Australian Government
Australian Taxation Office

Digital Service Provider (DSP) Operational Framework Review

Operational Framework Review Focus Group – Authentication

Presented by Kylie Johnston, Diana Porter, Karen Spicer & Jarrod Wellings

24 November 2020

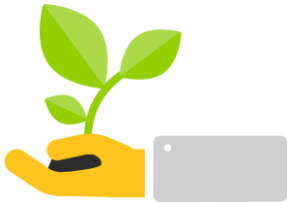
What are we trying to achieve?

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

1 Customer Verification & Entity Validation

A. Customer verification between DSPs and clients
B. Supporting end user clients within software

2 Exploring the Expansion of MFA

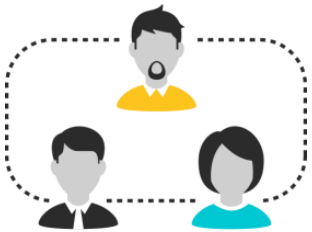


Explore feasibility to expand MFA to all environments and users

3 Opportunities to Improve Guidance

A. ‘Remember me’ Functionality & Cookies
B. Single Sign-On

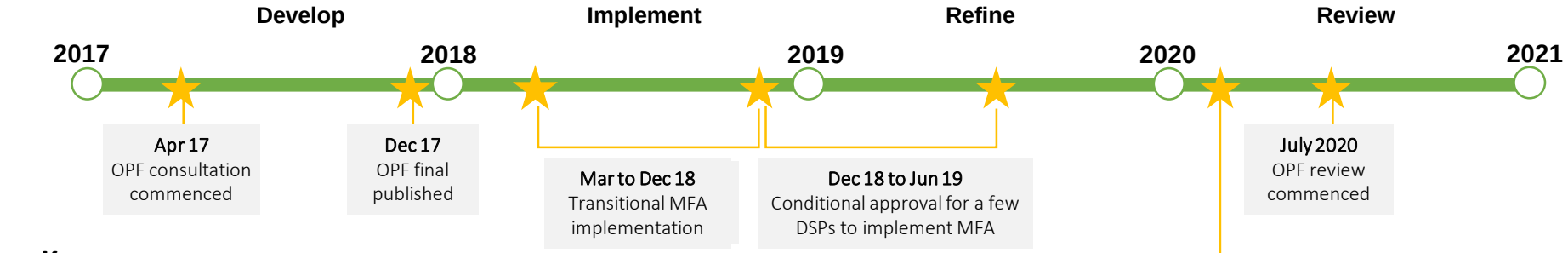
4 M2M Credential



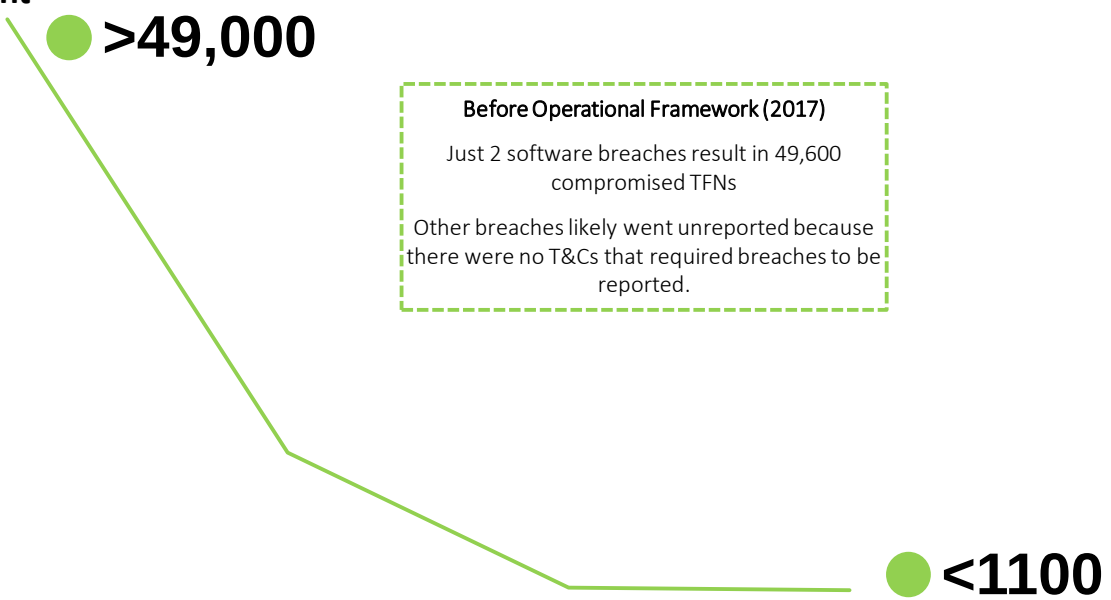
Explore feasibility to identify individual user of M2M credential

Our Journey for Operational Framework - Authentication

Timeline



Key Achievement



Before Operational Framework (2017)

Just 2 software breaches result in 49,600 compromised TFNs

Other breaches likely went unreported because there were no T&Cs that required breaches to be reported.

April 2020
Increased compromised identity

After Operational Framework and MFA implementation (2020)

19 Software breaches result in 1065 compromised TFNs/ABNs

T&Cs exist for DSPs to report **all** breaches

1. Customer Verification & Entity Validation
   - A. Customer verification between DSPs and clients
   - B. Supporting intermediaries & clients with recording customer verification

Outcome from Digital ID Working Group on Customer Verification and Entity Validation

A How could DSPs implement entity validation which supports a future pathway to customer verification?

Customer Verification	Entity Validation
Confirm identity of individual	ABN validation
Confirm validity of entity	Confirm at least one contact person with validated contact details e.g. email, phone number, address
Confirm link between individual and entity	

How would it work? What are the principles?

Supporting intermediaries & clients with recording customer verification

B It's important software can capture and support governing controls for customer verification processes between intermediaries and their clients

Ability for agents to capture the details of customer verification completion within software:

- who
- when
- what
- how

Discussion?

2 Explore the Expansion of MFA

Current State of Multi Factor Authentication

This requirement seeks to minimise the opportunity for unauthorised users to access taxation or superannuation related information.

How MFA is currently applied

	Access others data	Only access own data	Privileged User
Client Hosted	✗	✗	✗
DSP Hosted - End User	✓	✗	✓
DSP Hosted - DSP Staff	* ✓	✗	✓

Mandatory ✓ Optional ✗

How MFA is implemented

*MFA is mandatory for DSP staff with access to taxation or superannuation related information. This position applies unless the DSP can adequately demonstrate that the internal user does not perform a privileged administration role (system / database level) and the full range of compensating controls specified within the Australian Government Information Security Manual (ISM) have been suitably implemented.

Multi Factor Authentication

Opportunities to expand MFA to all environments and users

Expand MFA to include all users of data to:

- Reduce the likelihood and impact from an account take over event
- Reduce data breaches
- Reduce fraudulent activities
- Reduce compromised credentials

Risk Rating of APIs

Volume of Records

Cloud & Desktop

Discussion?

3 Opportunities to Improve Guidance

- A ‘Remember me’ Functionality & Cookies
- B Single Sign-On

Opportunities to Improve Guidance

A ‘Remember me’ Functionality & Cookies

Current requirement and application

The ATO currently recommends the token or temporary credential used for MFA should be isolated to an individual device and expire within 24 hours.

There is a wide discrepancy between DSPs and the length of time remember me is enabled for.

Opportunity for improvement

Have a risk based approach to set minimum timeframes across industry for cookies.

Find a balance between security and usability

Discussion?

Opportunities to Improve Guidance – Single Sign On

C Refining Single Sign On

Current process

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

SSO enables users to securely authenticate with multiple applications, by logging in only once.

The solution internally stores the various credentials for every piece of software that the user needs to access and validate that user with those systems.

Opportunities to improve documentation

Definition of Enterprise Customer

Improve existing evidence requirements

Discussion?

4 Machine to Machine (M2M) Credential

Machine to machine (M2M)credentials

Discuss opportunities to identify the individual user of M2M credential

When a M2M credential is stored on a server which multiple end users have access to, how do we identify the end user?

Do DSPs already have something in place to identify the end user?

How could we improve the consistency of the identification process across all solutions?

How could the Operational Framework requirements cover this?

Discussion?

Summary & Actions

Summarised Outcomes

1. Customer Verification & Entity Validation
2. Exploring the Expansion of MFA
3. Opportunities to Improve Guidance
4. Explore feasibility to identify individual user of M2M credential