Australian Government
Australian Taxation Office

Digital Service Provider (DSP) Operational Framework Review

Supply Chain & Payload Encryption Focus Group – Session 2

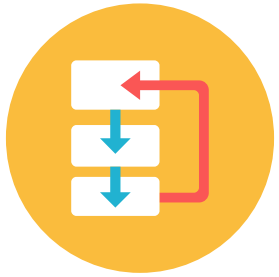
Presented by Diana Porter

10th March 2021

Recap on the groups aim and what we are trying to achieve

Explore opportunities to improve integrity of transactions over ATO gateways

1 Supply Chain Visibility



a. Governing controls through the supply chain.
b. Review supply chain solution.

2 Improved guidance on encryption

a. Encryption in transit
b. Encryption at rest
c. Encryption key management

3 Payload Encryption

a. Exploring payload encryption
b. Review of current documentation

1 Supply Chain Visibility

a. Governing controls through the supply chain

b. Review of interim supply chain visibility solution

1a Governing controls within the supply chain

REVIEW CONSIDERATIONS

Governing controls through the supply chain

CURRENT ENVIRONMENT

Governing controls are applied to Digital Service Providers whose product is within scope of the operational framework.

Software products are also covered through a range of controls such as:

- GNGB Gateway Standards
- APRA CPS 234
- Security Standards for Add-on Marketplaces
- CDR - Information security guidelines

UPDATE

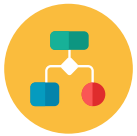
DPO has completed threat modelling scenarios against the digital ecosystem and governing controls.

Actions being taken as part of the review of the operational framework to improve existing process and guidance and when applicable develop new controls (entity validation).

The DPO will continue to work with software developers, across agencies and industry as needed to uplift governing controls through the end-to-end digital ecosystem supply chain.

1b Review supply chain solution

REVIEW CONSIDERATIONS



Interim solution applicable when software indirectly connects.

CURRENT ENVIRONMENT

Minor changes as bolded

DSP Operational Framework Requirements to utilise ATO digital services (pg.17)

The functional roles within a supply chain are defined as:

- **Data Collector**
  Party responsible for the acquisition of data through user interface interaction or APIs
- **Data Validator**
  Party responsible for the verification of data types, structures, formats and/or data values
- **Data Integrator**
  Party responsible for combining data from multiple sources for use
- **Data Analysis and Extraction**
  Party responsible for performing analysis on data to extract a data sub-set or additional derived/calculated data
- **Data Transformer**
  Party responsible for **changing representation of data to a compatible file format (e.g. CSV to XML)**
- **Data Provider**
  Party responsible for the payload (which may be encrypted)
- **Data Transmitter**
  Party responsible for the message with the payload. (e.g. ebMS3/AS4 transmission).

2 Improved Guidance on Encryption

a. In Transit

b. At Rest

c. Key Management

2a Improved guidance on encryption in transit

REVIEW CONSIDERATIONS

1. DSPs to support TLS 1.2 at a minimum.

2.Streamline evidence requirements for DSPs.

CURRENT ENVIRONMENT

DSP Operational Framework Requirements to utilise ATO digital services (pg.12)

This requirement seeks to protect the confidentiality and integrity of taxation or superannuation related information in transit.

You need to provide evidence that your product or service utilises TLS 1.3 or another ISM approved cryptographic algorithm and/or protocol. If you use an SSP and they are providing encryption in transit, you will need to demonstrate your relationship with the SSP.

Evidence required

When directly connecting to the ATO a screenshot of one of the below:

- SSL certificates
- Showing HTTPS protocol being enforced
- Call to API
- TLS handshake protocol being enforced.

When using an SSP/Gateway to indirectly connect to the ATO:

- Licensing agreement or contract for service with SSP
- Call to the SSP REST API
- Handshake agreement with SSP showing TLS 1.3 or HTTPS being enforced
- Screenshots from within SSP portal configuration page showing DSP as a linked entity.

2a Improved guidance on encryption in transit

REVIEW CONSIDERATIONS

1. DSPs to support TLS 1.2 at a minimum.

2. Streamline evidence requirements for DSPs.

WHATS NEW

This requirement seeks to protect the confidentiality and integrity of taxation or superannuation related information in transit.

You need to provide evidence that an approved protocol (**TLS 1.2 or TLS 1.3 preferred**) and algorithm are used as per ACSC - Guidelines for using Cryptography and **secure cipher suites** are used as per annex A of the ACSC Implementing certificates.

Evidence required

If you are directly connecting to the ATO one of the below represent suitable evidence:

- URL for public certificate; or
- Configuration screenshot for private or internal certificates

If you are indirectly connecting to the ATO one of the below represent suitable evidence:

- Licensing agreement with sending service provider; or
- Screenshots from SSP portal; or
- Screenshot of API call to 3rd party showing TLS protocol.

Note: Cloud solutions that **indirectly connect** to the ATO will be required **to provide both sets of evidence**.

2b Improved guidance on encryption at rest

REVIEW CONSIDERATIONS

Further guidance on application of encryption at rest to ensure it meets intent of control.

CURRENT ENVIRONMENT

DSP Operational Framework Requirements to utilise ATO digital services (pg.12)

This requirement seeks to protect taxation or superannuation related information from unauthorised access. The scope of encryption at rest covers data repositories that hold or manage tax or superannuation related information.

You can chose to apply encryption at the disk, container, application or database level. Encryption at rest should follow Guidelines for using Cryptography (May 2019).

Evidence required

- Screenshot showing encryption enabled at the database or disk level with the type of encryption at rest being used
- When using 'out of the box' encryption a licensing agreement or screenshot showing 'out of the box' encryption at rest enabled
- If using the infrastructure of a cloud provider to encrypt data at rest, an invoice or contract agreement could be provided or screenshot from within the cloud environment showing encryption enabled.

Where encryption at rest is not viable, evidence must be provided of a full range of data protection controls.

These must include:

- User/system (service account) access control (including authentication and authorisation) and active logging and monitoring protocols
- Intrusion Detection System/Intrusion Prevention System
- Internal employee screening or vetting
- Isolation of/and handling procedures for sensitive data including restrictions such as 'need to know' principles.

2b Improved guidance on encryption at rest

REVIEW CONSIDERATIONS

Further guidance on application of encryption at rest to ensure it meets intent of control.

WHATS NEW

The scope of encryption at rest covers data stored for the purpose of taxation, superannuation, accounting-payroll including personally identifiable information.

The approved symmetric encryption algorithms are **Advanced Encryption Standard (AES) using key lengths of 128, 192 and 256 bits, and Triple Data Encryption Standard (3DES) using three distinct keys** as per the ACSC - Guidelines for using Cryptography.

DSPs can choose to apply this control by either encrypting 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.

Evidence required

One of the below represent suitable evidence:

- Screenshot showing encryption enabled, confirmation of method of encryption applied, and algorithm used.
- Licensing agreement or invoice with whitepaper.
- Policies relating to data classification when applying block, field or column level encryption

All of the below to be met when encryption at rest is not viable:

- User/system role-based access controls and active logging and monitoring protocols.
- Restricting or limiting access to databases using the principle of least privilege.
- Separation of hosts and segregation of networks or micro segmentation.
- Intrusion Prevention and detection controls.

For DSPs who have implemented encryption at rest these controls are recommended. Further information is available at ACSC implementing network segmentation and segregation.

2c Improved guidance on encryption key management

REVIEW CONSIDERATIONS

Improved guidance by mapping to other standards

CURRENT ENVIRONMENT

DSP Operational Framework Requirements to utilise ATO digital services (pg.13)

This requirement seeks to minimise the risks of compromised encryption keys.

You need to demonstrate that a policy or process in place to govern the use of your encryption keys.

The scope of this policy should cover three categories: asymmetric/public key algorithms, hashing algorithms and symmetric encryption algorithms.

WHATS NEW

This requirement seeks to minimise the risks of compromised encryption keys.

You need to demonstrate that a policy or process is in place to govern the lifecycle management of encryption keys. The scope of this policy should cover three categories: asymmetric/public key algorithms, hashing algorithms and symmetric encryption algorithms.

The use of algorithms must align to the ACSC - Guidelines for using Cryptography.

Consistent with attachment F of the APRA CPS 234 a key management plan must include generation, distribution, storage, renewal, revocation, recovery, archiving and destruction of encryption keys.

Note: For software products that don't handle encryption keys this requirement is not applicable e.g. desktop and indirect connect through portal upload.

3 Payload Encryption

a. Exploring payload encryption

b. Review of current documentation

3a Exploring payload encryption

REVIEW CONSIDERATIONS

Implementation of payload encryption solution, end-to-end from the client to recipient

Implementation of payload encryption solution as an optional requirement

Use of a risk scaled model to determine appropriate use of payload encryption

Payload encryption and the potential of SSP model expansion

UPDATES

Payload encryption

There will be no change to the technical requirements e.g. no implementation of payload encryption at this stage.

DPO recognises the value of a payload encryption solution to support some supply chain models and potentially high risk services. Further investigation will be on hold and DPO will review in approximately 12 months.

Feedback raised during this review has been documented and will form part of any future conversations

SSP model expansion

The SSP model was developed to support STP payevent a low risk service and expansion of this model won't be supported at this time.

3b Review of current documentation on payload encryption

Review considerations

Current documentation relating to payload encryption.

CURRENT ENVIRONMENT

DSP Operational Framework Requirements to utilise ATO digital services (pg.13)

This requirement seeks to protect the confidentiality and integrity of taxation or superannuation related information from the source to the end point.

Payload encryption solution is not currently available, but will be developed in the near future.

DSP Operational Framework (pg.30)

Operational Framework Terms and Conditions (condition 5)

There are a number of requirements that have outstanding technical solutions. For example - authentication, payload encryption and supply chain visibility. As these solutions are completed we will advise you of the further requirements for your implementation.

WHATS NEW

We will be removing reference to payload encryption from our documentation and terms and conditions. Any future requirements will be incorporated at the time.

Open Discussion & Thankyou

Actions & support for working group

- Do the changes meet the overarching aim of the intent to improve integrity of transactions over ATO gateways?
- Will changes address specific outcomes relating to:
  - Supply Chain Visibility
  - Improving guidance on encryption
  - Payload encryption
- Are there any other concerns or gaps we haven't been able to address?
- Closure of Supply Chain & Payload encryption?

Next steps

1. Incorporate feedback and finalise changes within the draft requirements documentation.
2. Following all smaller working groups, DPO will provide draft requirement documentation for review by the Operational Framework Review working group.