



Australian Government
Australian Taxation Office

Cloud Software

Authentication & Authorisation (CAA)

(replaces 'AUSkey in the Cloud')

Software developer information kit

Version Control



Australian Government
Australian Taxation Office

	Revision date	Author / modifier	Distributed to	Key changes
0.9	10 March 2015	Scott Gruber	External SWD stakeholders	Appendix-Detailed design AUSKey in the Cloud Solution Appendix -How your client will nominate an Online Lodgement Provider via Access Manager
0.10	20 March 2015	Scott Gruber	Internal ATO project team	Set up and authorisation process Appendix-Detailed design AUSKey in the Cloud Solution Appendix -How your client will nominate an Online Lodgement Provider via Access Manager
0.11	23 March 2015	Scott Gruber	External SWD stakeholders	Set up and authorisation process Transition timeframes timeline Cloud Software Authentication & Authorisation requirements Appendix-Cloud Software Authentication & Authorisation - Detailed Design
0.12	2 April 2015	Scott Gruber	External SWD stakeholders	Executive Summary Policy Advice Set up and authorisation process Cloud Software Authentication & Authorisation requirements Appendix-Detailed design AUSKey in the Cloud Solution
1.0	28 April 2015	Scott Gruber	External SWD stakeholders	Set up and authorisation process Cloud Software Authentication & Authorisation requirements Appendix-Detailed design AUSKey in the Cloud Solution
1.1	21 May 2015	Scott Gruber	External SWD stakeholders	Transition timeframes timeline
1.2	27 July 2015	Scott Gruber	External SWD stakeholders	Set up and authorisation process Transition timeframes Appendix - Setting up your Device AUSKey for online (cloud) transmissions Appendix - Provider views clients, nomination details and disable a nomination Appendix - How your client will nominate you as an Online Software Provider Appendix - CAA Steps to verify transmissions
1.3	19 October 2015	Scott Gruber	External SWD stakeholders	Set up and authorisation process Transition timeframes Appendix - CAA - Detailed Design Appendix - Setting up your Device AUSKey for online (cloud) transmissions Appendix - How cloud transmissions are verified Appendix - Lodgement scenarios Appendix - Online Software Provider Appointment Web Service
1.4	5 November 2015	Scott Gruber	External SWD stakeholders	Appendix - Frequently Asked Questions (FAQ)
1.5	10 December 2015	Scott Gruber	External SWD stakeholders	Appendix - Setting up your Device AUSKey for online (cloud) transmissions Appendix - Provider views clients, nomination details and disable a nomination Appendix - How your client will nominate you as an Online Software Provider
1.6	7 March 2016	Scott Gruber	External SWD stakeholders	Appendix - Hybrid desktop via cloud software Change of term 'nominate' to 'notify'



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 [CAA requirements](#)
- 8 [Transition timeframes](#)
- 9 [Transition assistance](#)

[Appendix A - CAA - Detailed Design](#)

[Appendix B - Selecting a Device AUSkey to use for hosted SBR services](#)

[Appendix C - Provider views clients, notification details and can disable a notification](#)

[Appendix D - How your client will notify the ATO of your software services](#)

[Appendix E - How cloud transmissions are verified](#)

[Appendix F - Lodgement scenarios](#)

[Appendix G - Online Software Provider Appointment Web Service](#)

[Appendix H - Hybrid desktop via cloud software](#)

[Appendix I - Frequently Asked Questions \(FAQ\)](#)



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 (eg WofG authorisation and Single Touch Payroll).

The ATO will implement changes to support a Cloud Software Authentication & Authorisation (CAA) 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 notify the ATO of a software providers services, for the purposes of using the software provider device AUSKey to secure 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.

SWD can begin transitioning from the deployment date for the CAA solution (initially for ATO lodgements only), 24 July 2015 for SBR1 deployment and 5 August 2015 for SBR 2 deployment.

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 **31 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 SBR Service Desk by email at sbrservicedesk@sbr.gov.au or by phone on 1300 488 231.



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 (eg 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 in the cloud 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.

The Department of Finance (as the Gatekeeper Competent Authority) have assessed the proposed 'CAA' solution (outlined in this document) and determined that it is compliant with the terms and conditions of the AUSkey Certification Practices Statement (CPS) and Certificate Policies (CP).

Responsibilities in relation to the AUSkey Standard Certificate

<p>4.1</p> <p>The Certificate Holder and the Business must not:</p> <ul style="list-style-type: none">disclose the password for the AUSkey Standard Certificate to any other personstore the AUSkey Standard Certificate in a keystore to which any other person has accessotherwise allow, grant, permit or enable any person other than the Certificate Holder to use the AUSkey Standard Certificate.	<p>There is no definition of 'person' in the policy.</p> <p>We have received legal advice stating that 'person' includes computers, systems and software.</p>
<p>4.2</p> <p>The Certificate Holder and the Business must promptly advise the ABR CA if:</p> <ul style="list-style-type: none">the Certificate Holder is no longer authorised to use the AUSkey Standard Certificate on the Business' behalfit becomes aware of any unauthorised use of the AUSkey Standard Certificatethe security of the AUSkey Standard Certificate or its password has been compromised.	<p>There is no definition of 'compromised' in the policy.</p> <p>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 (ie uploading to any form of cloud storage) , constitutes a breach of the terms and conditions.</p>



Responsibilities in relation to the AUSKey Device Certificate

<p>4.1.1 Who can submit an application for a Device Certificate?</p> <p>An application for an AUSKey Device Certificate (to be held for a Business Entity):</p> <ul style="list-style-type: none">• 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 <i>who holds a valid AUSkey Standard Certificate</i> (for that same Business Entity) as the Device Custodian to be associated with that Device Certificate.	<p>Device custodians must hold pre-existing Standard AUSKeys for the business, thus typically aren't the Cloud provider.</p> <p>The Device Custodian creates the password, which cannot be disclosed to any other <i>'person'</i> (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.</p>
<p>4.4.1 Device Custodian responsibilities</p> <p>The Device Custodian for an AUSKey Device Certificate is responsible for:</p> <ul style="list-style-type: none">• 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 <i>attached to the correct Device</i>, 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:<ul style="list-style-type: none">• 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• <i>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.</i>	<p>The Device AUSKey conditions-of-use do not expressly forbid Cloud use, however given the definition of <i>'compromised'</i> (as per previous slide) Device Custodians cannot send the Device AUSKey across the internet, or by any other comparable means. Cloud providers aren't allowed to have the password 'disclosed' to them, their systems or software.</p>



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.financegov.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 Computings.

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 (eg 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 infrastructure¹⁰. The applications are accessible from various client devices through either a thin client interface, such as a web browser (eg 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 (eg host firewalls).*

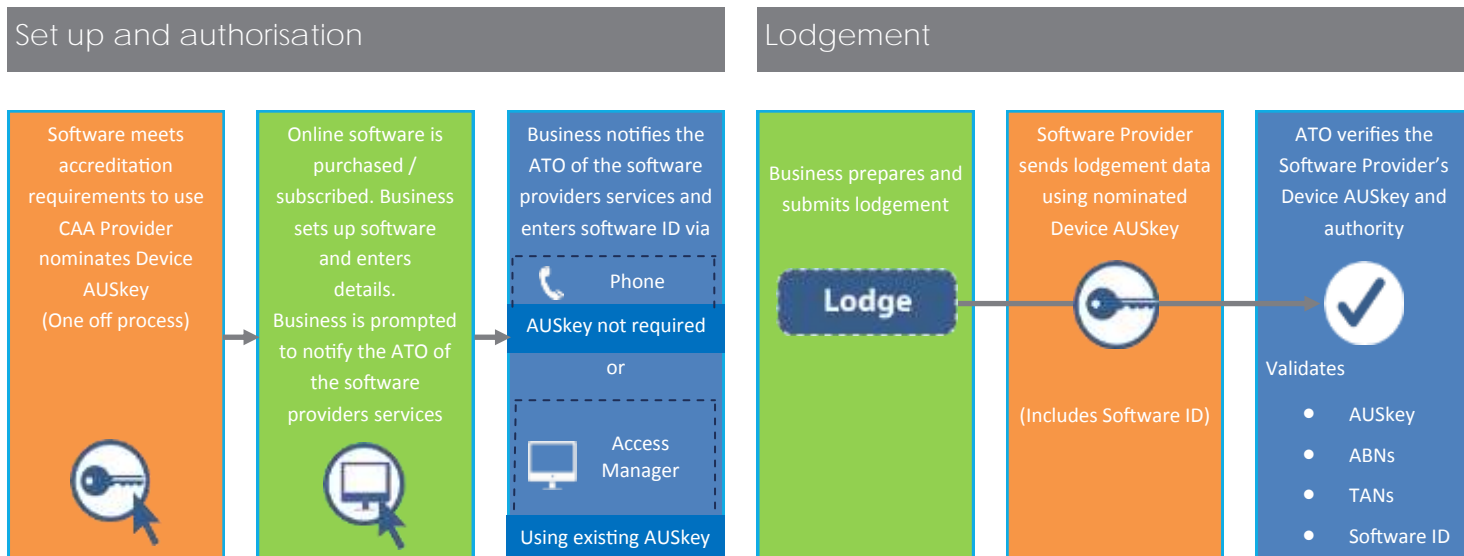


5. High Level Solution

The proposed CAA 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 CAA
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 (eg 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.



[Appendix E. CAA - Steps to verify transmissions - Link to page section](#)

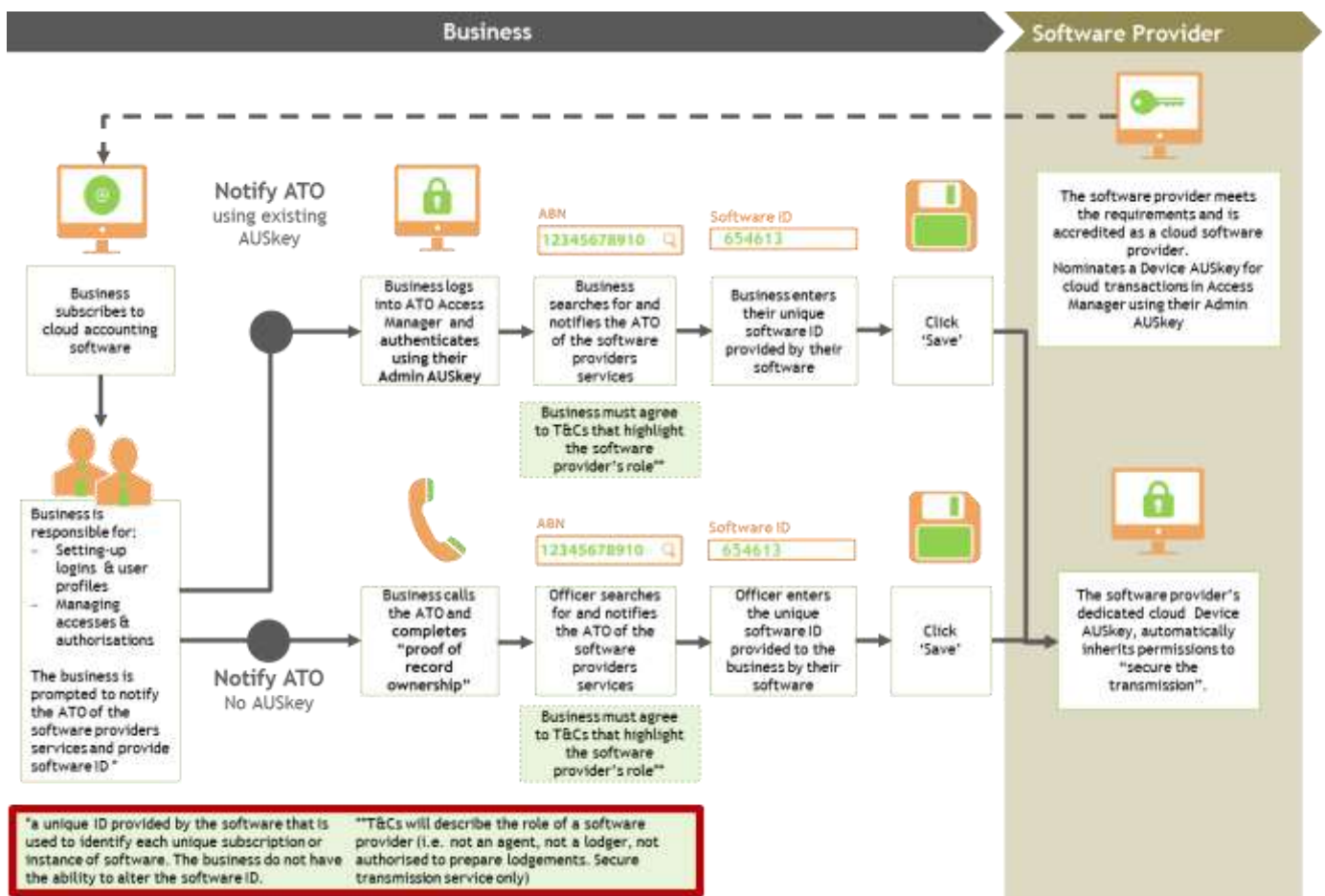
¹'SoftwareID' is a unique ID that is used to identify each unique subscription or instance of software and is automatically generated by the software. See [Appendix A. CAA - Detailed Design - Link to page section](#)



Benefits of the CAA solution

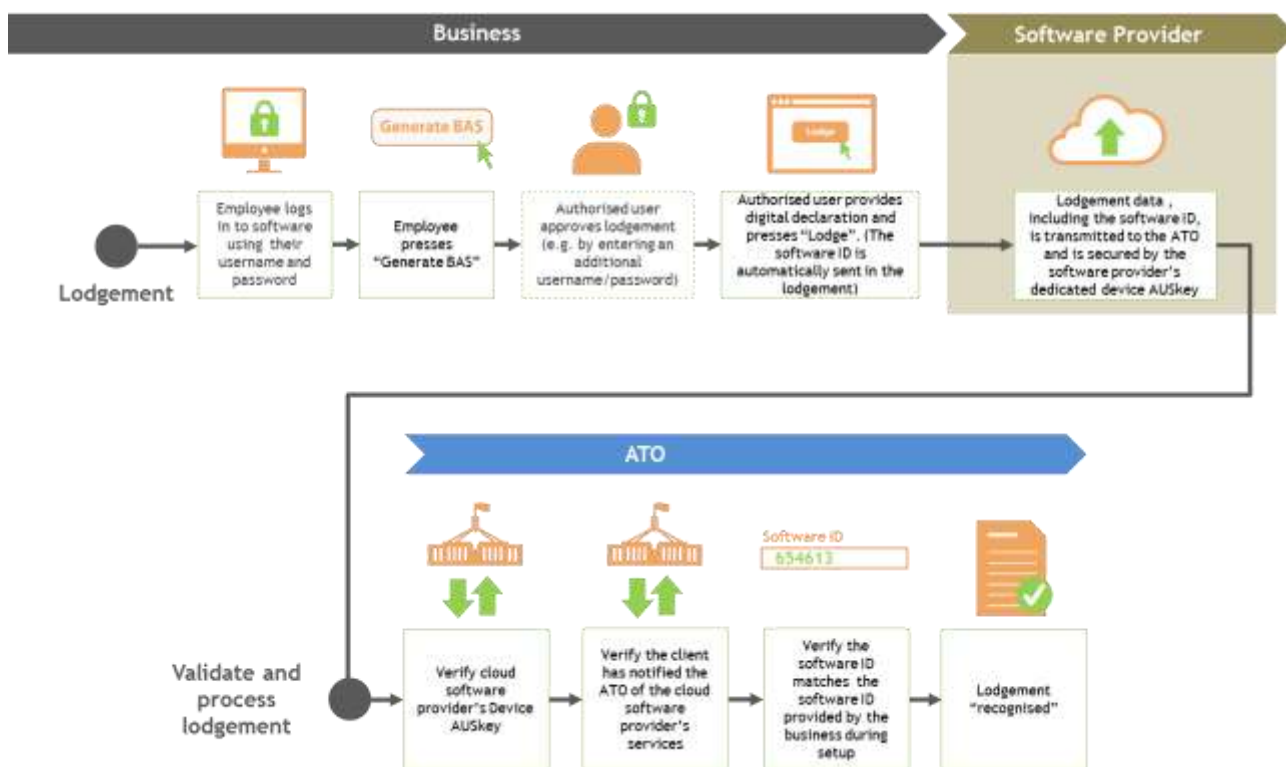
- Simplified on-boarding process for the business client offering them choice during transition/on-boarding on how to notify the ATO of a cloud software providers services
- Businesses do not need to register for and obtain an AUSKey in order to authorise a Software Provider and transact in cloud, maximising 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
- Compliant with current AUSKey terms and conditions of use

Business notifies the ATO of an online software providers services

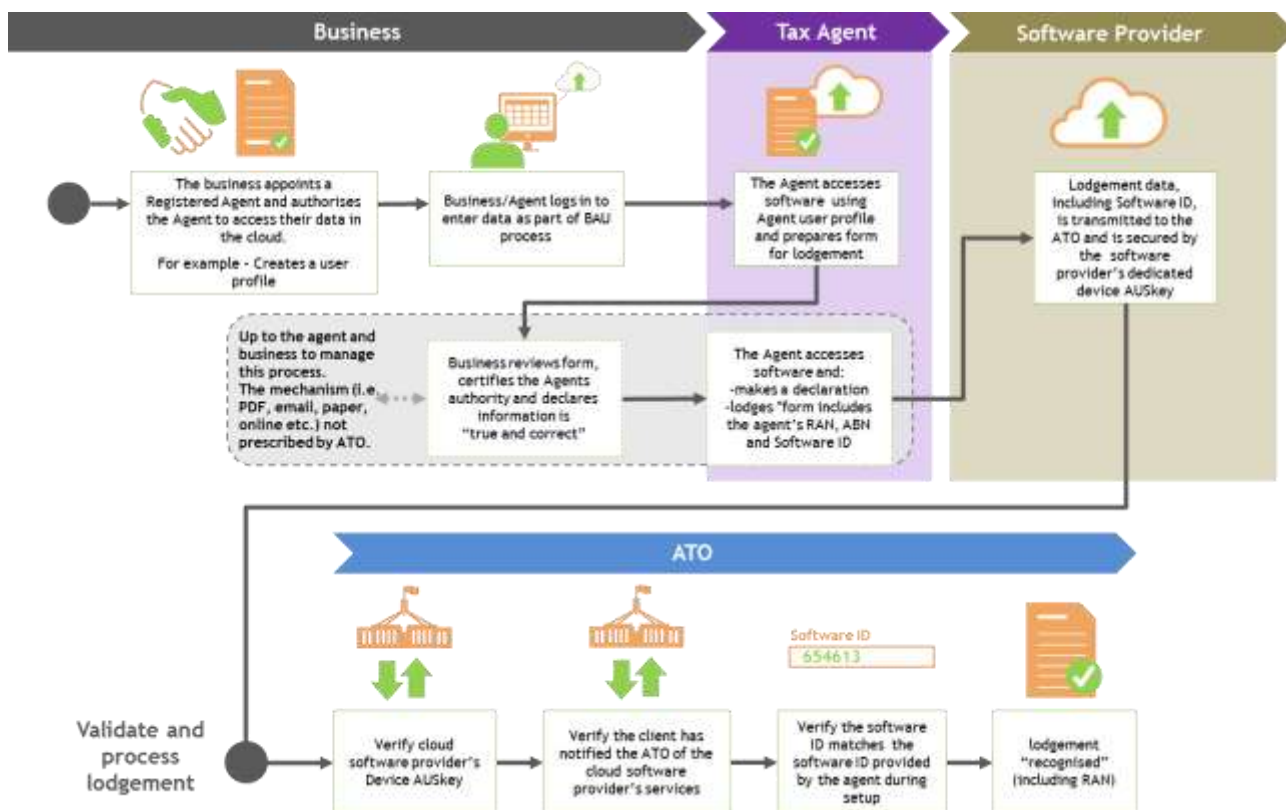




Lodgement by "business" using cloud software



Lodgement by Registered Agent in the cloud





6. Set up and authorisation process

To provide services using the CAA solution, software developers will be required to complete the following steps to on-board. The steps below also outline what your client is required to do to on-board.

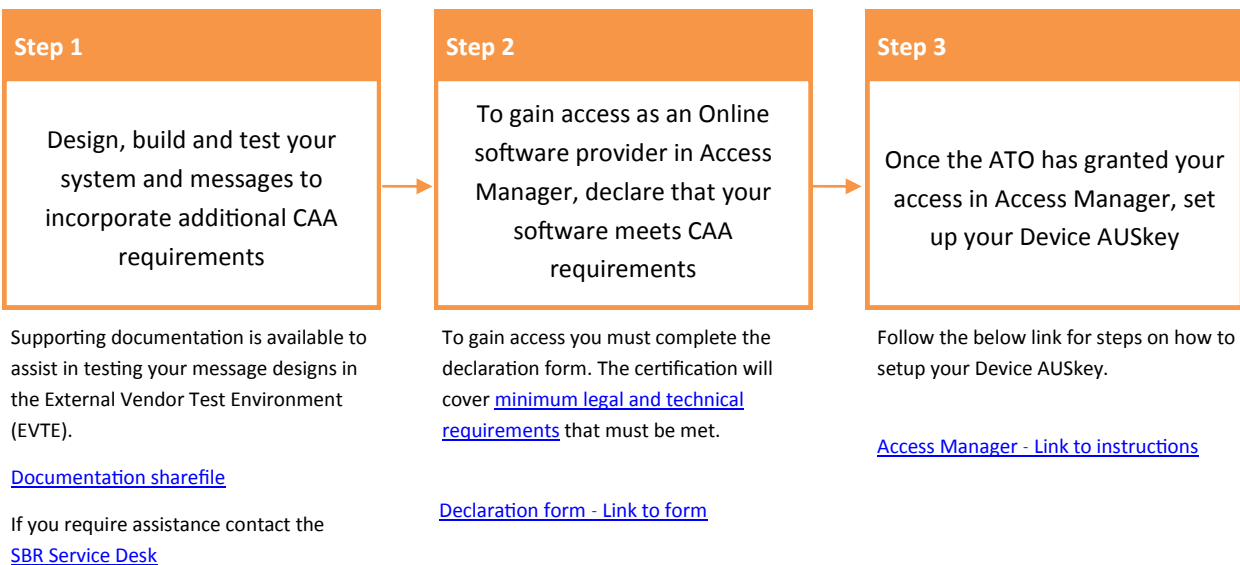
Please note, to be able to secure transmissions through the SBR channel you will also be required to follow the current process and:

- register as a SBR licenced SWD, and
- assess, test and certify your message designs against the current (SBR 1 and SBR 2) certification process.

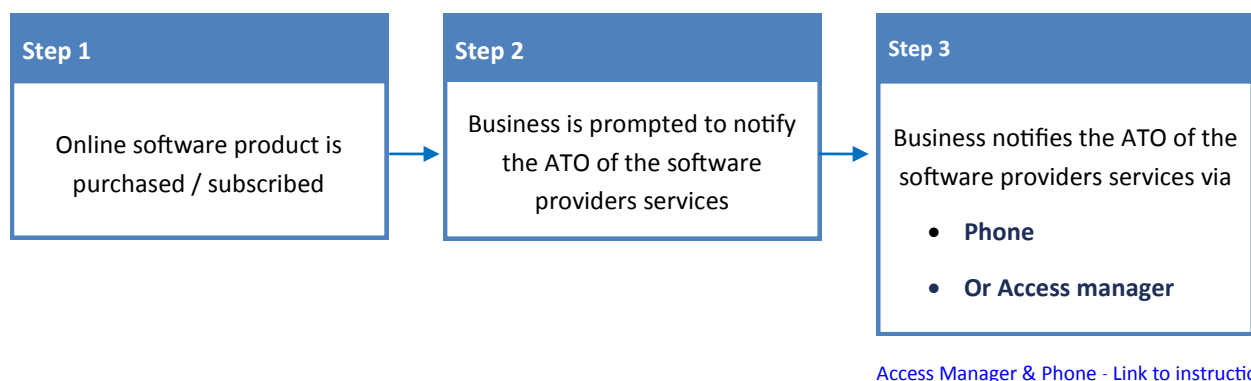
Software Developer on-boarding process

There are no additional certification requirements for CAA. The Integrated Product Test (IPT) suite is available to support software developers integrate with SBR and ATO by providing authentication and authorisation scenarios which may be used to test any message implementation.

Once software developers intending to use CAA have completed these scenarios they can then complete the [CAA declaration form](#) to declare that they have met the CAA requirements and to gain relevant permissions in Access Manager.



Client on-boarding process





7. CAA Requirements

To provide services using the CAA solution, software developers will be required to ensure their software product meets the requirements outlined below. (Please note that these are CAA specific requirements only, other existing SBR and AUSkey requirements and standards apply).

The following reinforces key requirements set out in the SBR Message Implementation Guides (Common and message specific MIGs) that must be adhered to. CAA specific requirements will also need to be incorporated into your software products. You will be required to certify that you have met these requirements to gain access via the [declaration form on the SBR website](#), before being granted access as an online software provider in Access Manager.

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 Guides .
2	Lodgement	Lodgements from a Registered Agent user must include the Registered Agent Number (RAN) as outlined in the SBR Message Implementation Guides .
3	Software terms and conditions	Software terms and conditions must describe the role of a software provider (ie not an agent, lodger or authorised to prepare lodgements. Secure transmission service only). Declaration <i>"I acknowledge that [software provider name] , through the use of [software product name], is not providing an agent service and is not responsible for the preparation of any taxation, superannuation or other related documents on behalf of my business/entity. It can, however, submit transmissions (eg lodgements and prefill) through the SBR channel that my business/entity chooses to make through [software product name]."</i>
4	User authorisation	Upon authentication the software must recognise the role of the user (eg 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 via secured electronic communication (or over the phone) The online cloud software must ensure the unique 'Software ID' of the software subscription or instance of software is automatically sent within the message of a transmission (Software ID not manually entered by client). <i>The Software ID must be recorded in Access Manager or provided over the phone when an authorised business representative notifies the ATO of their Software Providers services. On lodgement, the Software ID will be verified against the software provider notification in Access Manager.</i>



No	Description	Requirements
6	User authentication standards	<p>The Information Security Manual (ISM) is the standard which governs the security of government ICT systems. It is recommended that software developers align to these standards.</p> <p>However, based on current authentication standards provided by the financial sector, software developers must meet the below standards as a minimum, where cloud software requires the user to authenticate using a username and password.</p> <p>Please note: These minimum standards do not restrict software developers from administering more secure credential types.</p> <p><u>PASSPHRASE STRENGTH</u></p> <ul style="list-style-type: none">• Software developers must have a minimum password length of 6 characters, consisting of at least two of the following character sets:<ul style="list-style-type: none">— Lowercase alphabetic characters (a–z)— Uppercase alphabetic characters (A–Z)— Numeric characters (0–9)— Special characters <p><u>FAILED AUTHENTICATION ATTEMPTS</u></p> <ul style="list-style-type: none">• Software developers must lock out user accounts after five failed log on attempts to reduce the risk of brute force attacks.• Software providers can implement a temporary lock out feature after five failed attempts (eg 10 minutes or 24hours). Software developers must completely lock out the user account after a specific number of additional failed log on attempts (decided by the software developer).• Software must have a facility to allow authorised system administrators to reset locked accounts

Adhering to the SBR taxonomy

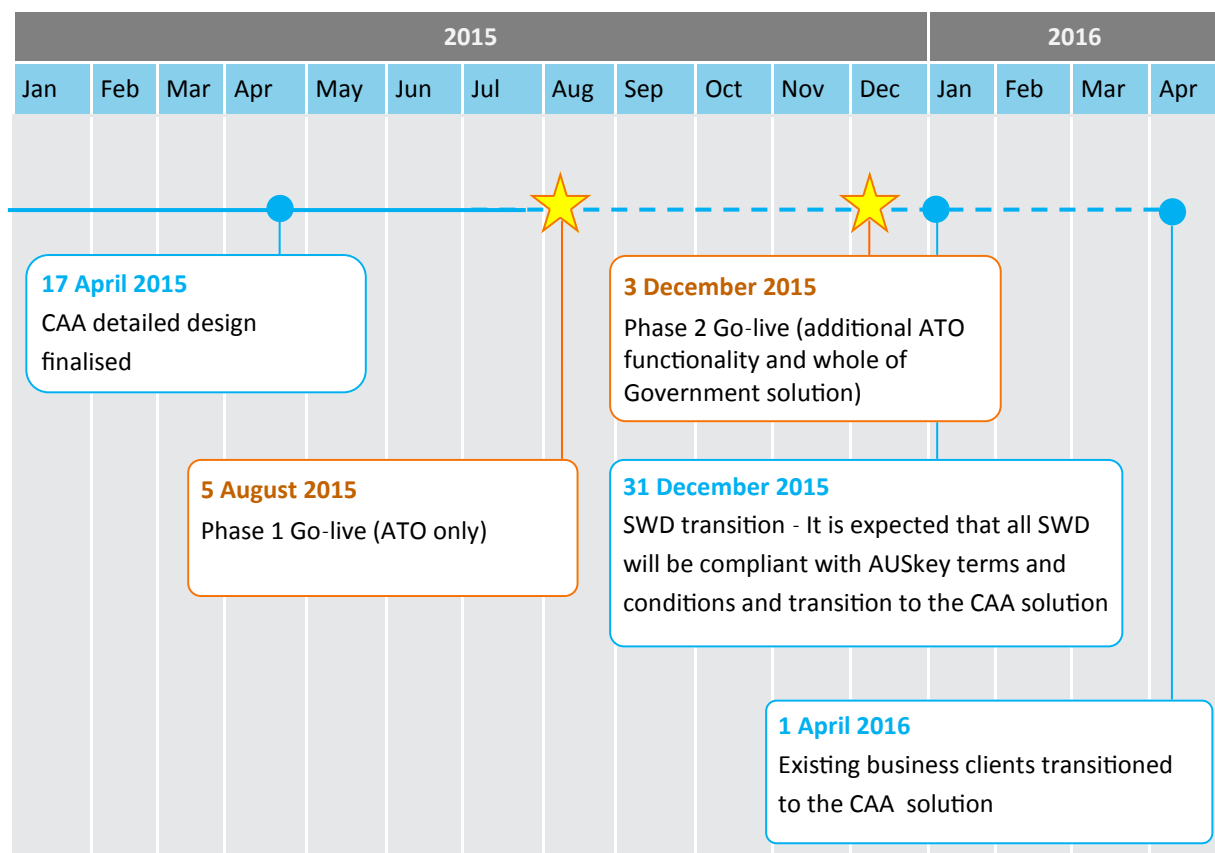
For information on how to build SBR enabled software refer to the link below.

<http://www.sbr.gov.au/software-developers/what-can-i-expect#design-build-test>



8. Transition timeframes

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 **31 March 2016**. The ATO will work with SWDs and assist with transitioning their products and their clients to the new solution.



Key dates

Key dates are also available via the [Cloud Software Authentication and Authorisation Working Group page](#).

Issues Register

Issues raised impacting design, accreditation and transition will be made available and managed via the [Cloud Software Authentication and Authorisation Issues Register](#).



9. Transition assistance

ATO assistance to support your transition to CAA

If you would like assistance with your transition to the CAA solution, contact the SBR Service Desk by email at sbrservicedesk@sbr.gov.au or by phone on 1300 488 231. The ATO will assist where possible regarding:

- the on boarding process (eg completing the Cloud Software Authentication & Authorisation declaration form 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 SBR Service Desk by email at sbrservicedesk@sbr.gov.au or by phone on 1300 488 231. The ATO will assist where possible regarding:

- tailored processes to transition your clients (eg Bulk telephone callouts to notify the ATO of your software providers services), and
- ongoing client support through existing channels.

Communications

Software providers are expected to communicate changes to affected businesses and registered agents directly. The ATO will provide high level messages and a link to instructions on completing a notification at ato.gov.au/cloudsoftwareaanda. This page will be the main source of information for software provider's clients.

SWDs will continue to be engaged and consulted in communication strategies to ensure timely communications are delivered to affected customers.

Key communication messages to businesses and registered agents will include:

- CAA will streamline the way businesses and registered agents interact with the ATO when using online software and will ensure compliant, secure and streamlined transactions online anytime from any device.
- Your Software Provider will advise you if you are affected and provide you with all relevant information, including where to find instructions on how to notify the ATO of an online software providers services.
- We are also working with software providers to extend the benefits of this solution to desktop software.
- Businesses and registered agents lodging via online software that do not use an AUSkey for other purposes will not be required to register for, upload or maintain an AUSkey.



Appendix A

CAA - Detailed Design

Software ID requirements

The following outlines the requirements around the software's automatic generation of a Software ID.

The Software ID **must**:

- be generated using the algorithm provided below and contain 10 digits (leading zeroes are required)
- be unique for each subscription or instance of software
- be passed to the user via a secured electronic communication or over the phone
- be given to the user for the purposes of notifying the ATO of a software providers services

The Software ID **must not**:

- be keyed in by the user for each transmission
- be used as a credential to authenticate the client within online software for lodgement

Software ID generation algorithm

1. Generate the first 9 digits of the Software ID (can be a randomly generated)
2. Pad the generated number with leading zeroes on the left to make 9 digit string
3. Calculate the sum of all digits in the string and apply the Modulo 10 division to calculate the remainder
4. Use the reminder as the 10th control digit
5. Concatenate the generated 9 digits (from step 2) with the control digit (from step 4) to form a 10 digit Software ID

The next table provides a few examples of Software ID generation.

Generated number	Zero padded string (9 characters)	Sum of all digits	Remainder from division by 10 (control digit)	Software ID
1	000000001	$0+0+0+0+0+0+0+0+1 = 1$	1	0000000011
2	000000002	$0+0+0+0+0+0+0+0+2 = 2$	2	0000000022
...
478593	000478593	$0+0+0+4+7+8+5+9+3=36$	6	0004785936



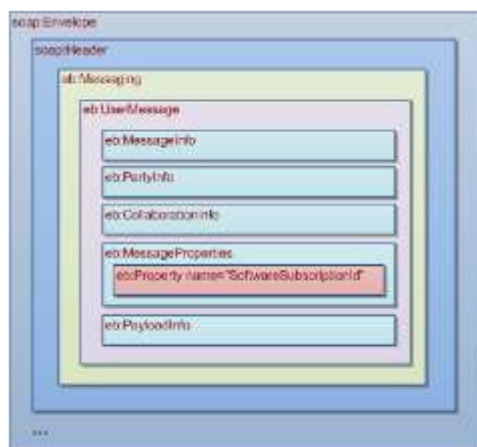
Passing of the software ID for SBR1 (SBR CORE)

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 signing) and it doesn’t break the message integrity or any existing signatures. There will be no impact on the Reference Client and/or SWDs software packages. The SBR Core Services Requester component will be updated to support setting of the “softwareSubscriptionId”



Passing of the software ID for 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.



Error messages returned by SBR as part of Authorisation checks

The specific error codes and corresponding external error messages have been published in the [ATO Common Message Implementation Guide \(MIG\)](#) hosted on sbr.gov.au.



Appendix B

Selecting a Device AUSKey to use for hosted SBR services

The steps below outline the process of setting up your Device AUSKey as an Online software provider.

Before selecting a Device AUSKey to use for hosted SBR services, you must complete the following steps outside of the Access Manager user interface.

a) Complete the CAA declaration form.

After you complete the declaration form, you will be notified when you have been granted access as an online software provider (Hosted SBR software service provider) in Access Manager.

b) Register for and install your Device AUSKey

If you don't have a Device AUSKey see [how to register for a Device AUSKey](#)

c) Submit an initial SBR transaction with your Device AUSKey.

To make the Device AUSKey visible in Access Manager, an initial transaction with a new Device AUSKey, through the SBR channel, must be performed. This transaction will likely fail (this is normal). Once this has occurred the Device AUSKey will become visible in Access Manager. See [Using Access Manager - Access and permissions](#)

d) Login to Access Manager with a user AUSKey (with Administrator privileges).

Step 1 of 1 – The provider selects a Device AUSKey to use for hosted SBR services

To Select a Device AUSKey to use for hosted SBR services, the software provider will need to;

1. Click on 'My hosted SBR software services' in the left hand menu,
2. Click on a 'Select for use in hosted SBR services you provide' checkbox, within the list of AUSKeys and click 'Save'

Business: REV PTY LTD ABN: 96089545483

You are here: Home » Hosted SBR software service provider functions

Hosted SBR software service provider functions

< Home Client notifications held by the ATO for your hosted SBR software service >

Hosted SBR software service provider display name

1 Clients search for their hosted SBR software service provider by their ABN and/or display name. You can modify your display name below (changes will be stored when you select 'Save').

Your display name: REV PTY LTD

Device AUSKeys used for your SBR software hosting services

1 Listed below are Device AUSKeys held by your ABN entity. Select those you want to be used in the hosted SBR software environments you provide your clients and select 'Save'.

Device AUSKey name	User account status	Last accessed	Last updated	Select for use in hosted SBR services you provide
ProviderDevice_74A190D7B0	Active	14 Dec 2015	14 Dec 2015	<input type="checkbox"/>
ProviderDevice_81EBEC623D	Active	14 Dec 2015	14 Dec 2015	<input type="checkbox"/>
ProviderDevice_98FB4442F	Active	14 Dec 2015	14 Dec 2015	<input type="checkbox"/>
ProviderDevice_DAAA42C969	Active	14 Dec 2015	14 Dec 2015	<input checked="" type="checkbox"/>

Cancel Save

TIPS
Display name
Your default display name is your entity name as listed in the Australian Business Register.
Clients will see your display name next to your ABN.
Your clients identify you (as their hosted SBR software service provider) by selecting your ABN.
Device AUSKey not listed?
You must attempt an initial SBR transmission with your Device AUSKey for it to be recognised in Access Manager.



Appendix C

Provider views clients, notification details and can disable a notification

The steps below outline the process of viewing clients, notification details and disabling a notification as an Online software provider.

Before viewing clients, notification details, you must complete the following steps outside of the Access Manager user interface.

- Complete the CAA declaration.
After you complete the declaration an ATO operator will notify you when they have allocated your permissions as an online software provider (Hosted SBR software service provider) in Access Manager.
- Login to Access Manager with a user AUSkey (with Administrator privileges).

Step 1 of 2 – The provider views clients who have notified the ATO of their hosted SBR services . The client's ABN is selected to view more details.

To view a client's notification details (including software IDs) or disable the notification;

- Search for clients using the ABN or Business name
- Click on the client's ABN hyperlink

The screenshot displays the 'Access Manager' web application. The top navigation bar includes the Australian Government logo and the text 'Access Manager'. The left sidebar contains a menu with 'Access Manager Links' and 'External Links'. The main content area is titled 'Business: REV PTY LTD ABN: 96089045483' and shows 'Client notifications held by the ATO for your hosted SBR software service'. A search bar is present with the text 'ABN: and/or Business name:'. Below the search bar, a table lists client notifications. The first row shows an ABN of 96 080 155 669, Business Name STRATA PLAN LC, and Notification status Active. A 'Cancel' button is located at the bottom left of the table area. A 'TIPS' box on the right provides instructions on how to search for a client.

ABN	Business Name	Notification status
96 080 155 669	STRATA PLAN LC	Active



Provider views clients, notification details and can disable a notification

Step 2 of 2 – The provider views the Software IDs in the notification and can disable the notification if required

1. The notification can be changed between Active and Disabled, then selecting Save will confirm the change.

Note: You can disable a notification to prevent a business from using your software to make online (cloud) transmissions. Disabling the notification will not delete it and the notification can be re-activated after being disabled.

The screenshot shows the 'Access Manager' interface for the Australian Taxation Office. The top navigation bar includes the ATO logo, 'Access Manager', and user information. A left-hand menu lists various links under 'Access Manager Links', 'My business', and 'External Links'. The main content area is titled 'Client notification details' and shows information for business 'REV PTY LTD' with ABN 96089845483. It includes a breadcrumb trail, a sub-header for client notifications, and a section for details notified by the client. This section contains fields for ABN, Business Name, Notification status (with 'Active' selected and 'Disabled' highlighted), and Software IDs. A 'TIPS' box on the right provides guidance on handling incorrect Software IDs. At the bottom, there are 'Cancel' and 'Save' buttons.

Business: REV PTY LTD ABN: 96089845483

You are here: [Home](#) » Client notification details

Client notification details

← Client notifications held by the ATO for your hosted SBR software service

Details notified by the client to the ATO

1 Your client notified the ATO that they identified your business as providing them with a hosted SBR software environment. You can disable (or re-activate) your client's notification below. This will not delete the notification.

ABN:	96 090 155 669		
Business Name:	STRATA PLAN LC		
Notification status:	<input checked="" type="radio"/> Active <input type="radio"/> Disabled		
Software IDs:	<table><thead><tr><th>Software IDs</th></tr></thead><tbody><tr><td>1000000001</td></tr></tbody></table>	Software IDs	1000000001
Software IDs			
1000000001			

[Cancel](#) [Save](#)

TIPS

If a Software ID is incorrect, contact the client to update it in Access Manager.

When a client initially notifies the ATO of the software service you provide, its status is automatically set to 'Active'. You can change the status.



Appendix D

How your client will notify the ATO of your software services

New and existing subscribers to an online software product will be required to notify the ATO a software providers services and present a unique software ID.

To assist your clients to notify the ATO of your services, you can instruct them to call us on **1300 85 22 32** and state they would like to 'Notify the ATO of a hosted SBR software service'. Normal proof of record ownership will apply when they call.

When notifying, your clients will need to have the following information ready:

- Their ABN (Registered Agents can also use their RAN)
- The ABN or name of the Software Provider (supplied by the software provider)
- Unique software ID (supplied by the software provider)

Alternatively, if they have an Administrator AUSkey, your clients can log into Access Manager to complete their notification. The ATO have provided a link to instructions on completing a notification and high level messages at ato.gov.au/cloudsoftwareaanda. This page will be the main source of information for software provider's clients.

To further assist software providers to support their clients, The ATO have provided a link to screenshots from Access Manager on the [SWD Cloud software authentication and authorisation web page](#).



Appendix E

How cloud transmissions are verified

For a cloud transmission to pass verification through SBR, the ATO will perform the following steps.

Determine if the SWD is setup to secure transmissions with cloud

Step 1

Does the SWD have online software provider access in Access Manager?

- ✓ SWD has been granted online software provider access in Access Manager.

Step 2

Is the Device AUSkey set up?

- ✓ [The Device AUSkey has been enabled to secure online \(cloud\) transmissions in Access Manager](#)

Determine if client making transmission has correctly notified the ATO of the software providers services

Step 3

Does the notification exist?

- ✓ The client (Business or Agent) has notified the ATO of the online software providers services in Access Manager.
- ✓ The client's ABN sent in the transmission and SWD ABN (AUSkey) must relate to the notification.

Step 4

Does the Software ID match the notification?

- ✓ The client (Business or Agent) has entered a software ID against the notification in Access Manager.
- ✓ The Software ID sent in the transmission matches against the notification in Access Manager.

Step 5

Has the notification been disabled?

- ✓ The notification has not been [disabled by the SWD in Access Manager](#)

Determine if the intermediary is authorised to act on the clients behalf

Step 6

If an intermediary sent the transmission, are they authorised?

- ✓ The intermediary (eg registered tax agent or BAS agent) is authorised to act on the clients behalf.

Step 7 - Lodgement Accepted




Appendix F

Lodgement scenarios

The scenarios below illustrate the process of verifying a lodgement received as part of the new cloud solution.





1 - Business lodging from their own subscription

Data Fields	
AUSkey ABN	
Intermediary ABN/TAN	
Reporting Party ABN	
Software ID	

The ATO will check if:

- a notification exists between Reporting Party (ABN) and SWD (AUSkey ABN), and
- the Software ID relates to the Reporting Party (ABN) notification.

2 - Agent lodging from their own subscription

Data Fields	
AUSkey ABN	
Intermediary ABN/TAN	
Reporting Party ABN	
Software ID	

If intermediary ABN/TAN is provided, the ATO will check if:

- a notification exists between Intermediary (ABN/TAN) and SWD (AUSkey ABN),
- a Software ID is related to the Intermediary (ABN/TAN) notification, and
- the Intermediary (ABN/TAN) is authorised to act on behalf of the reporting party (ABN).

3 - Agent lodging from businesses subscription (the business has authorised the provider)

Data Fields	
AUSkey ABN	
Intermediary ABN/TAN	
Reporting Party ABN	
Software ID	

If intermediary ABN/TAN is provided, the ATO will check if:

- a notification exists between Intermediary (ABN/TAN) and SWD (AUSkey ABN),
- the Software ID is related to the Reporting Party (ABN) notification, and
- the Intermediary (ABN/TAN) is authorised to act on behalf of the reporting party (ABN).

No Relationship Check Forms (NRCF)

NCRF are SBR forms lodged through software where the ATO does not verify that the Intermediary lodging is authorised to act on behalf of the business. NCRF include TFN Declaration (TFN Dec), Taxable Payment Annual Report (TPAR) & PAYG Payment Annual Summary (PSAR).

SWD can continue to use their device AUSkey to secure NCRF transmissions without a Software ID. *This will negate the need for their clients to notify the ATO of the software providers services.*



Appendix G

Online Software Provider Appointment Web Service

This service will be made available for SWD with online software provider access in Access Manager. This service can be used to verify if a software developer's client has notified the ATO of their services and registered their Software ID correctly. To call this service the software provider must authenticate using their AUSkey credential and provide their ABN, client's ABN and the Software ID. This service will be available in production as part of the phase 2 release. The service will not be made available in External Vendor Test Environment (EVTE).

Detailed instructions to call this service have been uploaded to the [SWD Cloud software authentication and authorisation web page](#) as part of the phase 2 release (3 December).



Calls 'Online Software Provider Appointment Web Service'

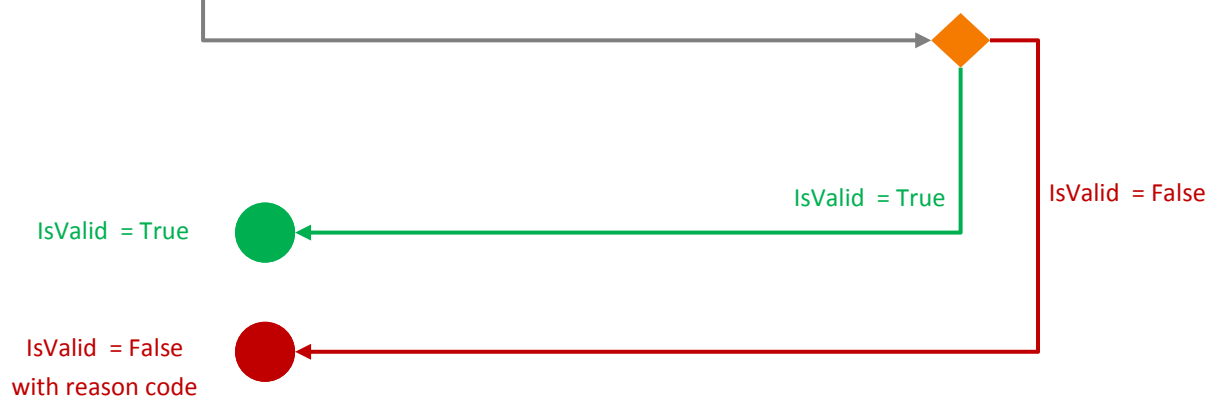
Required attributes
SWD ABN
Clients ABN
Software ID

Authenticates
using SWD Device
AUSkey

Online Software Provider Appointment Web Service

Web service checks

- the AUSkey is a device AUSkey
- the SWD has online software provider access in Access Manager
- The AUSkey is enabled to secure online transmissions in Access Manager
- a notification exists
- the notification is enabled (notifications can be disabled by the SWD)
- the Software ID matches the notification





Appendix H

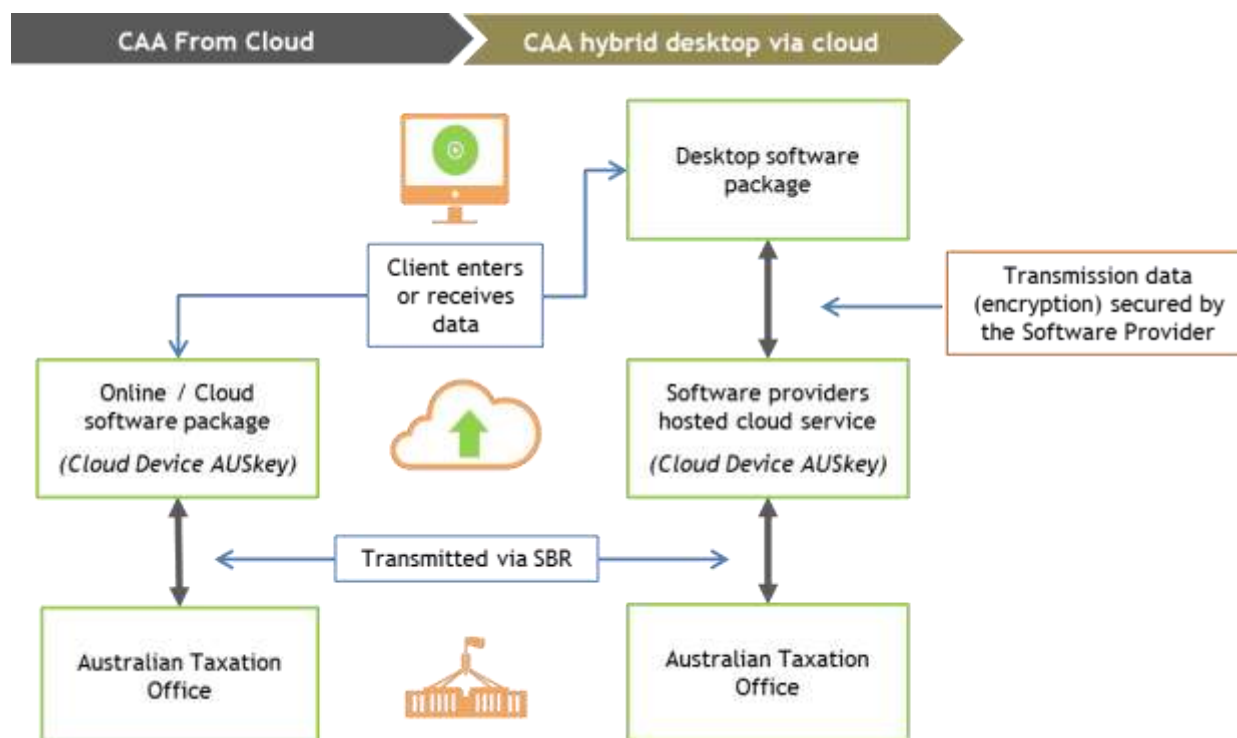
Hybrid desktop via cloud software

By software provider request the CAA solution can now be leveraged using hybrid desktop via cloud software.

Users of hybrid desktop via cloud software can then experience the benefits of CAA and can now submit information to the ATO without needing their own AUSkey. The software providers AUSkey is used to secure the transmission from the software providers hosted cloud service. For a hybrid desktop via cloud software provider to on-board CAA, they will be required to follow the same [CAA set up and authorisation process](#) as cloud software providers.

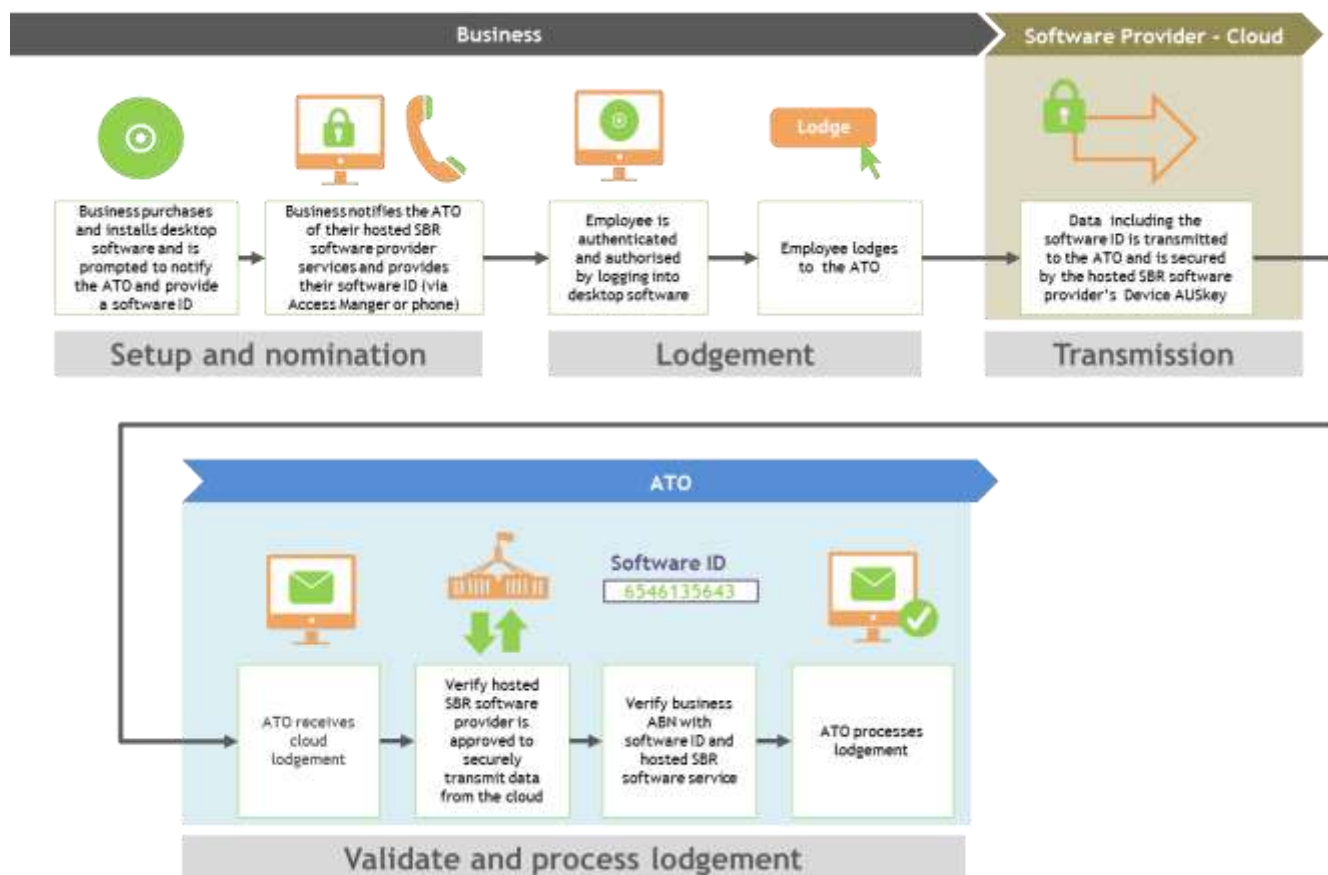
The hybrid desktop via cloud design:

- leverages the current CAA solution
- allows software to transmit and receive data from the desktop via a cloud service hosted by the SWD to the ATO
- still requires the client's Software ID in the transmission and for it to be secured by the software providers Device AUSkey
- is subject to all the relevant [cloud authorisation checks](#) and [minimum security requirements](#).





Lodgement by “business” using hybrid desktop via cloud software





Appendix I

Frequently Asked Questions (FAQ)

FAQ are hosted on the [CAA FAQ webpage](#)