



Cloud Software Authentication & Authorisation (CAA)

Digital Service Provider information kit



Version Control

	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 Lodgment 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 Lodgment 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- Lodgment 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'
1.8	July 2022	Paul Walters	External DSP stakeholders	General update to remove AUSKey references Update metrics and reflect current solution state Remove transition timeframes and references to deprecated web service
2.0	September 2022	Paul Walters	External DSP stakeholders	Endorsed for publication



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 [Assistance implementing CAA](#)

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

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

[Appendix C - Provider views client’s 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 - Lodgment scenarios](#)

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

[Appendix H - 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).

In 2015, taking into consideration the feedback received from the software developer (SWD) (now referred to as Digital Service Providers – DSP) community the ATO implemented a solution to streamline the client experience, support a move toward Digital by Default and be compatible with future directions (eg Whole of Government (WofG) authorisation and Single Touch Payroll).

The ATO implemented changes to support a Cloud Software Authentication & Authorisation (CAA) solution that:

- enables approved DSPs to setup a dedicated machine credential for the purposes of securing transmissions to the ATO made by businesses and tax agents through online (cloud hosted) software,
- allows businesses and tax agents to notify the ATO of a software provider's services, for the purposes of using the software provider's machine credential to secure transmissions made from within their online (cloud hosted) software,
- eliminates the need for businesses and tax agents to obtain, upload or use a machine credential to secure transmissions when interacting with the ATO via online (cloud hosted) software, and
- co-exists with existing compliant DSP solutions.

It is expected that Digital Service Providers will satisfy requirements that address legal and technical aspects of the solution and comply with conditions defined within the [DSP Operational Security Framework](#).

If you would like further information on CAA or the ATO Operational Security Framework, or wish to report a technical issue you can do so by raising an incident or question in [Online Services for DSPs](#) or by emailing the DPO at dpo@ato.gov.au.



2. Context

Registering for and maintaining credentials across government

The Australian Government is continuously improving the use of digital credentials when accessing government services online. However, registering for and maintaining credentials across government in order to interact digitally is still seen as difficult for businesses today. This continues to impact the take-up rate of digital services offered by government.

There were approximately 2.402 million actively trading businesses in Australia at June 2021¹. Currently there are approximately 82 thousand active machine credentials, in use by approximately 39,000 unique businesses.

As businesses become more mobile, and the use of cloud based services expands, credentials used to access government services will continue to evolve to 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.

Through the efforts of the Digital Transformation Agency (DTA), government is committed to streamlining access to government services, making it simpler, clearer and faster for individuals and businesses. The DTA is responsible for improving digital identity across government, leveraging myGov, myGovID, Relationship Authorisation Manager (RAM) and the Australian Business Register to transform the way services are delivered to both individuals and business. The DTA is committed to ensuring all users can obtain a secure and easy-to-use digital identity to access all digital government services.

¹ Australian Bureau of Statistics ([Counts of Australian Businesses, including Entries and Exits, July 2017 - June 2021](https://www.abs.gov.au/ausstats/13500nmain2611111?val=202106) | Australian Bureau of Statistics ([abs.gov.au](https://www.abs.gov.au)))



3. Policy Advice

The current myGovID terms-of-use (<https://www.mygovid.gov.au/mygovid-terms-of-use-user>) outlines the responsibilities placed upon MyGovID and machine credential holders. Failure to uphold these responsibilities will result in the cancellation of the credential.

Under the existing terms-of-use and consistent with advice on previous Government credentials software developers remotely storing their client's machine credentials and/or their associated passwords in cloud based solutions are in breach of the terms and conditions of use.

The Department of Finance (as the Gatekeeper Competent Authority) assessed the original CAA solution (outlined in this document) and determined it to be compliant with the terms and conditions of the AUSkey Certification Practices Statement (CPS) and Certificate Policies (CP). This compliance extends to the MyGovID CPS and CP (<http://pki.ato.gov.au/policy/ca.html>) that replaced the previous AUSkey policies and practices.

Responsibilities in relation to the myGovID Machine Certificates (Machine Credentials)

<p>4.1.1 Who can apply for a machine credential?</p> <p>An application for a machine credential (to be held for a Business Entity):</p> <ul style="list-style-type: none"> • can only be made by a Machine Credential Administrator for that same Business Entity, and • can only be made online through the Relationship Authorisation Manager (RAM) System, and • must hold a valid myGovID User ID as the custodian to be associated with that machine credential. 	<p>Machine credential custodians must hold pre-existing myGovIDs authorised for use by an Authorisation Administrator of the business, thus typically aren't the Cloud provider. The Machine Credential Administrator creates the password and ensures the machine credential is only used on the intended device, requiring physical access to installed sites, or some other form of secure transference.</p>
<p>4.4.1 Machine Credential Custodian responsibilities</p> <p>The Custodian for a machinecredential is responsible for:</p> <ul style="list-style-type: none"> • downloading the machine credential when it is issued, following registration • creating the password that protects the machine credential and its associated Keys, and changing that password at recommended intervals • ensuring the machine credential is attached to the correct Machine • safely transferring the machine credential from the download location to the server location, if required for example because the Organisation has an IT Outsourcing, SaaS or similar arrangement with another entity, and needs to transfer its machine credential to that other entity's hosting location • managing the use of, and safeguarding, the machine credential • requesting revocation of the machine credential, when required. 	<p>The machine credential conditions-of-use do not expressly forbid Cloud use, however the definition of 'compromised' as defined in the Gatekeeper PKI Framework (V3.1 – December 2015)(https://dta-www-drupal-2018013021541115340000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/digital-identity/Gatekeeper/01%20Gatekeeper%20PKI%20Framework%20v%203.1%20May%202015_01d.docx) states that "uncontrolled" keys no longer offer assurance of integrity of signed messages. Machine credentials hosted in third party cloud services are no longer in the control of the Custodian.</p>



4. What is the 'Cloud'

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.

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.

In 2017 the Digital Transformation Agency released the Secure Cloud Strategy (<https://www.dta.gov.au/our-projects/secure-cloud-strategy>) replacing the prior Australian Government Cloud Computing Policy. Additionally, the Australian Cyber Security Centre has published guidance on [Cloud Computing Security Considerations](#).

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. 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).*

Applicability

The Cloud Software Authentication and Authorisation solution applies to commercially supplied cloud hosted software (SaaS) securely transacting with the ATO using standard APIs.

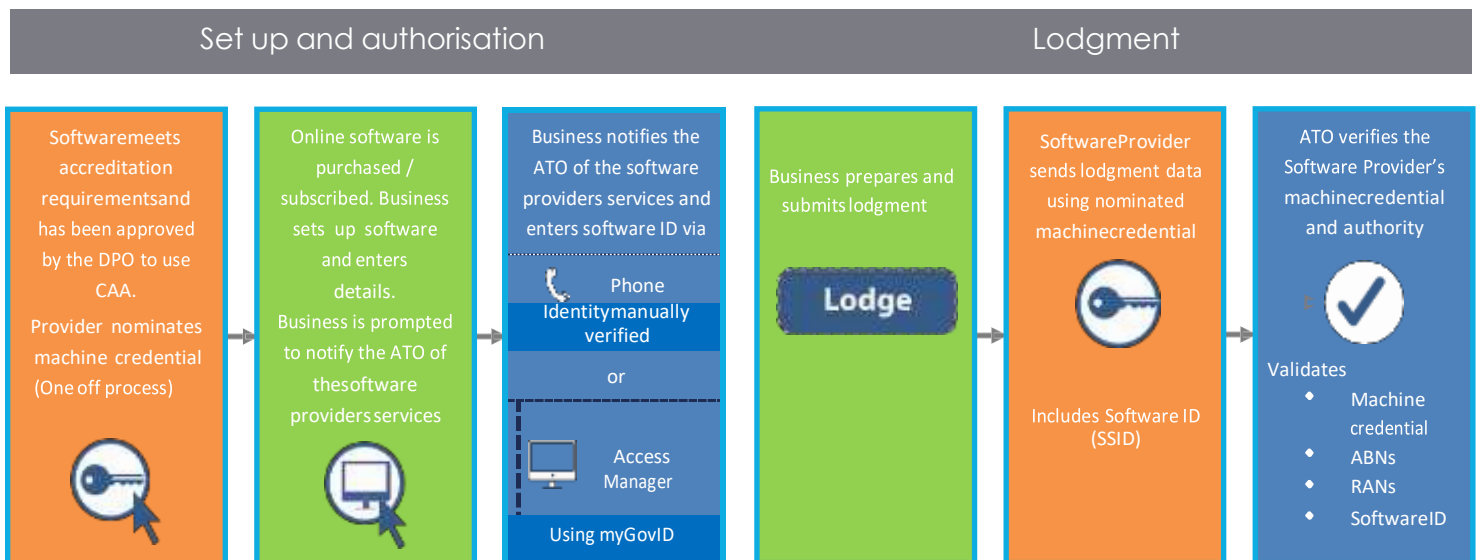


5. High Level Solution

The proposed CAA solution allows a business to authorise a Digital Service Provider’s dedicated machine credential for the purposes of securing a transmission/lodgment to the ATO via online ‘cloud’ software.

How does it work?

1. The DSP meets accreditation requirements to use CAA
2. The DSP nominates a dedicated machine credential which is used to secure transmissions initiated by their business clients via online (cloud enabled) software.
3. The DSP’s clients are asked to contact the ATO and authorise the DSP via Access Manager using their myGovID or over the phone (They 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 lodgment data (including the Software ID) is sent to the ATO and secured using the DSP’s dedicated machine credential
5. Once the lodgment data is received, the ATO verifies that the authorisation between the DSP 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](#)

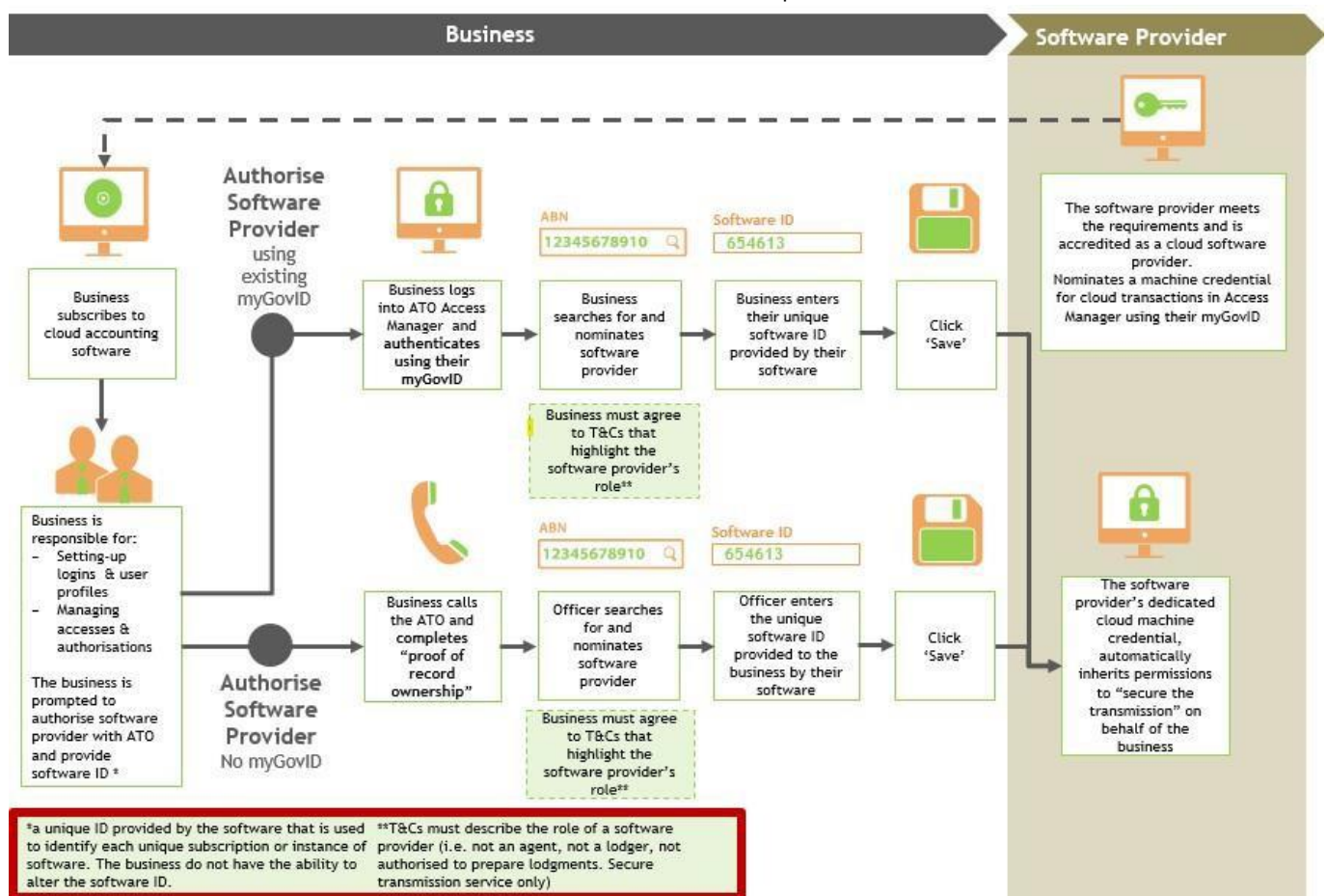
¹‘Software ID’ is a unique ID that is used to identify each unique subscription or instance of software and is automatically generated by the software. See [Appendix A. CAA - Detailed Design](#)



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 provider's services
- Businesses do not need to register for and obtain a myGovID in order to authorise a Software Provider and transact in cloud, maximising take up of these services
- Machine credential nomination by the Software Provider is only required once using an authorised myGovID (in Access Manager). Only myGovID Machine Certificates (*machine credentials*) can be used with Standard Business Reporting (SBR) services²
- Software Providers can nominate multiple machine credentials if required
- Dedicated machine credential limits the potential for fraudulent access by unauthorised individuals
- No concentration of customer credentials in a single location
- Compliant with myGovID terms and conditions of use

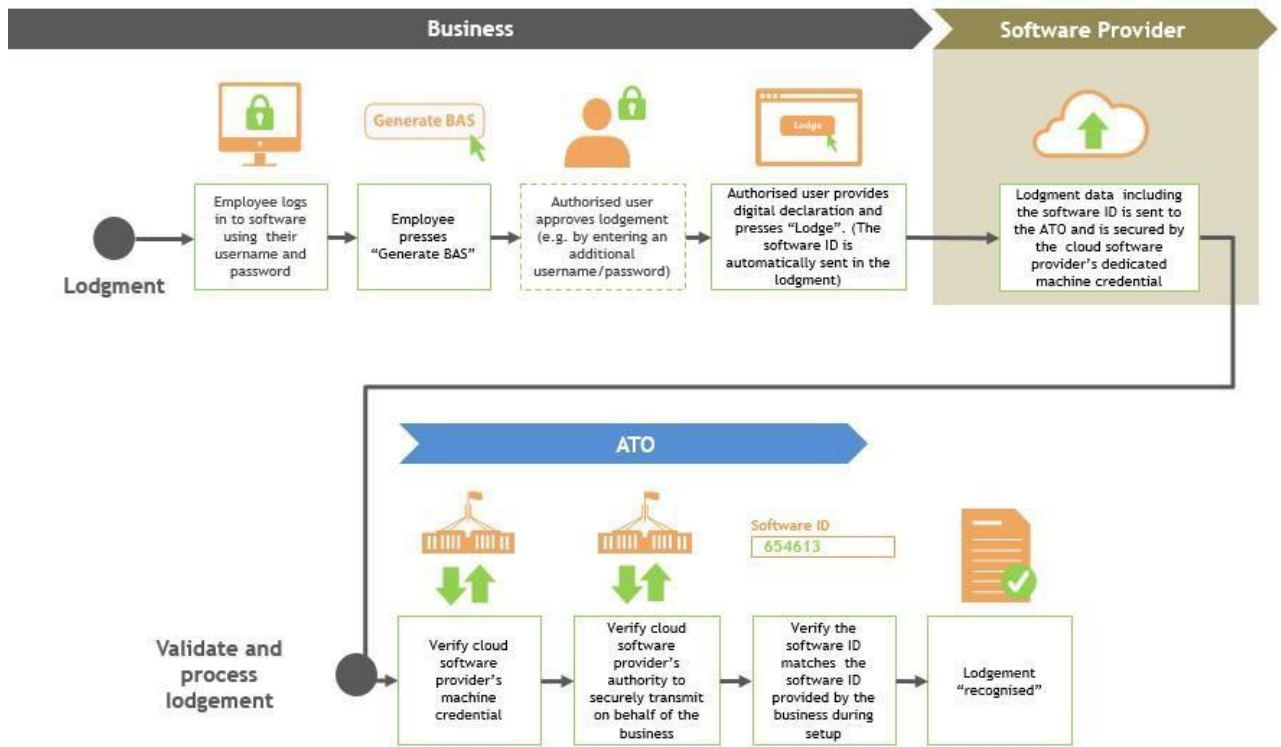
Business notifies the ATO of a Hosted SBR software service provider



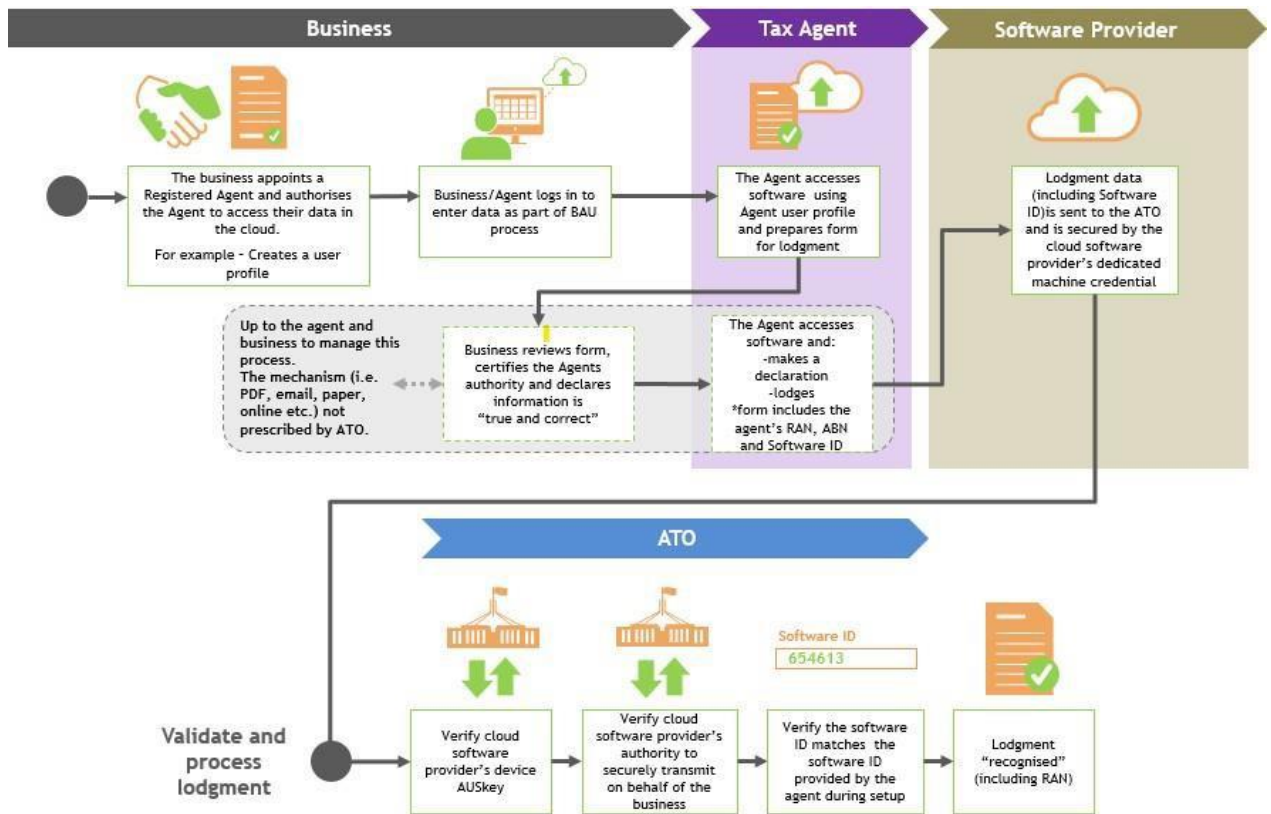
² Machine credentials will also be required for ATO APIs published in the ATO Digital Services Gateway. References to SBR services in this document are also references to ATO APIs.



Lodgment by "business" using cloud software



Lodgment by Registered Agent in the cloud



6. Set up and authorisation process

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

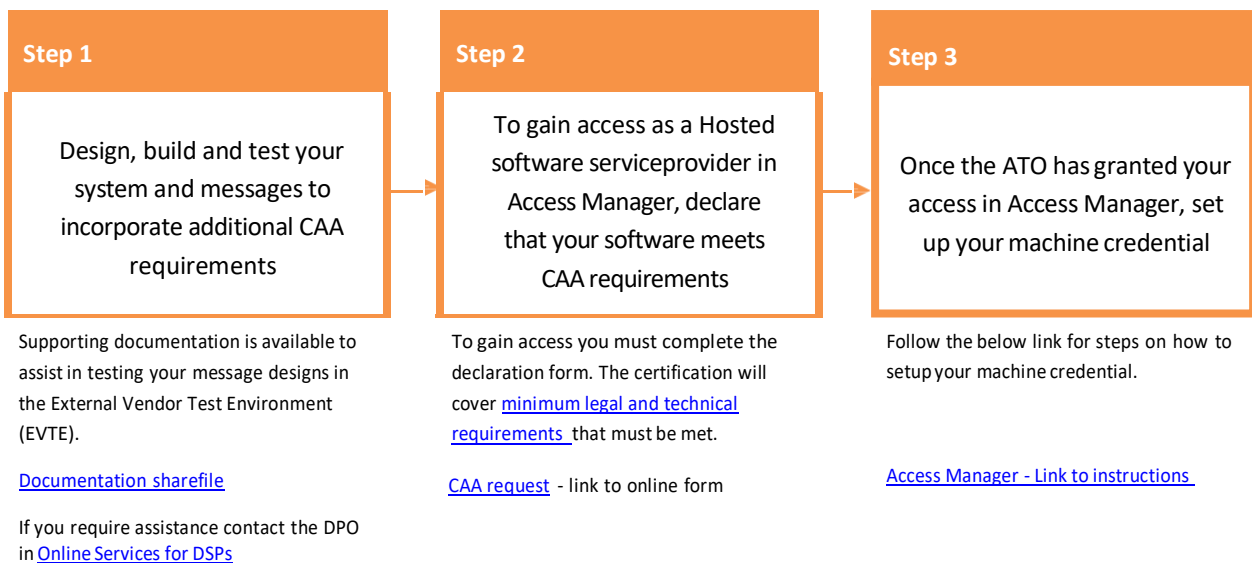
Please note, to be able to secure transmissions through the SBR channel you will also be required to follow the current process and:

- register as a DSP with the ATO Digital Partnership Office; and
- assess, test and certify your software against the current (SBR1 and SBR2) conformance process.

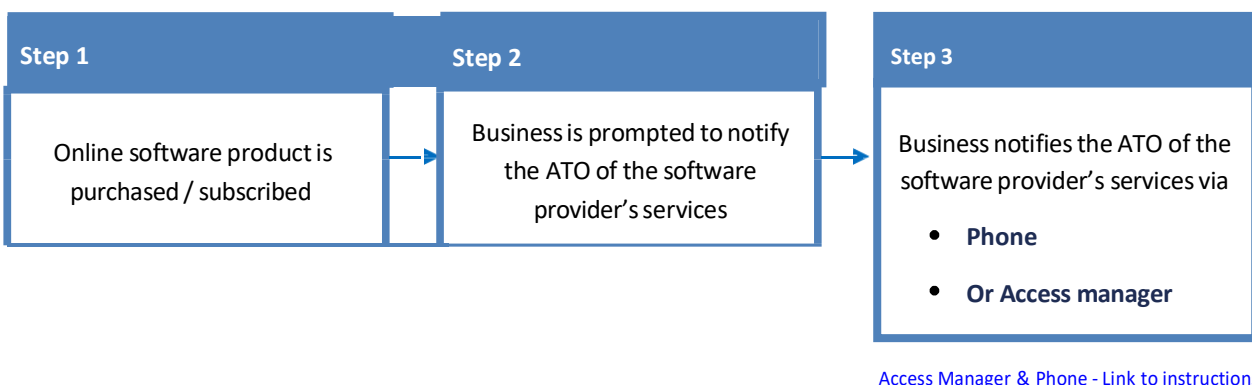
Digital Service Provider on-boarding process

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

Once DSPs intending to use CAA have completed these scenarios they can then lodge a [CAA request](#) through Online Services for DSPs 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, DSPs 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, ATO API and machine credential 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 via a [CAA request](#) through Online Services, before being granted access as an online software provider (Hosted SBR software service 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 ATO Common Business Implementation and Taxpayer Declaration Guide .
2	Lodgment	Lodgments from a Registered Agent user must include the Registered Agent Number (RAN) as outlined in the ATO ebMS3 Implementation Guide .
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 lodgments. 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 lodgments 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 lodgment, the Software ID will be verified against the software provider notification in Access Manager.</i>



No	Description	Requirements
6	Authentication	The ATO Operational Security Framework specifies authentication requirements for DSP controlled environments. Multi-Factor Authentication (MFA) must be implemented for end users of DSP hosted cloud services. User logins must be unique and shared logins must be blocked by the DSP.
7	Cyber security	<p>The Information Security Manual (ISM) is the standard which governs the security of government ICT systems. It is recommended that DSPs align to these standards.</p> <p>The ATO takes the security and privacy of personal information very seriously. The ATO Operational Security Framework establishes DSP obligations when implementing hosted single and multi tenanted environments.</p> <p>Additionally, the Australian Cyber Security Centre (ACSC) provides resources to assist DSPs and their customers to secure their systems and data. DSPs should review the available resources including updates on emerging threats.</p> <p>Additional ACSC resources:</p> <ul style="list-style-type: none">• Creating strong passphrases• Implementing multi factor authentication• Guidelines for System Hardening Cyber.gov.au

8. Assistance implementing CAA

ATO assistance to support you onboarding to CAA

New cloud software developers and existing DSPs implementing cloud services can seek support from the Digital Partnership Office. If you would like assistance with onboarding to the CAA solution, contact the DPO in [Online Services for DSPs](#), 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 onboarding process(eg completing the Cloud Software Authentication & Authorisation [request](#) and setting up your machine credential),
- designing your software to requirements, and
- testing and certification processes.

Communications

Software providers are expected to communicate changes to affected businesses and registered agents directly. The ATO provides high level messages and instructions on completing a notification at [My hosted SBR software services | Australian Taxation Office \(ato.gov.au\)](#) This page will be the main source of information for software provider's clients.

Key communication messages to businesses and registered agents will include:

- CAA streamlines the way businesses and registered agents interact with the ATO when using online software and ensures 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 a hosted software provider's services.
- Businesses and registered agents lodging via online software that do not use a machine credential for other purposes will not be required to register for, upload or maintain a machine credential.



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 provider's 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 lodgment

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 remainder 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

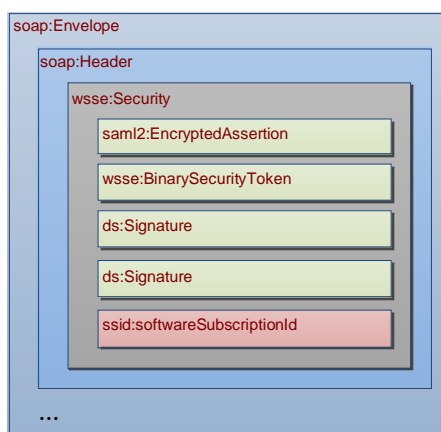
The next table provides a few examples of Software ID generation.

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



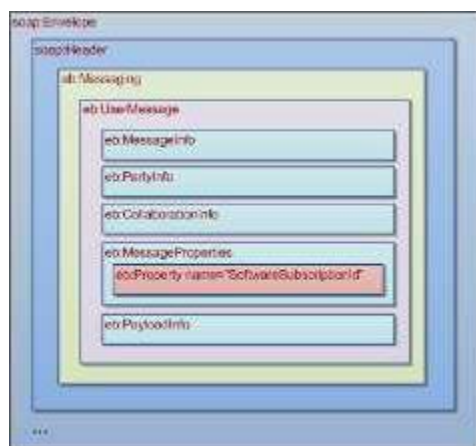
Passing of the software ID for SBR1 (SBR CORE)

The software ID is passed in the message through an incorporated 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 DSPs 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 (ebMS3)

The software ID is passed in the soap:Header by using the 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. The property is located in the eb namespace (<http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/>).³



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 Authorisation Errors](#) hosted on sbr.gov.au.

³ ATO ebMS3 Implementation Guide [https://www.sbr.gov.au/sites/default/files/ato_ebms3_implementation_guide.docx]

Developing SBR services

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>

Passing the software ID for the ATO API Gateway

The software ID is provided when requesting an access token from the ATO Authorisation Server (grant jwt). The grant jwt must also include the external identifier (ABN/ACN/ARBN)⁴ of the customer. The access token request will fail where no cloud notification has been created in Access Manager by the software user.

Further information regarding using the ATO API Gateway can be found at the [ATO API Portal](#).

Registered DSPs can login to [Online Services for DSPs](#) to obtain guidance on [integrating to the ATO Authorisation Server](#).

⁴ ACN and ARBN can only be used after the Company release of the Australian Business Registry System.



Appendix B

Selecting a machine credential to use for hosted SBR services

The activities below outline the process of setting up your machine credential as an Cloud Software Provider.

Before selecting a machine credential to use for hosted SBR services, you must complete the following actions outside of the Access Manager user interface.

1. Complete the relevant conformance testing and lodge a [CAA request](#) through Online Services for DSPs. After you complete the request, you will be notified when you have been granted access as an online software provider (Hosted SBR software service provider) in Access Manager.
2. Register for and install your machine credential.
If you don't have a machine credential see [how to register for one](#).
3. Submit an initial SBR transaction with your machine credential.
To make the machine credential visible in Access Manager, an initial transaction with a new machine credential, through the SBR channel, must be performed. This transaction may fail (this is normal). Once this has occurred the machine credential will appear as a user in Access Manager. See [Using Access Manager – Access and permissions](#) for guidance on managing user permissions.
4. Login to Access Manager with a myGovID (with RAM Authorisation Administrator privileges) and complete the following step:

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

To select a machine credential to use for hosted SBR services, the software provider will need to:

1. Click on 'Hosted SBR software service provider functions' in the left hand menu
2. Click on a 'Select for use in hosted SBR services you provide' checkbox, within the list of machine credentials and click 'Save'

The screenshot shows the 'Access Manager' interface for a user with the business 'REV PTY LTD' (ABN: 95080645483). The page title is 'Hosted SBR software service provider functions'. The main content area includes a form for 'Hosted SBR software service provider display name' with a text input field containing 'REV PTY LTD'. Below this is a table titled 'Device AUSkeys used for your SBR software hosting services' with columns for 'Device AUSKey name', 'User account status', 'Last accessed', 'Last updated', and 'Select for use in hosted SBR services you provide'. The table lists four Device AUSKeys, with the last one, 'ProviderDevice_DAAA42C969', having its checkbox checked. A 'TIPS' box on the right explains that the default display name is the entity name from the Australian Business Register and that clients identify the provider by selecting their ABN. It also notes that an initial SBR transmission is required for the Device AUSKey to be recognized in Access Manager.

Device AUSKey name	User account status	Last accessed	Last updated	Select for use in hosted SBR services you provide
ProviderDevice_74A19B07B0	Active	14 Dec 2015	14 Dec 2015	<input type="checkbox"/>
ProviderDevice_81EBEC823D	Active	14 Dec 2015	14 Dec 2015	<input type="checkbox"/>
ProviderDevice_98FFB4442F	Active	14 Dec 2015	14 Dec 2015	<input type="checkbox"/>
ProviderDevice_DAAA42C969	Active	14 Dec 2015	14 Dec 2015	<input checked="" type="checkbox"/>



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 (Hosted SBR software service provider).

NB. Before viewing your clients' notification details, you must complete actions 1 and 4 in Appendix B.

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;

1. Search for clients using the ABN or Business name
2. Click on the client's ABN hyperlink

The screenshot shows the 'Access Manager' interface. At the top, it says 'Business: REV PTY LTD : ABN: 96089845483'. Below this, there's a breadcrumb trail: 'Home > Client notifications held by the ATO for your hosted SBR software service'. The main heading is 'Client notifications held by the ATO for your hosted SBR software service'. A sub-heading is 'Hosted SBR software service provider functions'. A tip box states: 'The list below shows businesses that have notified the ATO that they send and receive transactions with the ATO via the SBR channel in a hosted SBR software environment that you provide them.' There is a 'Client search' section with input fields for 'ABN' and 'and/or Business name', and a 'Search' button. Below this is a table titled 'Client notifications' with columns 'ABN', 'Business Name', and 'Notification status'. The table contains one row: ABN: 96 090 155 569, Business Name: STRATA PLAN LC, Notification status: Active. Below the table, it says 'Displaying 1 to 1 of 1 records found.' There is a 'Cancel' button. On the left, there is a sidebar with 'Access Manager Links' and 'External Links'. On the right, there is a 'TIPS' box with instructions on how to search for a client and what actions can be taken.

ABN	Business Name	Notification status
96 090 155 569	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 a business named 'REV PTY LTD' with ABN 96089845483. The page title is 'Client notification details'. A breadcrumb trail shows 'Home > Client notification details'. Below this, a blue header reads 'Client notification details' with a link to 'Client notifications held by the ATO for your hosted SBR software service'. The main content area is titled 'Details notified by the client to the ATO:' and contains a message: '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.' Below the message is a form with the following fields: 'ABN: 96 098 155 669', 'Business Name: STRATA PLAN LC', 'Notification status: Active Disabled', and 'Software IDs:

Software Ids
1000000001

'. There are 'Cancel' and 'Save' buttons at the bottom. On the right, a yellow 'TIPS' box states: '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.' The left sidebar contains navigation links for 'Access Manager Links', 'My business', 'Business appointments', and 'External Links'.



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 they are using a software providers services and present a unique software ID.

If your clients have a myGovID authorised for their business in the [Relationship Authorisation Manager \(RAM\)](#), they 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 [My hosted SBR software services | Australian Taxation Office \(ato.gov.au\)](#). This page will be the main source of information for software provider's clients.

Alternatively, 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)

To further assist software providers to support their clients, the ATO have provided responses to frequently asked questions at [Cloud software authentication and authorisation – Frequently asked questions | ATO Software Developers](#).



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 DSP is setup to secure transmissions with cloud software	Step 1	<p>Does the DSP have online software provider access in Access Manager?</p> <ul style="list-style-type: none"> ✓ DSP has been granted access as a Hosted SBR Software Service in Access Manager.
	Step 2	<p>Is the machine credential set up?</p> <ul style="list-style-type: none"> ✓ The machine credential has been enabled to secure hosted SBR software service transmissions in Access Manager
Determine if client making the transmission has correctly notified the ATO of the software providers services	Step 3	<p>Does the notification exist?</p> <ul style="list-style-type: none"> ✓ The client (Business or Agent) has notified the ATO of their Hosted SBR software service provider in Access Manager. ✓ The client's ABN sent in the transmission and DSP ABN (in the machine credential) are related by the notification.
	Step 4	<p>Does the Software ID match the notification?</p> <ul style="list-style-type: none"> ✓ The client (Business or Agent) has entered a software ID against the notification in Access Manager. ✓ The Software ID sent in the transmission matches that against the notification in Access Manager.
	Step 5	<p>Has the notification been disabled?</p> <ul style="list-style-type: none"> ✓ The notification has not been disabled by the DSP in Access Manager
Determine if the intermediary is authorised to act on the client's behalf	Step 6	<p>If an intermediary sent the transmission, are they authorised?</p> <ul style="list-style-type: none"> ✓ The intermediary (eg registered tax agent or Business Intermediary) is authorised to act on the clients behalf.
Step 7 - Lodgment Accepted		







Appendix F

Lodgment scenarios

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





1 - Business lodging from their own subscription

Data Fields	
Machine credential ABN	
Intermediary ABN/TAN	
Reporting Party ABN	
Software ID	

The ATO will check if:

- a notification exists between Reporting Party (ABN) and DSP (machine credential ABN), and
- the Software ID relates to the Reporting Party (ABN) notification.

2 - Agent lodging from their own subscription on behalf of a client

Data Fields	
Machine credential 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 DSP (machine credential 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).

No Relationship Check Forms (NRCF)

NRCF 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. NRCF include TFN Declaration (TFN Dec), Taxable Payment Annual Report (TPAR) & PAYG Payment Annual Summary (PSAR).

The DSP can continue to use their machine credential to secure NRCF transmissions without a Software ID. *This will negate the need for their clients to notify the ATO of the software providers services.*

Appendix G

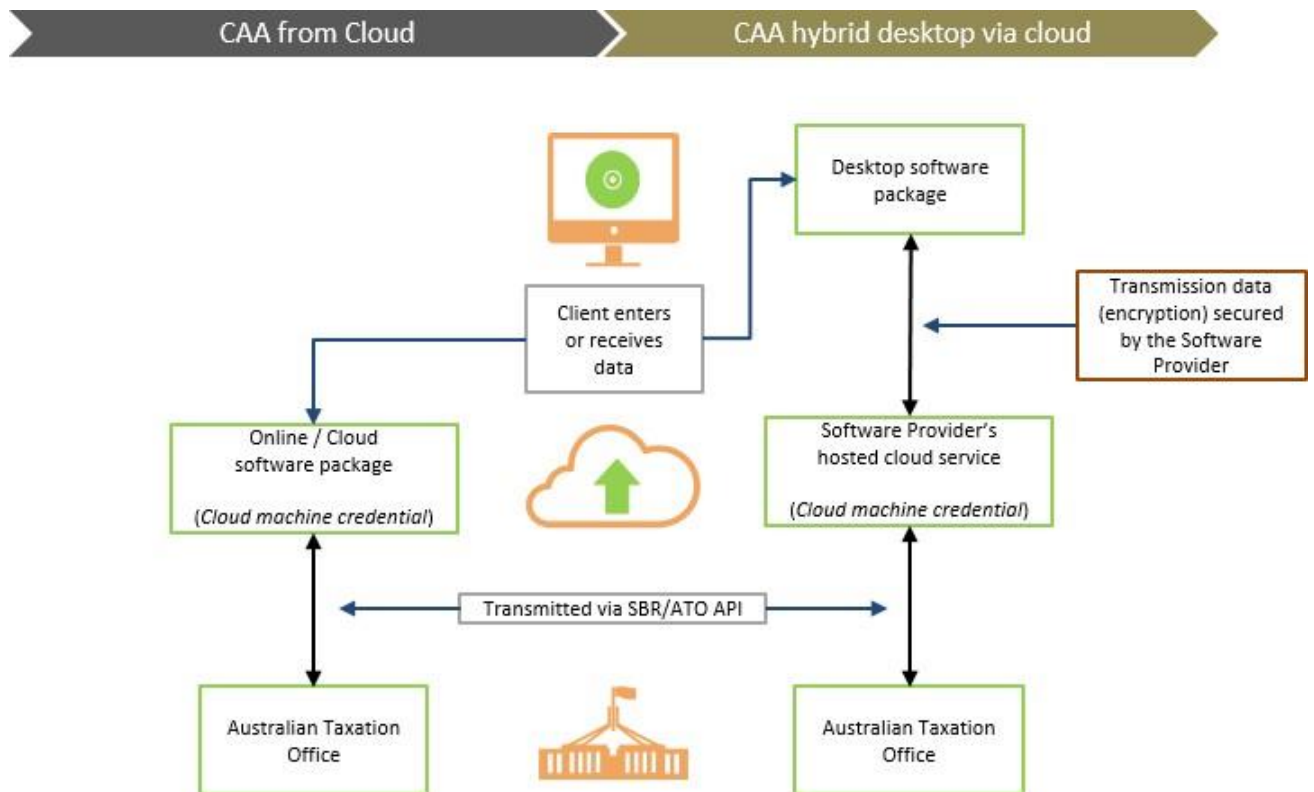
Hybrid desktop via cloud software

The CAA solution can be leveraged using hybrid desktop via cloud software, although this is a diminishing model.

Users of hybrid desktop via cloud software can experience the benefits of CAA and can submit information to the ATO without needing their own machine credential. The software providers machine credential 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.

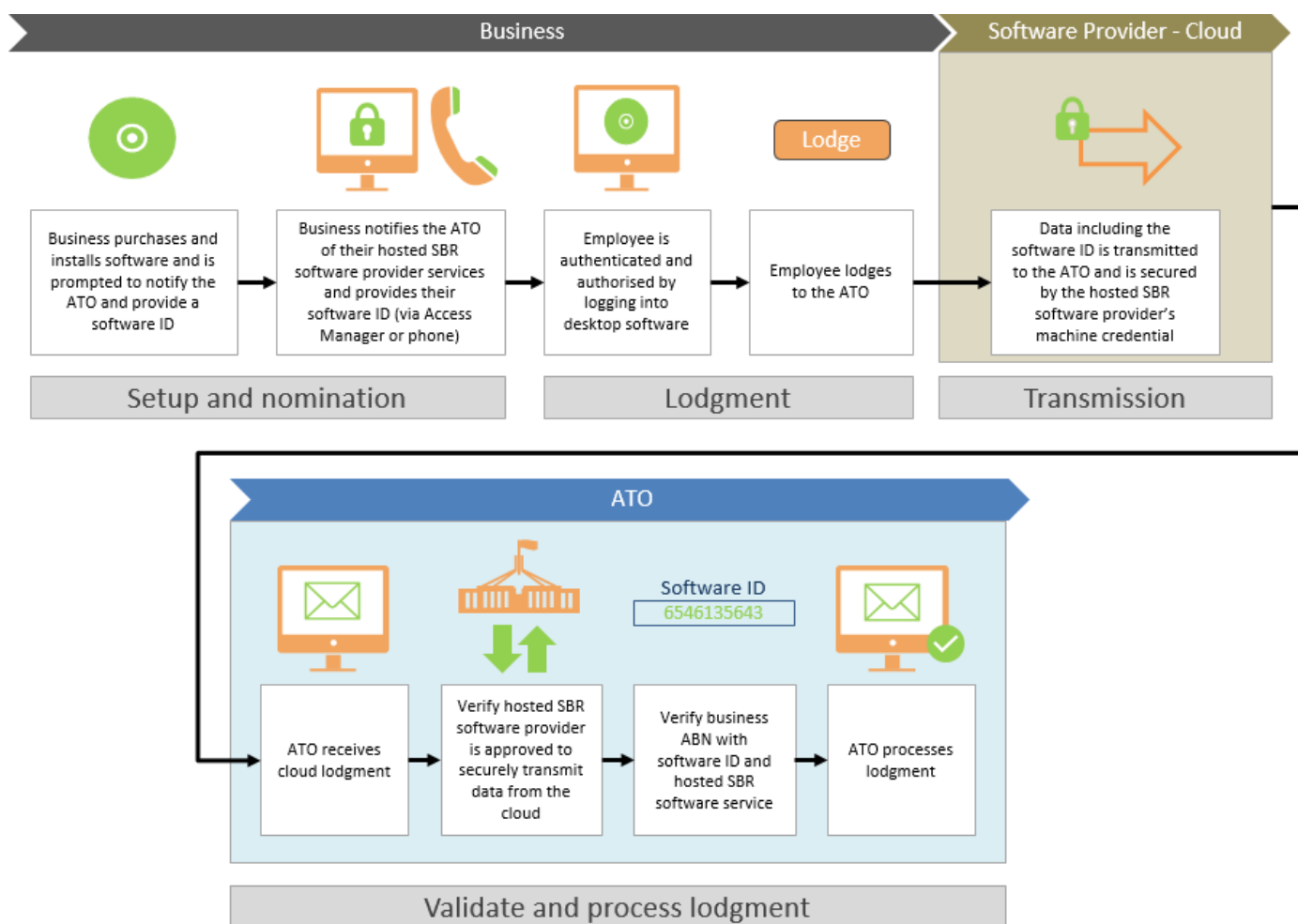
The hybrid desktop via cloud design:

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





Lodgment by "business" using hybrid desktop via cloud software





Appendix H

Frequently Asked Questions (FAQ)

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