Australian Government
Australian Taxation Office

Key Outcomes

OFFICIAL External

Title:	Digital Service Provider, Operational Framework Review Authentication Focus Group Focus Group		
Issue date:	6 May 2021		
Venue:	WEBEX		
Event date:	24 March 2021	**Start:** 11:00	**Finish:** 13:00

Chair:	Diana Porter	**Facilitator:**	Diana Porter
Contact:	Julie Huynh	**Contact phone:**	(02) 8894 9304

Intent:	Identify and explore opportunities to improve Authentication

Attendees:

ATO
Diana Porter, Operational Framework Lead, DPO
Toby Amodio, Assistant Commissioner Cyber Security
Miranda Shaw, Director, Information & Cyber Security
Fiona Homan, Director, Information & Cyber Security
Joda Walter, ICS Lead, Information & Cyber Security
Paul Walters, IT Relationship Manager, DPO
Operational Framework Team

Industry

Australian Super Funds Association	Paul Larsen
Cashflow Manager	Tim Covark
Class Super	Philip Boadi
Datacom Solutions	Doreen Bhamii
Institute of Certified Bookkeepers	Matthew Addison
Intuit	Matt Lewis
MYOB Australia	Mike Behling
Sage Software Australia	Michael Wright
Sunsuper	Stephen Milburn
Superchoice	Chris Denney
Thomson Reuters	Mary Yeruva

	Total Forms	Jack Wee
	Xero	Erin Adams
	Xero	Matthew Prouse

Apologies:	ABSIA	Simon Foster
	AMP	Andrew Strong
	Australian Super Funds Association	Hans van Daatselaar
	Iress	Ross Daws
	Link Administration Holdings	Matt Rea
	Qvalent	Grant Doherty
	Tanda	Roderick Schneider
	Xero	Helen MacGillivray

Next meeting	N/A

The key outcomes for this meeting are best read along with the Authentication focus group presentation.

Agenda item: Introduction

Three key themes were discussed including an overview of feedback from the first session on:

1. Entity Validation & Customer Verification
2. Expansion of MFA
3. Improved Guidance for MFA

DPO will consider feedback from the group when finalising updated guidance.

Agenda item: 1 – Entity Validation & Customer Verification

The group discussed previous feedback on supporting guidance for Entity Validation & Customer Verification

a) Entity Validation between DSPs and clients

b) Supporting Customer Verification within software

DPO recognises it is difficult for a DSP to undertake customer verification of an individual and link that individual to a business through currently available identify solutions. For example, the way ATO uses myGovID and RAM. Within the Digital Identity for DSPs working group it was agreed DSPs would undertake validation of an entity as a legitimate business (e.g. confirm valid ABN) instead of undertaking customer verification and linking to business.

a) Entity Validation between DSPs and clients

- The intent of Entity Validation is to ensure the consumer/user of a commercial software product is a legitimate business and has a genuine need to access ATO APIs. Additionally, the business should have a valid contact person with contact details. (this should be email and phone)

b) Supporting customer verification within software

- Entity Validation must be implemented by DSPs at registration or subscription renewal.
- DPO recognise that exception will occur e.g.
  - Trial users of software
  - Individuals not in business (no ABN)
  - Students / Research
  - Desktop products with no registration process

Outcome from industry discussion:

- The group discussed outcomes from the Digital Identify for DSPs Working Group which included the new customer verification requirements placed on Tax Professional community. DSPs that provide Practitioner Lodgment Software (PLS) should support capturing / documenting customer verification for their clients.

Further consideration needed for:

- Nil

Agenda item: 2 – Expansion of MFA

The group discussed previous feedback on supporting guidance for Entity Validation & Customer Verification

a) In client-controlled environments

b) In DSP controlled environments

a) In client-controlled environments

a. No change to the technical control within the DSP OPF at this stage, MFA remains optional but recommended.

b. DPO will undertake further consultation with DSP over the next 12 months to determine an appropriate uplift and timeframe for MFA to be implemented in desktop environments.

b) In DSP controlled cloud environments

- Proposed changes to expand MFA for an individual logging into their own information using a risk-based model. For example:
  - Implement MFA if accessing information contained within a high-risk service i.e. IITR prefill
  - MFA not required if accessing information containing within a low risk service i.e. Pay Event
- The group discussed a risk-based model would overcomplicate the process and agreed that MFA should be uplifted to protect the integrity of all client data when accessed via a DSP Controlled / Cloud environment.

Outcomes from industry discussion:

- MFA will be uplifted to ensure any user accessing any data from within a DSP controlled / cloud environment will require MFA as mandatory.
- Timeframes for transition were discussed with the group and clarification was provided. The requirement to implement this change would be in line with all other changes of the DSP OPF review.

- "From the time the requirements are published as final, changes must be implemented by each DSP by their next annual review. Consideration will be given on a case by case basis to any DSPs who has recently completed their annual review e.g. within the last 6 months".

Further consideration needed for:

- Nil

Agenda item: 3 – Improved Guidance for MFA

The group discussed previous feedback on improved guidance for:

a) Authentication Hardening Controls
b) Single Sign On

a) Authentication Hardening Controls

- 'Remember-me' functionality must be limited to 24 hours maximum.
- DPS to demonstrate a brute force lockout process is in place, following unsuccessful password attempts i.e. set to a maximum of 5 unsuccessful log in attempts.
- Credentials are stored separately from the system which grants access.
- Confirmation passwords are hashed, slated and stretched.
- 'Inactivity' clarified for web applications. E.g. multiple tabs with on-going inactivity of 15 minutes may trigger timeout and DSPs will need to re-authenticate. To maintain security and integrity of Taxation and Superannuation data.
- The group discussed alignment of standards for Online Service for DSPs. This setting is currently set at 60 minutes. Once you are logged in to a service i.e. Jira the service time out of 60 minute applies. It is recommended the device is not idle with an unlocked screen for this entire duration and compensating controls are in place i.e. strong passwords and lock screen timeouts.
- Note: myGovID app is set at 15 minutes, once you're logged in to the application, the timing of your session will depend on the service you're accessing and how long you remain active. If you're inactive for a certain amount of time you will automatically be asked to log in again and re-authenticate. Reference www.mygovid.gov.au
- ACSC Authentication Hardening includes additional guidance to support DSPs implementation of Authentication Hardening Controls.

b) Single Sign On

- Disablement of MFA is to be controlled by the DSP.
- Clients align to requirements of MFA.
  - SSO tokens to be limited to 24 hours inactivity.
  - Encryption in transit between client's system and software uses an approved protocol i.e. TLS 1.2 or TLS 1.3.
  - DPO will provide definition of the end user and privileged users.
  - Logs to be kept for a minimum of 12 months.

- ATO will not prescribe guidance material for SSO from social media platforms, this relationship is between the DSP and the client. ATO recommends MFA be implemented as an authenticator.
- The SSO requirement is an exception and DSPs must seek advice from the ATO on use. This position has not changed.

Outcomes from industry discussion:

- Uplift of SSO requirement and alignment of standards to ACSC guidelines i.e. SSO tokes to be limited to 24 hours of inactivity.
- Additional link to ACSC guidelines to implement MFA to be included in guidelines.
- DPO will provide additional guidance within the requirements documentation.

Further consideration needed for:

- Nil

Agenda item: Wrap Up & Next Steps

Outcomes of working group to be published and circulated.