Australian Government
Australian Taxation Office

# Digital Service Provider (DSP) Operational Framework Review

## Authentication Focus Group – Session 2

Presented by Diana Porter

24th March 2021

# Recap - What we are trying to achieve?

To identify and explore opportunities to improve authentication controls including Customer Verification & Multi Factor Authentication (MFA).

## 1 Entity Validation & Customer verification

a. Entity validation between DSPs and clients
b. Supporting customer verification within software

## 2 Expansion of MFA

a. In client controlled desktop environments
b. In DSP controlled environments

## 3 Improved guidance for MFA

a. Authentication hardening controls
b. Single-sign on

# 1 Entity Validation and Customer Verification

- a Supporting entity validation between DSPs and clients
- b Supporting customer verification within software

# 1a Supporting entity validation between DSPs and clients

## REVIEW CONSIDERATIONS

**Support for entity validation which will provide pathway to customer verification**

**Challenges in applying to desktop software**

**Frequency of entity validation**

**Exceptions to validation to be considered i.e. clients with no ABN**

## CURRENT ENVIRONMENT

No operational framework requirement for entity validation between DSPs and clients.

## UPDATE – RECOMMENDED REQUIREMENT

This requirement seeks to prevent unauthorised access to taxation, payroll and superannuation related information.

Entity validation establishes that the business registering to use software is the registered entity as per the Australian Business Register (ABR).

Entity validation will occur at registration or when there is a change in subscription. To complete entity validation you will need to verify the entity against reliable and independent sources, which may include ABN Lookup, website/URL, domain specific email addresses or media advertisement.

As part of entity validation you will also need to establish that the individual registering is contactable through corporate email or company phone.

Exceptions to entity validation may include users who do not have an ABN, are a student i.e. university/TAFE student using software for their course, or are using a product outside DSP Operational Framework scope.

**Evidence required**

Provide details of your onboarding or registration process.

# 1b Supporting clients record customer verification within software

## REVIEW CONSIDERATIONS

**Explore opportunities to support customer verification within software**

**No simple digital solution that links an individual to an entity**

## CURRENT ENVIRONMENT

No operational framework requirement for customer verification. There is no commercial digital solution available that links an individual to an entity.

Some DSPs apply principles of customer verification to verify an individual as part of SuperMatch Terms and Conditions.

No requirements under AML/CTF Legislation for DSPs.

## UPDATE

Not yet a requirement as ATO are currently working to expand customer verification.

As agreed in session one DSPs will support their clients to record customer verification within software.

Draft example of records include the below:

- When: Date and time
- Who: User who completed customer verification
- What: Identity documents were used
- How: Face-to-face, virtual, other

# 2 Expansion of MFA

- a In client controlled environments
- b In DSP controlled environments

# 2a Expansion of MFA in client controlled environments

## REVIEW CONSIDERATIONS

**Challenges and costs in implementing for desktop software**

**Decision to apply to all users is risk based.**

**Explore broadening scope**

## CURRENT ENVIRONMENT

DSP Operational Framework Requirements to utilise ATO digital services (pg. 6, 8 & 20-21)

MFA is optional for all users in client controlled environments.

Client controlled environments include:

- A software product hosted on the client's premise (e.g. desktop, local server or private cloud solutions)
- A software product hosted on infrastructure that is outside the clients premise but is controlled by the client (e.g. Infrastructure as a Service)
- A single instance of a software service that is hosted by the DSP in a single or multi-tenant infrastructure where the client has sole control of the application and control and ownership of the data.

# 2a Expansion of MFA in client controlled environments

## REVIEW CONSIDERATIONS

**Challenges and costs in implementing for desktop software**

**Decision to apply to all users is risk based.**

**Explore broadening scope**

## SUGGESTED UPDATE

MFA remains optional in all client controlled environments, however desktop solutions should have user based log and permissions.

This uplift will target client-controlled cloud environments, Infrastructure as a Service (IaaS) & Platform as a Service (PaaS) and hybrid web-based solutions.

MFA is required for users who access records that are not their own or who are privileged users, in the below client controlled environments:

- A software product hosted on infrastructure that is outside the clients premise but is controlled by the client (e.g. Infrastructure as a Service)
- A single instance of a software service that is hosted by the DSP in a single or multi-tenant infrastructure where the client has sole control of the application and control and ownership of the data.

This aligns to Australian Government ISM controls 1504, ACSC - Authentication Hardening.

## EXAMPLES MAY INCLUDE

DSP provides a desktop product but also provides remote access services.

Hybrid web based solutions including mobile applications.

# 2a Expansion of MFA in desktop environments

## REVIEW CONSIDERATIONS

**Challenges and costs in implementing for desktop software**

**Decision to apply to all users is risk based.**

**Explore broadening scope**

## UPDATE

MFA remains optional in desktop, however desktop solutions must have user based access, authentication and authorisation controls implemented.

Note: The ATO intends to progress an uplift of MFA to be applied to desktop products and DPO will continue consultation with industry over 6-12 months, to identify an appropriate future solution.

# 2b Expansion of MFA in DSP controlled environments

## REVIEW CONSIDERATIONS

**Decision to apply to all users is risk based.**

**Explore broadening scope**

## CURRENT ENVIRONMENT – DSP CONTROLLED

DSP Operational Framework Requirements to utilise ATO digital services (pg. 10 & 20-21)

In DSP controlled environments MFA is applied as a role based control and is applicable when users access client records that are not their own, or when they are privileged users.

For example a Tax/BAS agent lodging a BAS on behalf of their client.

## UPDATE – ACCESSING MEDIUM (3) OR HIGH RISK (4) APIs

MFA required for all users when accessing high risk APIs as per ATO Service Registry.

For example if an individual accesses their own pre-fill data then MFA will be required.

## 3 Improved guidance for MFA

- a Authentication Hardening Controls
- b Single-Sign On

# 3a Authentication Hardening controls

## REVIEW CONSIDERATIONS

**Discrepancy in 'remember me' timeframe exists**

**Guidance required around use of SMS for MFA**

**Timeframe impacts on user experience**

**Consistent standard for session timeouts to be applied across industry**

## CURRENT ENVIRONMENT

DSP Operational Framework Requirements to utilise ATO digital services (pg. 21)

- End users are those individuals, external to the DSP, who actually use the product or service.
- DSP staff are those staff (including contractors) working for or on behalf of the DSP.
- The ATO may consider exceptions to mandatory MFA for end users of DSP hosted products/services in extenuating circumstances.
- Where the transaction is authenticated within a machine to machine interaction, multi-factor authentication (MFA) is not applicable.
- Tokens or temporary credential should be isolated to an individual device and expire once used. Any token or temporary credential should expire within 24 hours.
- DSPs that have not implemented MFA, should consider implementing good passphrase practices including single factor authentication controls, account lockouts, resetting passphrases, session and screen locking as described in the Australian Government Information Security Manual (ISM)
- A privileged user is defined as a user who can alter or circumvent a system's security measures – this may include the capability to modify system configurations, account privileges, audit logs, data files or applications.

# 3a Authentication Hardening controls

## REVIEW CONSIDERATIONS

**Discrepancy in ‘remember me’ timeframe exists**

**Guidance required around use of SMS for MFA**

**Timeframe impacts on user experience**

**Consistent standard for session timeouts to be applied across industry**

## PROPOSED CHANGES

- Remember me functionality must be limited to 24 hours maximum.
- Enforcement of brute force lockouts are applied after a maximum of 5 unsuccessful login attempts.
- Credentials are stored separately from the system which grants access.
- Confirmation passwords are hashed, salted and stretched.
- Session time-out occurs after 15 minutes.

ACSC Authentication Hardening includes additional guidance to support DSPs implementation.

**Note:** Short Message Service(SMS), are more susceptible to compromise by an adversary than others. As such the ATO recommends utilising an alternative authentication factor when viable to do so.

### Evidence required

All of the below requirements to be provided:

- User description paired with screen shots of MFA workflow; and
- User access controls including remember me, session time-out, brute force lockouts; and
- Password or access control policy.

# 3b Single-Sign On

## REVIEW CONSIDERATIONS

**SSO has been supported by exception for DSPs**

**Clarification around social media signing on in this context**

**Definition of enterprise customer to be based on number of transactions/records**

**Increased interest for SSO by tax practitioners**

## CURRENT ENVIRONMENT

DSP Operational Framework Requirements to utilise ATO digital services (pg. 21)

**Enterprise Customers**

By exception, DSPs must seek advice from the ATO on the use of Single Sign On (SSO) for enterprise customers that access a DSP's system from behind their enterprise firewall. SSO must be controlled by the DSP and only enabled for a customer where the below controls are in place. In considering whether to support SSO for their customers, DSPs must ensure that that the customer:

- Is an enterprise that has control over the access management solutions e.g. (does not use social media as a sign in).
- Has strong encryption in place e.g. TLS1.2.
- Has a password or passphrase management policy, covering length and complexity including salt, hashing.
- Enforces brute force lockout.

# 3b Single-Sign On

## REVIEW CONSIDERATIONS

**SSO has been supported by exception for DSPs**

**Clarification around social media signing on in this context**

**Definition of enterprise customer to be based on number of transactions/records**

**Increased interest for SSO by tax practitioners**

## PROPOSED CHANGES

### Enterprise Single-Sign On (SSO)

By exception, DSPs must seek advice from the DPO on the use of enterprise SSO to support their clients.

In implementing Enterprise SSO DSPs must ensure that:

- Disablement of MFA is controlled by the DSP, not their client.
- Clients align to requirements of MFA as per the Operational Framework.
- SSO tokens must be limited to a maximum period of 24 hours.
- Encryption in transit between client's system and software uses as an approved protocol as per the ACSC - Guidelines for using Cryptography e.g. TLS 1.2 or 1.3.
- SSO occurs behind clients enterprise firewall i.e. gateway.

SSO can be adopted between you and your clients, on the provision you meet the above criteria in line with ACSC MFA Guidelines.

# Open Discussion & Thankyou

## Summary for working group

- Will changes address specific outcomes relating to:
    - Entity Validation, & Customer Verification
    - Expansion of MFA
    - Improved guidance for MFA
- Are there any other concerns or gaps we haven’t been able to address?
- Closure of Authentication working group?

## Next steps

1. Incorporate feedback and finalise changes within the draft requirements documentation.
2. DPO will provide draft documentation for review by DSPs.