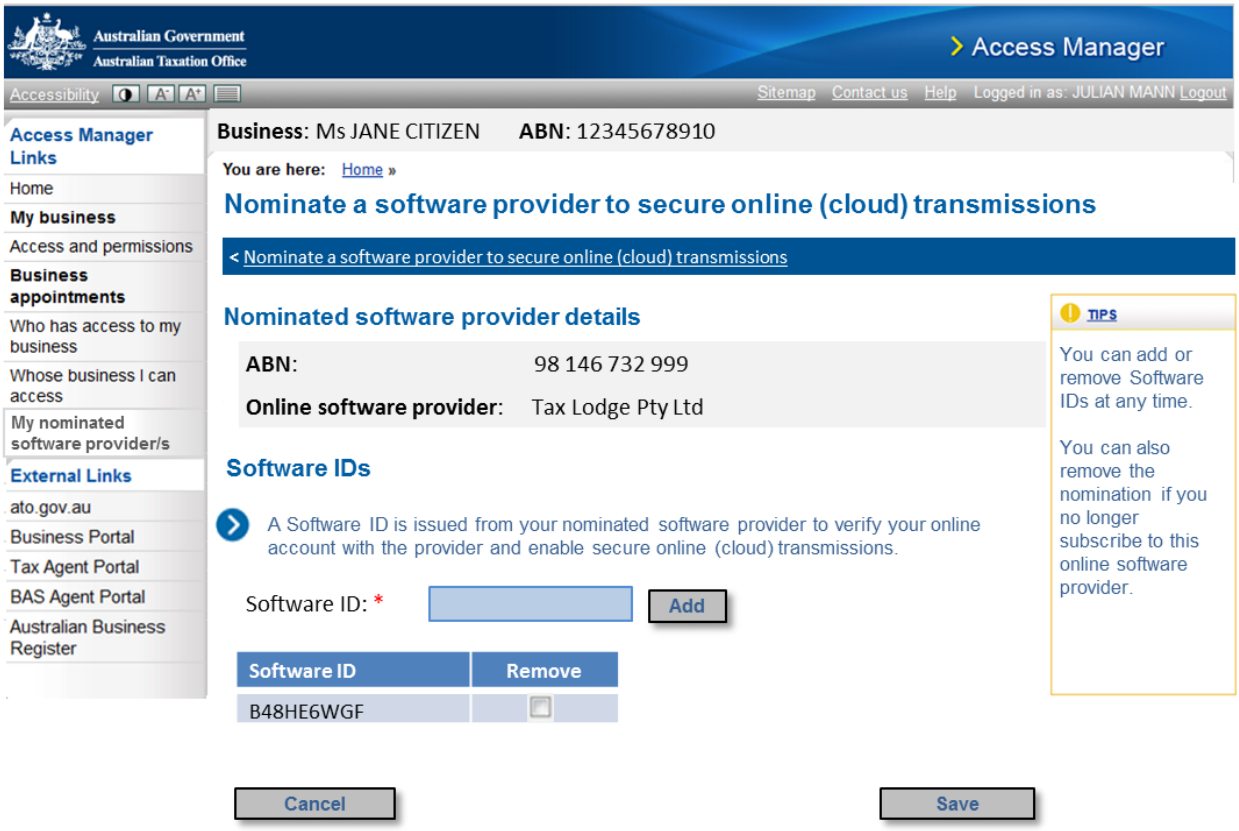
1 Client nominates a provider

Step 4 of 6 (continued) – Once a Subscription ID is added, the save button is activated

The client;

1. Clicks 'Save' button to continue. The 'Save' button will become activate once at least one Software ID has been added.

Note:
- The client is able to enter multiple Software IDs associated with the same ABN
- The client will not be able to proceed with the nomination without adding at least one Software ID

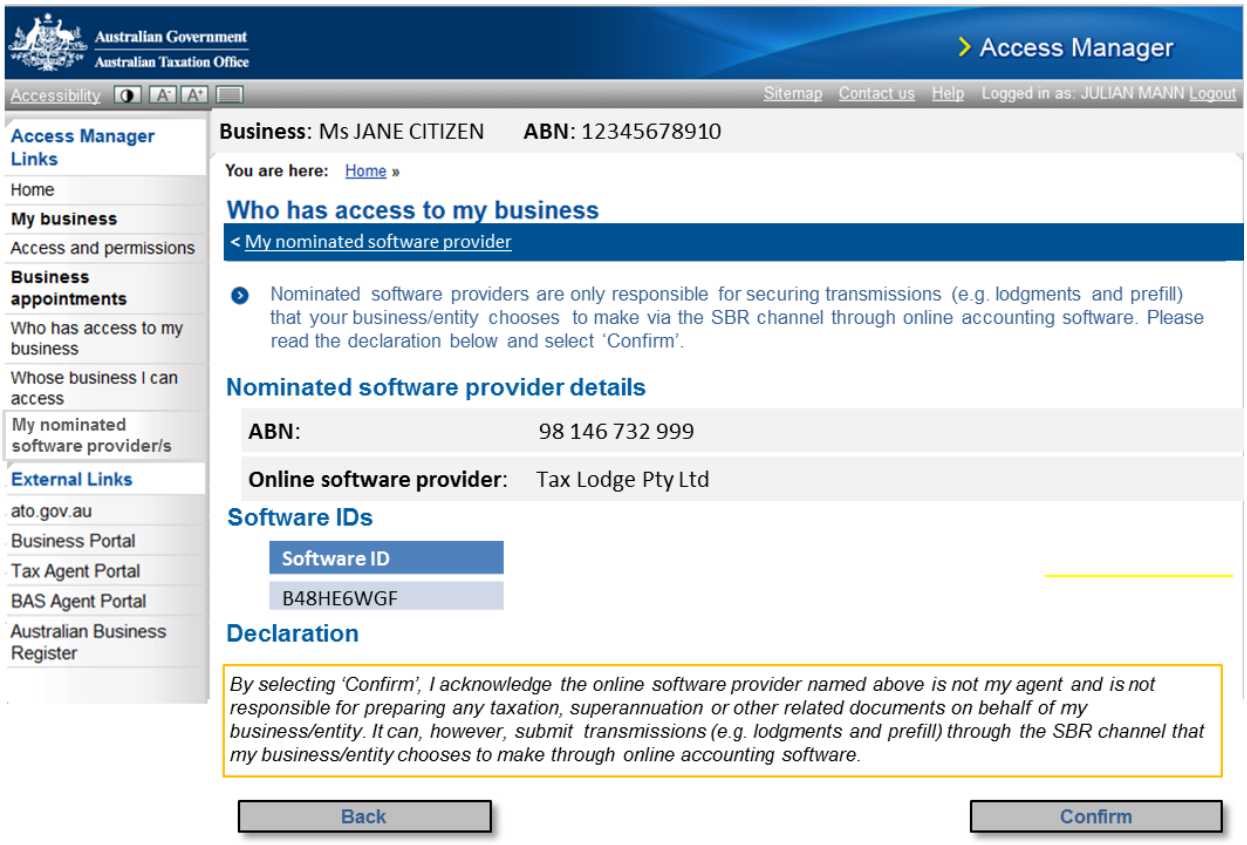


1 Client nominates a provider

Step 5 of 6 – The client confirms the nomination and agrees to the Declaration

The client;

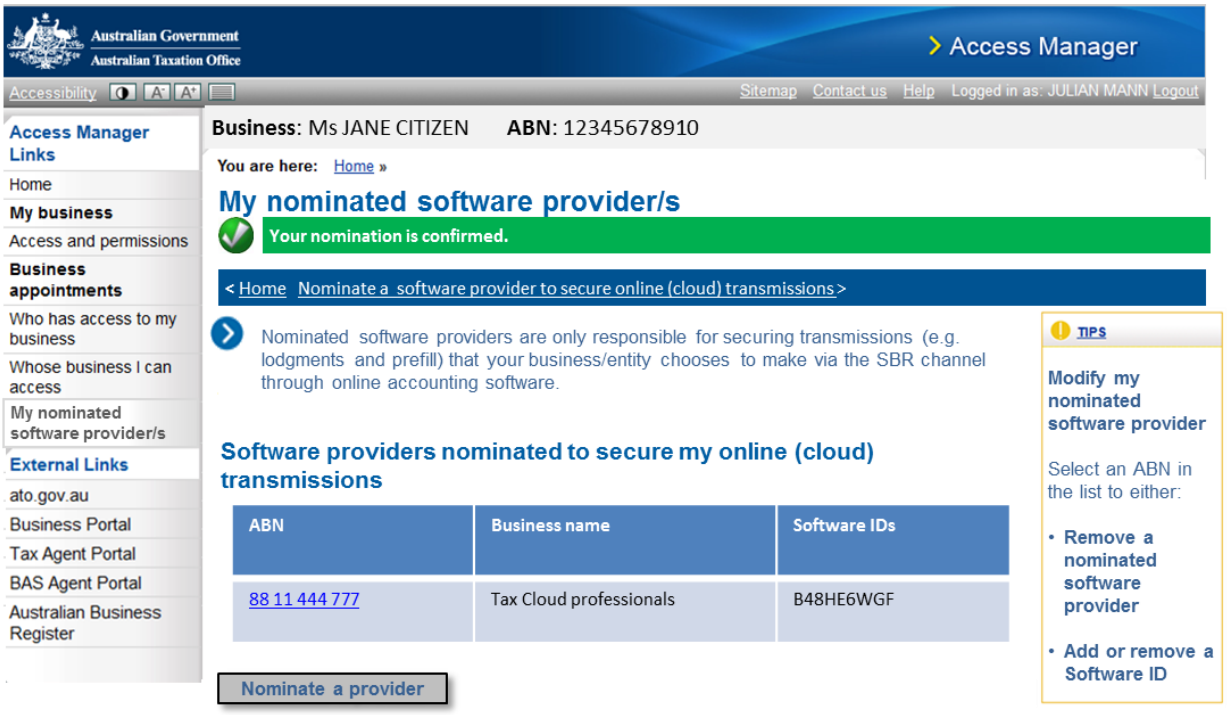
1. Clicks 'Confirm' to acknowledge the role of the online software provider and to finalise the nomination.



1 Client nominates a provider

Step 6 of 6 – Client returns to the list of providers - Nomination confirmed message is displayed

1. A confirmation banner is displayed, and
2. The nominated online software provider listed

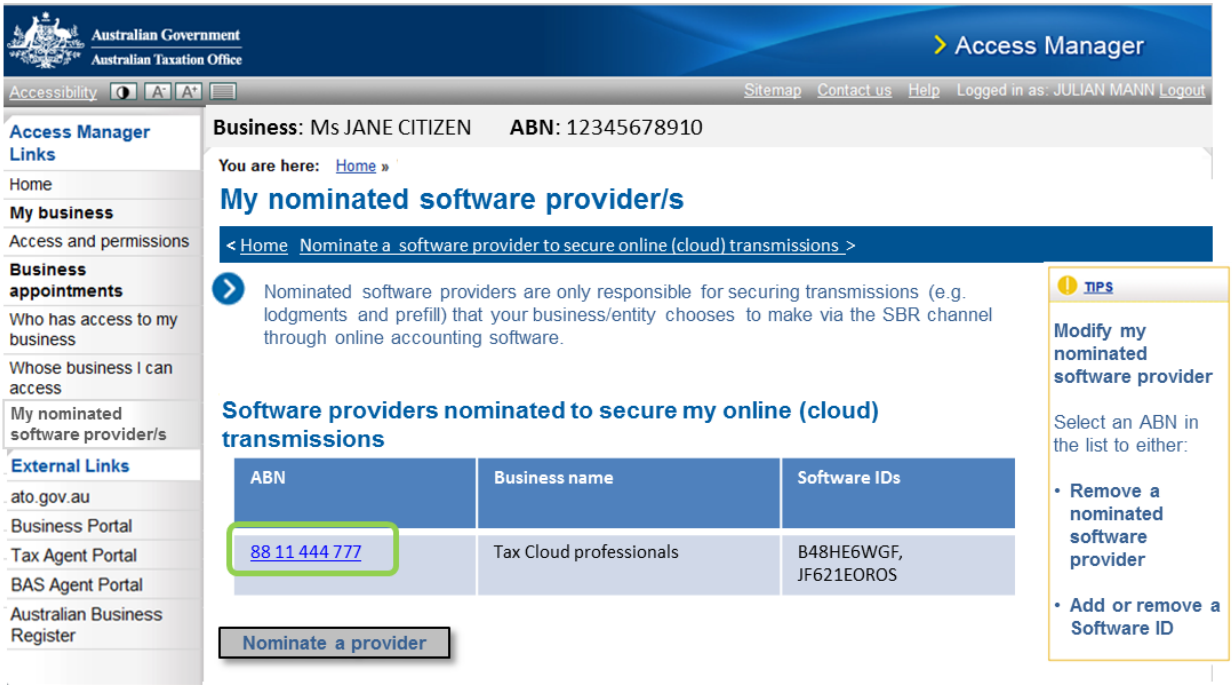


2 Client removes a software provider nomination

Step 1 of 4 – Client selects the nominated provider

To modify or remove a nomination;

1. The client selects the relevant ABN



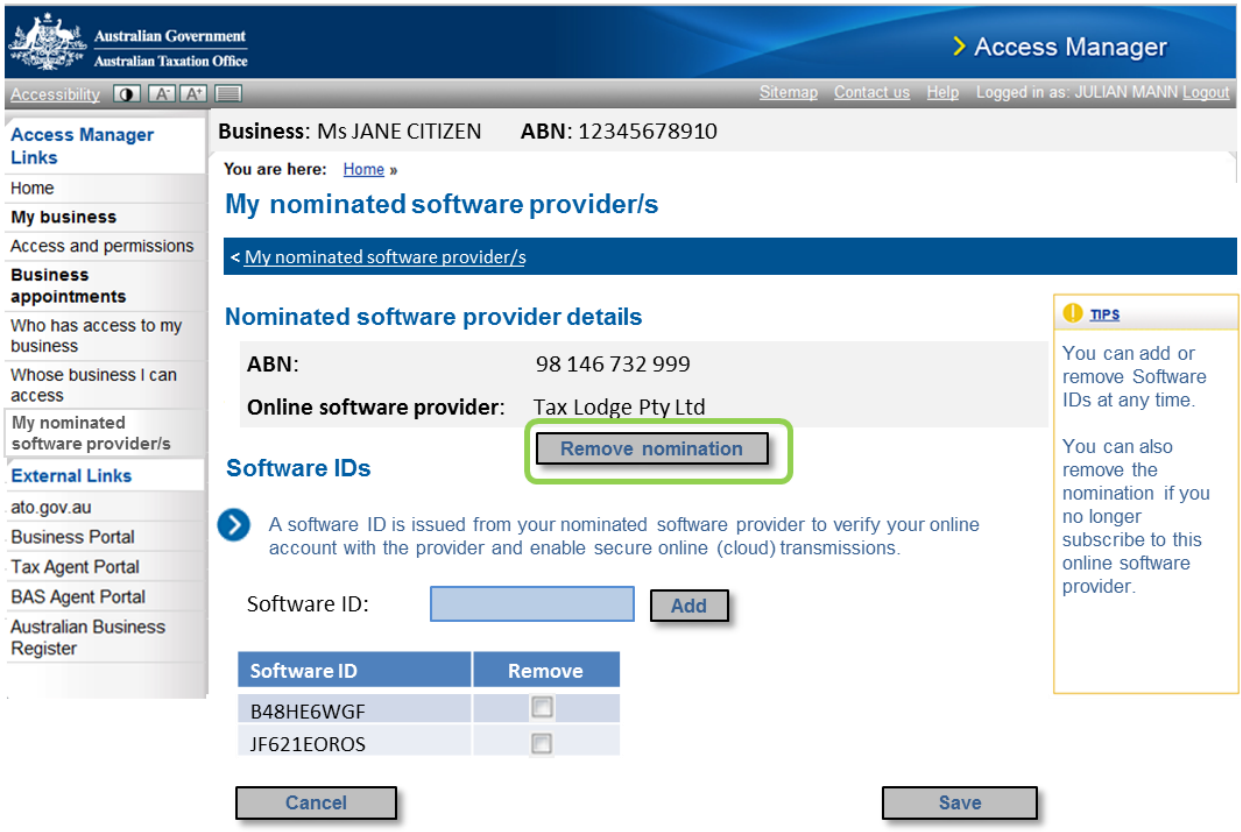
2 Client removes a software provider nomination

Step 2 of 4 – The client can remove the nomination or add/remove a Software ID

To remove an online software provider ;

1.The client must click 'Remove nomination'

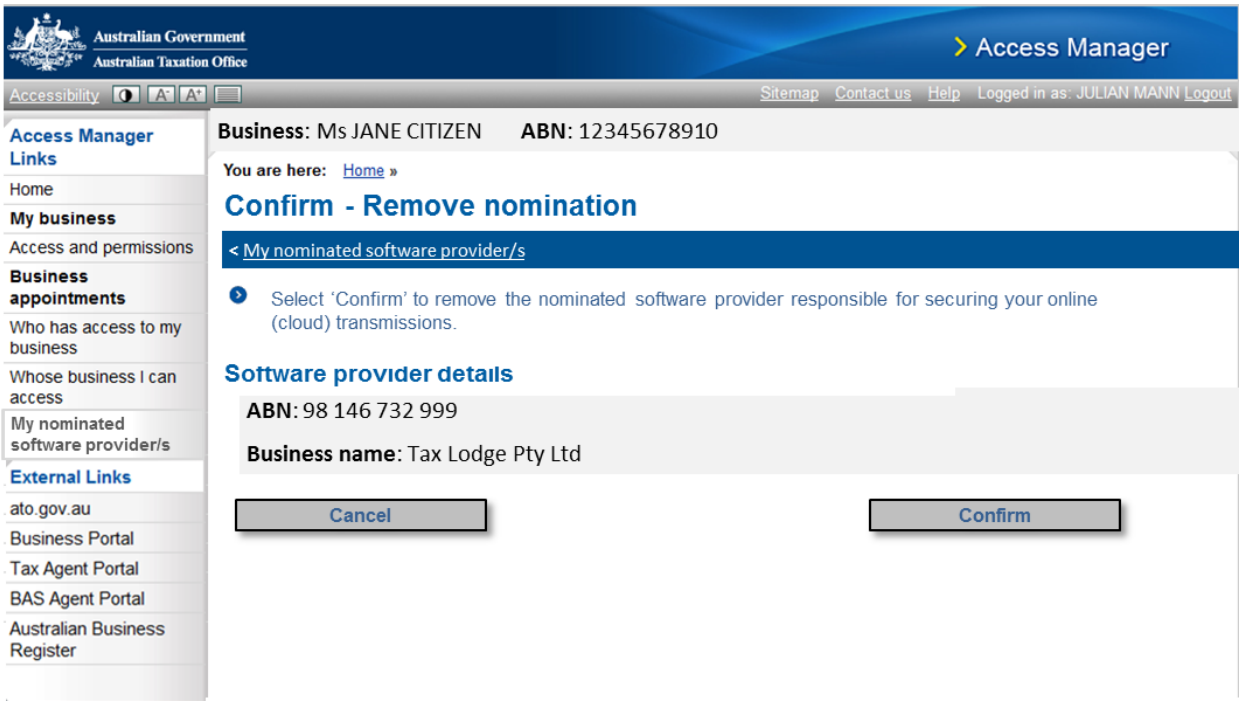
Note:
The client will be able to:
- Remove a software provider nomination entirely (including Software ID/s added
- Remove individual software IDs added as part of the software provider nomination



2 Client removes a software provider nomination

Step 3 of 4 – Client confirms the nomination removal

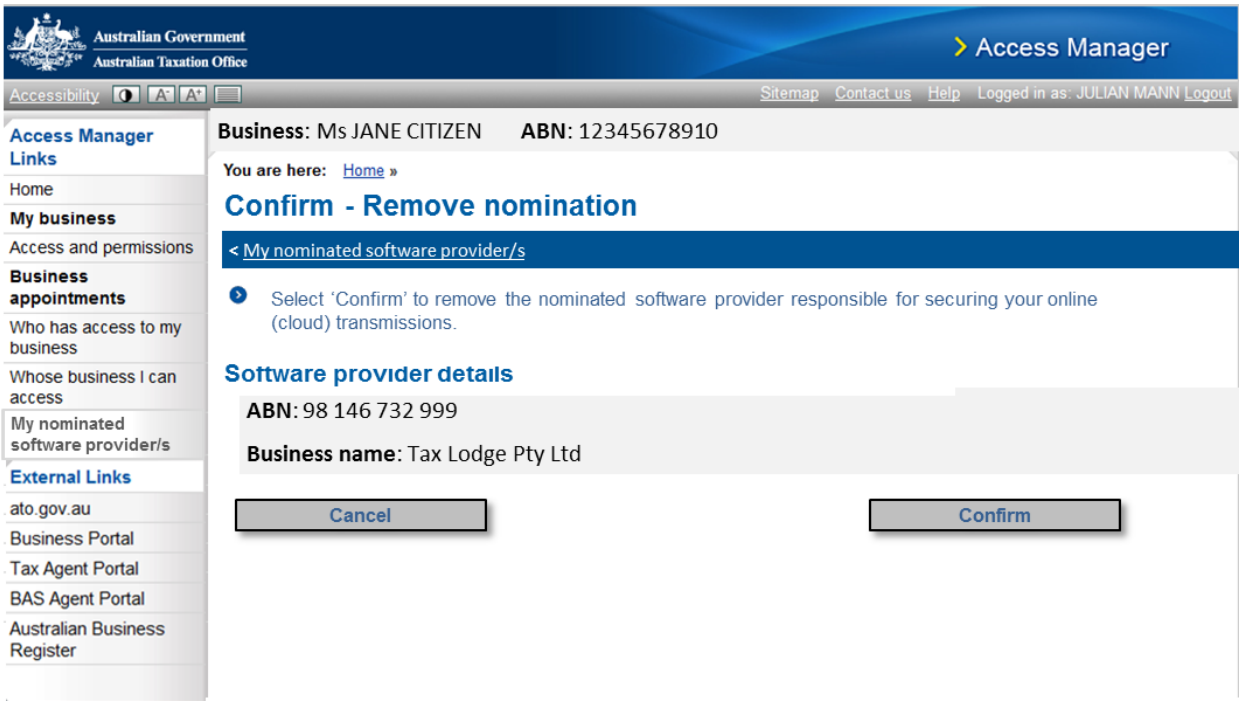
1. To confirm the removal of the nomination, the client clicks 'Confirm'



2 Client removes a software provider nomination

Step 4 of 4 – Nomination removed confirmation message

1. Once removed successfully, the client is returned to the 'My nominated software provider/s' screen and a confirmation banner is displayed

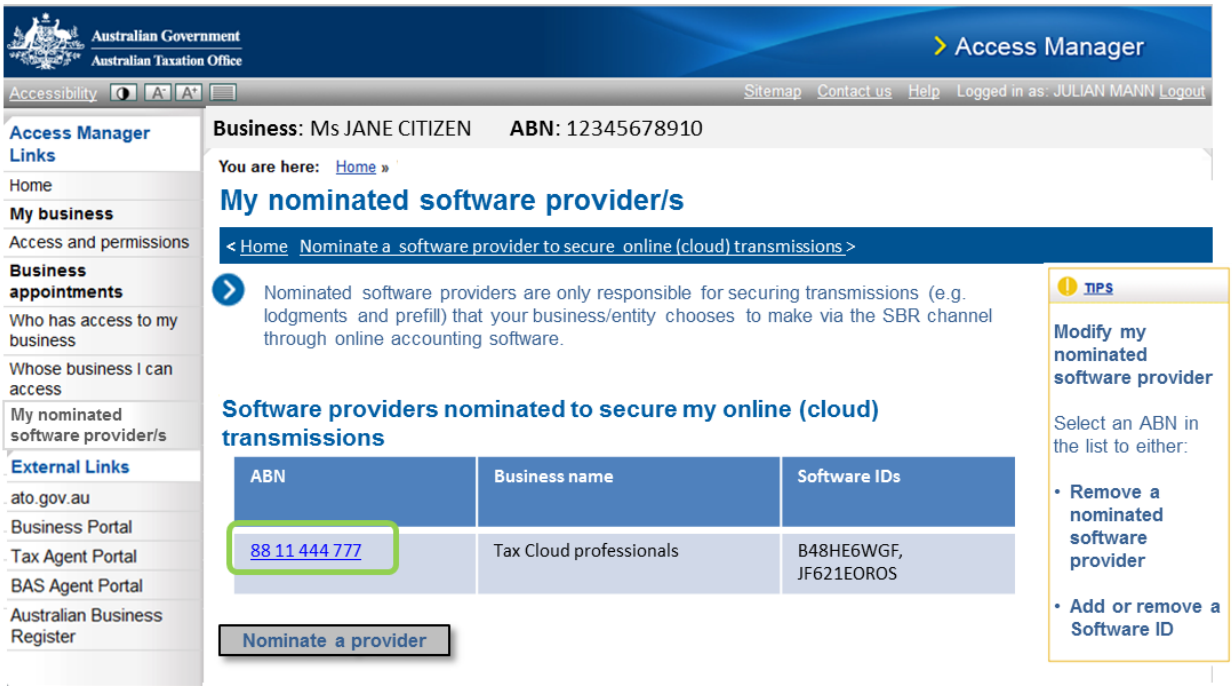


3 Client adds or removes a Software ID from a software provider nomination

Step 1 of 3 – Client selects the nominated software provider

To modify or remove a nomination;

1. The client selects the relevant ABN



3 Client adds or removes a Software ID from a software provider nomination

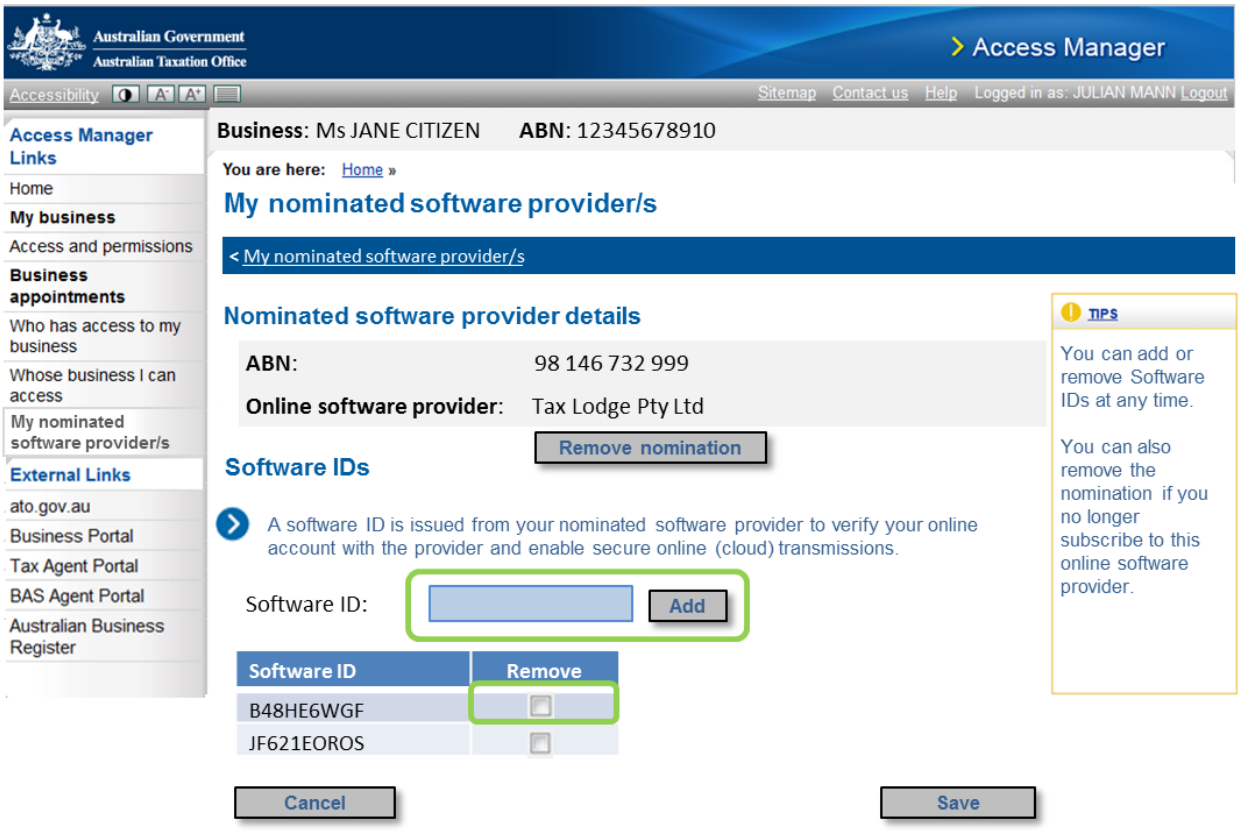
Step 2 of 3 – The client adds or removes a Software ID/s

To add a specific Software ID;

1. The client must enter the Software ID, click 'Add' and
2. Click Save

To remove a specific Software ID;

1. The client must select the remove check box beside the relevant Software ID and
2. Click Save

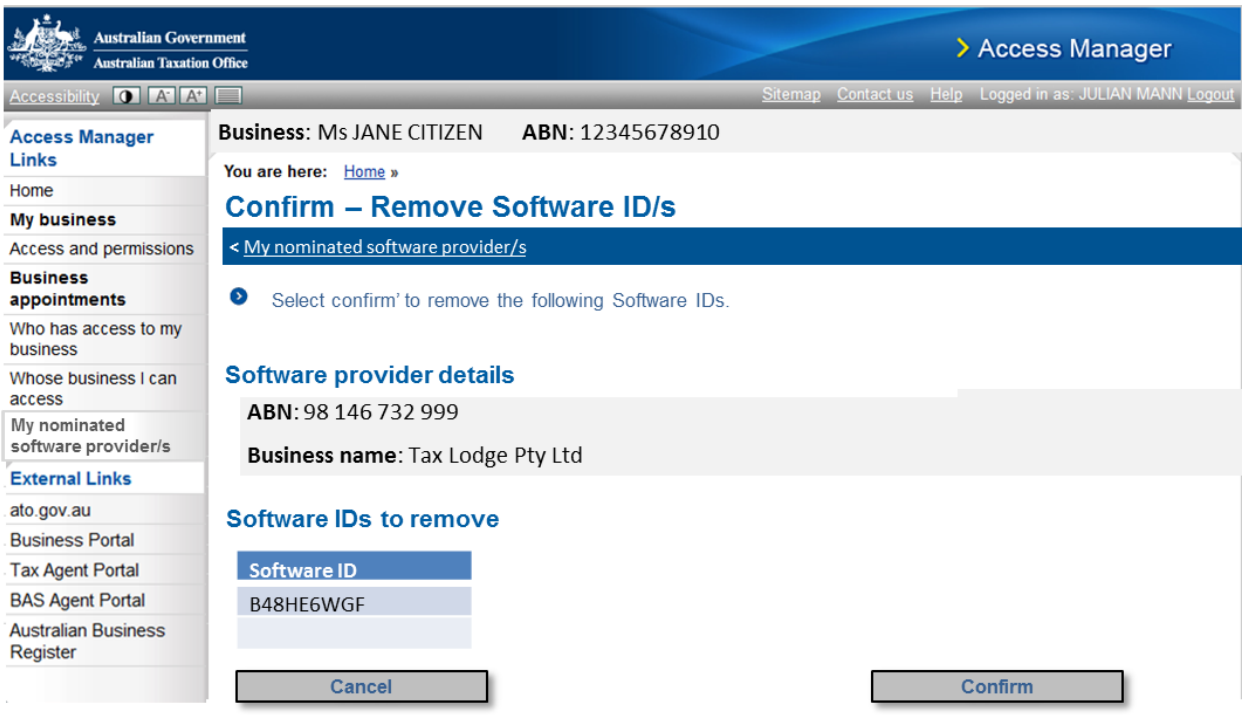


3 Client adds or removes a Software ID from a software provider nomination

Step 3 of 3 – Client confirms the Software ID removal

If the client chooses to remove a Software ID they must

1. Confirm the removal of a Software ID by clicking 'Confirm'



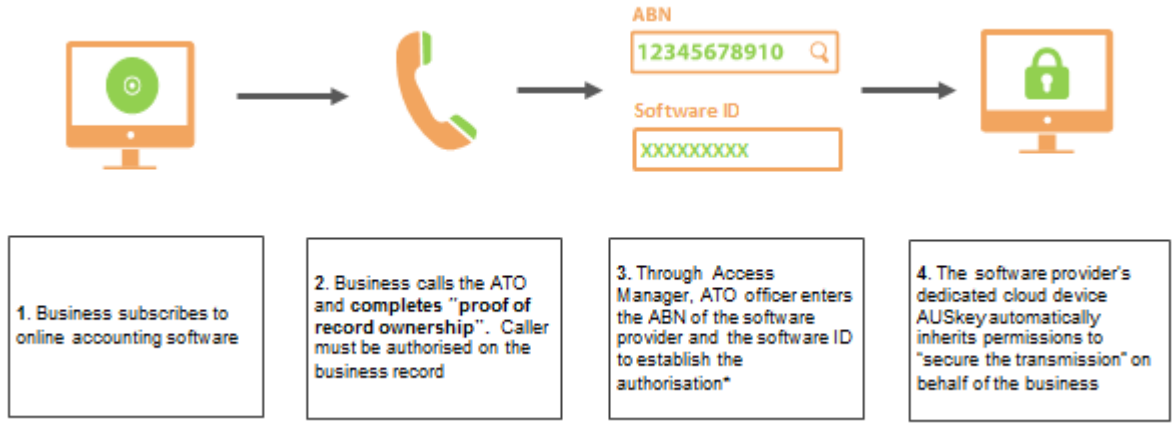
Appendix E

How your client will nominate an Online Software Provider via Phone

Phone (no AUSkey required)

The steps below outline the process for nominating an Online Software Provider over the phone without the need to register for an AUSkey.

1. An authorised business representative calls **1300 AUSkey (1300 287 539)** and selects ***Option x (to be determined)*** from the menu.
2. The ATO officer checks the caller's authorisation on the business record and conducts proof of record ownership.
3. The client recites the software ID and the ABN of the software provider, the ATO officer completes the Online Software Provider nomination request on behalf of the business.



Appendix F

Frequently Asked Questions (FAQ)

Q1. Will the Cloud Software Authentication & Authorisation solution be implemented for the ATO only?

The initial solution is for ATO only. It is intended that this solution will be leveraged for use across government.

Q1. Will desktop software solutions continue to be supported?

Yes. Businesses and intermediaries will still be able to maintain current processes and use existing AUSkey authentication models when using desktop software solutions.

Q2. Will business be permitted to authorise multiple providers?

Yes. Businesses will be able to nominate multiple online software providers.

Q3. Will businesses be able to specify certain permissions for each provider (e.g. BAS for one and not the other)

No. A standard set of permissions will be set when nominating an 'Online Software Provider'. It is up to the business to choose how they use their software product/s.

Q4. Will AUSkeys no longer be required?

The proposed solution will mean an AUSkey will not be required by business to transmit information to the ATO via SBR enabled cloud software. The online software provider will require an AUSkey to authenticate the transmission and AUSkeys will still be suitable for desktop versions of software.

Q5. Can there be multiple users under a single subscription? i.e. Mary Bob and Jane each have their own login under the single subscription.

Yes, potentially one ID for numerous users and / or numerous ABN. This is up to the discretion of software provider.

Q6. When a business owner/employee removes a nomination of software provider from within the ATO, will we notify the software provider?

The ATO will not be providing a service to notify the SWD if a nomination is created or removed. The business and SWD will be informed upon lodgement via error messages if the nomination has been removed.

Q7 How secure is this solution, what if a fraudulent user obtains the software ID?

On lodgement, the software automatically sends the Software ID within the message (Software ID not entered by client). If a fraudulent user obtains the Software ID, they wouldn't be able to enter it into the software. The ATO verification will fail if the ID does not match the nomination.

Q8 Is the Cloud Software Authentication & Authorisation solution for SBR 1 and SBR 2?

Yes, the AUSkey in the cloud solution is for both SBR 1 and SBR 2 channels

Q9. Is the ATO aware that this development will cause SWDs to support two SBR models if dealing with non-ATO organisations (eg SuperStream, other departments)?

Yes. It is intended that in the medium term, the proposed solution will be leveraged for use across government.

Q10. Are SWD in breach of conditions when uploading clients ASUKeys to the cloud?

Advice from the Department of Finance has confirmed that uploading an AUSkey into the cloud is a breach of terms and conditions. However as there are ongoing concerns from SWDs on the interpretation of the policy, an action item was recorded at the last eCommerceTWG (26/02/15) to obtain clarity on this issue.