



Australian Government
Australian Taxation Office

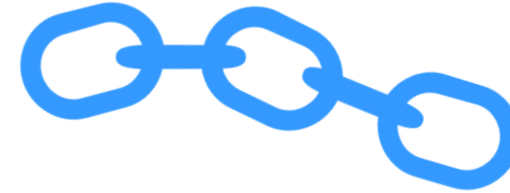
Digital Identity for DSPs

Identity assurance between ATO partners and their customers

Digital Identity for DSPs

Vision

To protect the community from identity related fraud through strong links in the supply chain.



Customer verification and identity crime

Inconsistent and insufficient customer verification processes can lead to identity crime. This enables criminals to use a fraudulent identity to commit 'other' crime, including financial crime through the tax and super systems.

Problem Statement

1. It is unclear who's responsibility customer verification is, within the various relationships and links in the supply chain
2. There is no simple or holistic solution for a DSP or business user to access a reliable and independent data source to accurately verify the identity of an individual and establish any authorised relationship they have with a business entity
 - a. The DTAs trusted digital identity framework (TDIF) and digital identity ecosystem has not yet reached a level of maturity to support DSPs.
 - b. DVS and myGovID systems are predominantly region specific (Australia) and a number of exceptions exist where individuals are unable to meet the identity requirements e.g. foreign resident with no Australian documentation.
 - c. RAM is currently only available to government agencies and business users are unable to access RAM to verify an authorised relationship.

Participants in the supply chain

ATO

As the tax and superannuation regulator, the ATO would like to have assurance customer verification and appropriate authorised relationship checks occur, when a relationship is established to facilitate the following actions:

- DSPs provide access to a business user to interact with the ATO
- DSPs provide services to access client data or register a new entity
- Business transacts with each other where it relates to a supply or acquisition
- e-invoices are sent between business and supplier/customer
- Registered agents agree to act on behalf of a customer and add a them to their client list

Possibilities of where customer verification may need to occur

DSP

Product registration for new business customer/user

- business (individual or non-individual entity) registers
- entity has an individual (legal) representative
- individual representative has a relationship with the entity

DSP is also a business, supplier and customer in its own right and uses software to manage business operations

- has employees who require access to product
- has suppliers they would like to verify identity of

DSP partners with another DSP, provides access to their product or consumes another within their own

Business

Business purchases software to manage business operations

as a Business user

- has employees who require access to product
- has suppliers they would like to verify identity of

as a Registered Agent

- has employees who require access to product
- has suppliers they would like to verify identity of
- has individual and non-individual customers they would like to verify identity of

Suppliers & Customers

Suppliers and customers interact with business, this could occur through software

as a Supplier

- sells products to business and may need to verify the identity of that business
- sells products to business and needs to prove own identity to business

as a Customer

- purchases goods or services from a business or registered agent
- needs to prove identity to business or registered agent
- if non-individual, needs to prove individual relationship to entity

Decisions following the meeting

Points of confirmation:

- Initially, the scenarios discussed have been based around using simple and common situations e.g. Business user subscribes to access a software product.
- The group is only discussing customer verification options at the establishment of the relationship, not for every transaction.
- Recognition of current authorisation and authentication that occurs through software - a machine credential is required for a business to transact with the ATO through software. Machine credentials are created in RAM by an authorised administrator who has been authenticated using their myGovID. Where cloud software is used an authorised administrator of the business must notify the ATO of the relationship (add an SSID) through AM using their myGovID, or by phone, after having passed an ATO PORO process.

DSP

- It is in the best interest of DSPs to validate the entity is a legitimate entity when a new customer is signed up e.g. through the ABN lookup or similar service action
- It is in the best interest of DSPs to ensure at least one if not more contacts have verified contact details e.g. email and phone numbers are verified
- Recognition that confirming the relationship between the contact and the entity would be beneficial but this is not a readily available option right now e.g. this could be considered when MBR or TDIF and digital identity infrastructure or services are more mature
- Whilst there is no responsibility to provide a full customer verification process, DSPs may be able to implement support functionality for their clients e.g. to capture, maintain or report on records of completion, document type, date or other items in their software

Business

- There is a need for businesses to complete customer verification when onboarding new clients
- There should be no requirement to complete customer verification at every transaction
- Businesses agree to terms of use with DSPs when purchasing and registering software

Suppliers & Customers

- There is a need for suppliers to complete customer verification processes when on-selling software to customers
- e-invoicing – responsibility for customer verification is covered by the PEPPOL framework in place and the Australian Peppol Authority has issued a guidance note that provides instructions on how Access Point (AP) Providers and Service Metadata Publisher (SMP) Providers in Australia and New Zealand can meet the requirements of the KYC principle in the PEPPOL Compliance Policy. However, recently Peppol has issued a new draft policy which the Australian Peppol Authority is reviewing and assessing the need to update the previous guidance