Australian Government
Australian Taxation Office

OFFICIAL External

Key Outcomes

Title:	Digital Service Provider, Operational Framework Review Supply Chain & Payload Encryption Focus Group
Issue date:	6 May 2021
Venue:	WEBEX

Event date:	10 March 2021	**Start:** 10:00	**Finish:** 11:00

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

Intent:	Explore opportunities to improve integrity of transaction over ATO gateways

Attendees:

ATO
Kylie Johnston – Director Digital Partnership Office (DPO)
Diana Porter – Operational Framework Lead, DPO
Operational Framework Team – Digital Partnership Office

Industry

ABSIA	Simon Foster
Commonwealth Bank Australia	John Kennedy
GNGB	Michelle Bower
Layer Security	Rick Harvey
MessageXchange	Helena Bone
Ozedi	David Field
QSuper	Mark Freestone
QSuper	Stephen Milburn
QValent	Grant Doherty
Superchoice	James Cameron
Superchoice	Chris Denney
Xero	Erin Adams
Xero	Helen MacGillivray
Xero	Matthew Prouse

Apologies:	AMP	Andrew Strong
	Automatic Data Processing	Michael Pogrebnoy
	Commonwealth Bank of Australia	John Kennedy
	Gateway Network Governance Body	Michelle Bower
	Iness	Ross Daws

Next meeting:	TBA

The key outcomes for this meeting are best read in conjunction with Supply Chain & Payload Encryption Focus Group presentation and attachments.

Agenda item: Introduction

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

1. Supply Chain Visibility
2. Improved Guidance on Encryption
3. Payload Encryption

It was noted some items raised during the review that will be taken out of session and finalised post review.

Agenda item: 1 – Supply Chain Visibility

The group discussed previous feedback on supply chain visibility:

a) Governing Controls through the Supply Chain

- DPO created scenarios of ATOs digital infrastructure, DSPs connections to ATO environment and the varying governing controls. This diagram was shared within the first working group.
- ATO completed threat modelling exercises against these scenarios with no significant risks identified.

b) Review of Supply Chain Solution

- Feedback from the session to clarify Data Transformer i.e. File Transformer vs Data Transformer language to be clarified. This will be incorporated into the drafted wording of the DSP requirements documentation.

Outcomes from industry discussion:

- DPO will undertake further threat modelling exercise when any new service/product build uniquely differs from the existing DSP OPF scope.
- DPO will provide further clarity and definitions regarding File Transformer and Data Transformer and update glossary.

Further consideration is needed for:

- DPO will provide additional information including examples and scenarios in a newly created Operational Framework support page in the knowledge hub.

Agenda item: 2 – Supporting Guidance for Encryption

The group discussed previous feedback on supporting guidance for Encryption:

a) Encryption in Transit
b) Encryption at Rest
c) Encryption Key Management

a) In Transit

- ATO supports both TLS1.2 and TLS1.3 and documentation will be updated to remove reference of ‘TLS 1.3 preference’.
- Additional link to ACSC guidelines for implementing certificates to be included within the drafted requirements documentation.

b) At Rest

- Specific symmetric algorithms as per ACSC guidelines for using cryptography will be updated in the guidance material.
- Alternative options for using partial encryption of block, field or column have been added to guidance material.
- Clarification of the requirements i.e. must be met when encryption at rest is not viable.

c) Key Management

- Adding in a reference to attachment F from the APRA CPS 234.
- When using default key management tools AWS or Azure, they should be referenced in the DSP’s internal encryption key management (EKM) plan, this is suitable evidence for the EKM requirement.

Outcomes from industry discussion:

- Additional context for cloud solutions that indirectly connect to the ATO will be required to provide both public certificates and evidence of indirect connection.
- DPO will provide additional guidance for encryption at rest. i.e. DSPs can choose to apply this control by either encryption the disk, container, application or database. Alternatively, DSPs may choose to apply partial encryption to data at the block, field or column level but this must cover data that is stored for the purpose of Taxation, Superannuation Accounting-Payroll and Personally Identifiable information. (For products and or services controlled by the DSP).
- DSPs will be able to select other ISM approved protocols on a case by case scenario in consultation with the DPO relating to encryption in transit control.
- DPO will provide further clarity and definitions regarding TLS Standards and update glossary.
- DPO provided clarity on the type and amount of evidence to be supplied by the DSP and will update documentation i.e. one of the below or all the below.

Further consideration is needed for:

- DPO will provide additional information including examples and scenarios in a newly created Operational Framework support page in the knowledge hub, regarding EKM Plans.

Agenda item: 3 – Payload Encryption

a) Payload Encryption

- No technical changes to payload encryption control at this time.
- The value of payload encryption is recognised by the ATO and DSPs, especially within message transformation. ATO will not progress a technical solution at this stage due to competing priorities however it will be explored in the future from within the Digital Service Provider Architecture Reference Group (DARG).

b) Review of current documentation

- DPO will update current documentation and remove the reference of "Payload encryption solution is not currently available but will be developed in the near future".

Outcomes from industry discussion:

- DPO will remove reference to payload encryption from documentation, including DSP terms and conditions.

Further consideration is needed for:

- DPO will update the requirements relating to payload encryption and will keep DSPs informed when the topic arises for further discussion.

Agenda item: – Wrap Up & Next Steps

Outcomes of working group to be published and circulated.