Key Outcomes

Title:	Operational Framework Review – Authentication Focus Group		
Issue date:	3 December 2020		
Venue:	WEBEX		
Event date:	24 November 2020	**Start:** 11:00	**Finish:** 13:00

Chair:	Diana Porter	**Facilitator:**	Kylie Johnston
Contact	Diana Porter	**Contact phone:**	(02) 4724 0528

Attendees: names/section	ATO Kylie Johnston – Director, Digital Partnership Office Miranda Shaw – Director, IT Security Sangitha Sivayogaraj - Director, Digital Wholesale Integration Diana Porter - Digital Partnership Office Karen Spicer - Digital Partnership Office Jarrod Wellings - Digital Partnership Office Industry Chris Denney - SuperChoice Chris Howard - Australian Business Software Industry Association Doreen Bhamji - Datacom Solutions Grant Doherty - Qvalent Hans van Daatselaar - Australian Super Funds Association Helen MacGillivray - Xero Jack Wee – Total Forms Mary Yeruva – Thomson Reuters Matt Rea - Link Administration Holdings Matthew Addison - Institute of Certified Bookkeepers Matthew Prouse - Xero Michael Wright - Sage Software Australia Mike Behling - MYOB Australia Philip Boadi - Class Super Simeon Duncan - Intuit Stephen Milburn - Sunsuper Tim Covark - Cashflow Manager

Apologies: name/section	Claire Miller - Director, Digital Communication & Identity Services Paul Dwyer – Director, Digital Wholesale Integration Toby Amodio - Director, IT Security

Next meeting	TBA

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

Agenda item: 1 – Introduction

An overview of findings from independent review and DSP feedback included 4 opportunities to improve authentication controls

These include:

1. customer verification & entity validation
2. exploring the expansion of MFA
3. opportunities to improve guidance
4. M2M credential

Agenda item: 2 – Customer Verification & Entity Validation

The group discussed opportunities to improve authentication controls for customer verification between DSPs & clients and supporting end user clients in software.

A Digital ID for DSPs working group was established separately based on action items raised with ATOs strategic level working groups. The group discussed the options and responsibility to undertaken customer verification of entities registering with DSPs to consume products that connect to ATO. Outcomes include:

- Customer verification includes individual identity validation, entity validation and the confirmation of the relationship between the individual and the entity.
- Whilst there are a few options available to business to undertake individual identity validation there is no simple solution for verifying a relationship between individual and entity exists covering all types of entities.
- DSPs agreed they could support entity validation rather than customer verification.
- Entity validation will provide a future pathway that supports customer verification when additional solutions are available.
- DSPs also agreed they could support Tax Professionals through their PLS products to record details of customer verification undertaken. This would be based on future outcomes required through ATO discussions with Tax Professional industry in 2021.

Key points from industry discussion and feedback included:

- Challenge of applying entity validation to desktop software.
- Frequency of customer verification - initial registration and when changes occur, re-verification annually.
- Transitional timeframe to be considered for existing users.
- Exceptions to validation to be developed covering items such as:
    - using a product outside scope of Operational Framework
    - if the user is a student
    - If user does not have ABN
    - free-trial user

Agenda item: 3 – Exploring the Expansion of MFA

Discussion on opportunities and feasibility of expanding MFA to all environments and users.

Key points from industry discussion and feedback included:

- Expanding MFA to secure all software and its users is a positive step for the industry.
- Definition of '*tax or superannuation'* related information is required, questions related to implementation of MFA to access software is unclear including:
    - the actual data vs a screenshot of that information
    - distinction of personal information that could be '*tax or superannuation'* related
    - inclusion of document storage facilities, Dropbox, Google Drive etc, which may contain '*tax or superannuation'* related information
- Consideration should be given to the following if expanding MFA to more environments including desktop:
    - concerns MFA will not address risk for desktop software
    - define the risk being managed by applying MFA to desktop
    - there will be significant impacts on cost, service availability and time for DSPs to enforce the control
    - nuances of applying MFA to different desktop products requires further investigation with ATO internal IT security team
    - Decision to apply to all users to be risk based.

Agenda item: 4 – Opportunities to Improve Guidance

Discussion on opportunities to improve guidance for 'Remember me' functionality & cookies and Single Sign On.

Remember me & cookies

- Some DSPs apply up to 30-day remember me functionality to their software which provides for positive (or less negative) user feedback.

- Some DSPs have implemented a 24-hour remember me functionality and although there has been some negative feedback from users, DSPs have managed this in the interest of stronger security.
- There is a lack of guidance around the use of SMS as an insecure second factor authentication.
- Request for a consistent standard around the duration of remember me and timeouts is required.

Single Sign On

- Some DSPs have been asked to remove MFA and support single sign on provisions. A few have advised their customers 'No' it is a requirement of ATOs DSP Operational Framework, a few have approached DPO for consideration and guidance. DPO has supported an approach for exceptional circumstances for some of the requests.
- The definition of 'Enterprise Customer' needs to be established e.g. number of transactions/records.
- Clarification around what social media sign on in this context
- There is a growing interest for SSO by Tax Practitioners.

Agenda item: 5 – M2M Credentials

Scheduled time did not allow for a full discussion and update on the gaps with M2M credentials and it will continue in session 2.

It was noted this item overall will be discussed outside of Operational Framework as it has broader Digital Identity aspects.

DPO confirmed no immediate changes are expected, the conversation was to obtain feedback from industry on the potential risks of M2M credentials including those stored on local servers where multiple client have access, potentially without MFA or user logins.

Agenda item: Wrap Up & Next Steps

Outcomes of the focus group to be published and circulated, members are encouraged to provide further feedback and comment.

ATO will establish a second meeting in December.