December 2017

Australian Government
Australian Taxation Office

Operational Framework for Digital Service Providers

Draft Implementation Approach

For more information on this paper, email
DigitalBusinessCouncil@ato.gov.au

Contents

What is the DSP Operational Framework?

Through the implementation of ATO application programming interfaces (APIs) and services, digital service providers (DSPs) make a range of taxation and superannuation related services available to the community. The ATO recognises the strategic importance of this service delivery channel and is at the forefront of API exposure being significantly more advanced than other revenue agencies.

However, the ATO also acknowledges the inherent risks of exposing API services and sensitive information externally. The DSP Operational Framework (Framework) is part of the ATO response in recognising and responding to these risks. The Framework has also been developed in line with the Tax File Number Rule of the Privacy Act 1988 (sections 10, 11) which regulates the storage, use and security of TFN information.

The Framework requirements and implementation approach has been developed through a consultation process involving the Digital Business Council (DBC), Australian Business Software Industry Association (ABSIA), Gateway Network Governance Body (GNGB) and numerous DSPs.

What are the benefits?

The Framework aims to strengthen the security of the digital taxation and superannuation ecosystem by establishing a level of confidence and certainty. The Framework will enable the ATO to continue to invest in and extend the services made available through our digital wholesale channels.

Securing the ecosystem will also provide increased levels of confidence to tax professionals, businesses and individuals. Furthermore, the ATO will publish each DSPs high level conformance outcomes, enabling full transparency and increased levels of comfort for potential and existing users.

Who is covered by the Framework?

If a DSP provides a software product or service that reads, modifies or routes any tax or superannuation related information, then that DSP is in scope of the Framework. This includes DSPs that use an intermediary (such as a gateway or sending service provider (SSP)) to interact with the ATO.

DSPs that are already using our services are required to transition to these requirements over time.

What are the requirements?

The Framework utilises a risk differentiated model in determining the requirements needed for utilising our APIs. Factors include:

- the API risk rating
- volume of accessible individual taxpayer or superannuation records
- a number of elements of the DSPs operating model (eg on premise or cloud based software, data hosting arrangements and if there is an intermediary within the supply chain to the ATO).

Requirements for products and services hosted by the client

This includes desktop software or software hosted by the client on premise, or within either an infrastructure as a service (IaaS) or platform as a service (PaaS) environment.

Requirements	Connects directly to the ATO	Connects indirectly to the ATO (eg via gateway or SSP)
Personnel security	A personnel security integrity check process should be in place	
Encryption in transit	Encryption in transit is mandatory using Australian Signals Directorate (ASD) approved cryptographic algorithms and protocols (for example, TLS 1.2)	
Encryption at rest	Optional	
Payload encryption	Not applicable	The payload encryption solution is currently in development. The solution will be based on Cryptographic Message Syntax (CMS)
Encryption key management	Encryption key management (including public key infrastructure (PKI)) complies with ASD / industry guidelines (see pg 259-262)	
Audit logging	Appropriate audit logging functionality implemented	
Product ID in message header	The Product ID must be included in the message	
Certification	Self-assessment against either: • iRAP, • ISO/IEC 27001, • OWASP ASVS3.0 • SOC2	
Supply chain visibility	Not applicable	The supply chain visibility solution is currently in development
Data hosting	Not applicable	
Authentication	Multifactor authentication is optional	
Security monitoring practices	DSPs that utilise web services (ie hybrid) are required to have security monitoring in place For example: • network / infrastructure layer • application layer • transaction (data) layer	

Requirements for products and services hosted by the DSP

This includes software as a service (SaaS), gateways and sending service providers.

Requirements	Low volumes of taxpayer or superannuation records (<10k)		Highly leveraged or high volumes of taxpayer or superannuation records (>10k)[1]
	Consumes no/low risk APIs only	**Consumes medium or high risk APIs**	
Personnel security	A personnel security integrity check process should be in place		
Encryption in transit	Encryption in transit is mandatory using ASD approved cryptographic algorithms and protocols (for example, TLS 1.2)		
Encryption at rest	Encryption at rest is mandatory using ASD approved cryptographic algorithms and protocols. Examples may include; full-disk, container, application or database level encryption techniques		
Payload encryption Applicable when the product or service does not connect directly to the ATO and the supply chain visibility functionality is not available	Payload encryption solution is not currently available, but will be developed in the near future. The solution will be based on CMS		
Encryption key management	Encryption key management (including PKI) complies with ASD/industry guidelines (see pg 259-262)		
Audit logging	Appropriate audit logging functionality implemented		
Product ID in message header	The Product ID must be included in the message		
Certification	Self-assessment against either: • iRAP • ISO/IEC 27001 • OWASP ASVS3.0 • SOC2	Self-assessment against either: • iRAP • ISO/IEC 27001	Independent assessment against either: • iRAP • ISO/IEC 27001
Supply chain visibility Applicable when the product or service does not connect directly to the ATO and the payload encryption is not used	The supply chain visibility solution is currently in development		
Data hosting	Data hosting is onshore by default. Offshore hosting arrangements (including redundant systems) are managed by exception only		

[1] Refer to Glossary for definitions

Authentication	Multifactor authentication is mandatory	
Security monitoring practices	Not applicable	Security monitoring is in place. For example: • network / infrastructure layer • application layer • transaction (data) layer

Minimum evidence requirements

As part of the security questionnaire, DSPs need to provide suitable evidence of how their product or service meets the relevant requirements. Examples of suitable evidence include:

- Authentication
  - published product description
  - user manual, user description, user instructions paired with screen shots of the user interface

- Encryption – relevant combinations of:
  - screen shots (of the configuration page)
  - configuration files
  - product data sheet/white papers (together with Product purchase/ownership documentation such as receipts, front page of a contract of product/support/service)
  - Federal Information Processing Standard Validation documents (US government computer security standard, eg FIPS 140-2)
  - product common criteria evaluation documents
  - product evaluation assurance level (EAL) documents.

- Certification
  - iRAP letter of compliance or iRAP assessor engagement details
  - ISO/IEC 27001 documentation and certificate of compliance/registration or statement of applicability with certificate of compliance
  - OWASP ASVS3.0 or SOC2 assessment.

- Data hosting
  - name of ASD certified data hosting provider
  - data hosting provider details, including:
    - provider name
    - provider location (onshore / offshore)
    - redundancy location
  - if data is stored offshore further evidence is required. See *Additional conditions for offshore data hosting* below for more information.

- Personnel security
  - internal policy document and process description.

- Encryption key management
  - Key Management Plan (internal documentation).

- Security monitoring practices
    - network/infrastructure layer examples. Relevant combinations of:
        - screen shots (product page, the management console page)
        - product purchase/ownership doco (eg receipts, front page of a contract of product/support/service)
        - configuration files
        - photos of the product
        - photos of SOC/SIEM centre (using the products).

- Application layer example
        - screen shots of the function page in the application, and
        - reports from the backend system.

- Transaction (data) layer example
        - reports from the backend system
        - previous unusual cases.

Additional requirement information

Certification and assessment

The ATO has assessed the following security standards:

- iRAP
- ISO/IEC 27001
- OWASP ASVS3.0
- SOC2

DSPs are able to request to use an alternative security standard if they feel it would be more suitable for their circumstances. These requests will be assessed on a case-by-case basis.

Payload encryption

Payload encryption can be used to provide end-to-end protection for sensitive or classified information. Payload encryption is the preferred solution for transporting sensitive or classified information through a supply chain. DSPs must, at a minimum, implement either payload encryption or supply chain visibility requirements.

Supply chain visibility

When information is sent from one party to another (eg from a taxpayer to the ATO), the data can be sent through a number of different parties in a 'supply chain'. Each party in the supply chain can perform one or more functional roles.

The below design principles and functional roles will inform the development of a future technology solution to deliver supply chain visibility.

Supply chain visibility involves annotating the identity and functional role to the message for every DSP that reads or modifies the data – where the payload is not encrypted end-to-end (ie payload-level encryption).

Where payload encryption has been implemented supply chain visibility is not required.

Design Principles

- The technical solution will seek to balance the need for risk mitigation against need for operational effectiveness
- If a DSP reads or modifies any data, the message must be annotated with that DSPs identity and functional role(s) in the supply chain
- DSPs are not responsible for information after it has been securely delivered to an authenticated and authorised customer
- If a DSP routes a message, the message must be annotated with that DSPs identity and functional role for operational support reasons

Functional roles within a supply chain

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 & extraction – party responsible for performing analysis on data to extract a data sub-set or additional derived/calculated data
- data transformer - party responsible for change syntactic representation of data
- data provider - party responsible for the payload (which may be encrypted)
- data transmitter - party responsible for the message with the payload (eg ebMS3/AS4 transmission).

Onshore/Offshore data hosting

Storing data in a foreign jurisdiction presents additional risks that must be considered.

Requirements

Consistent with guidelines for APRA-regulated entities the ATO expects DSPs to apply a cautious and measured approach when considering retaining data outside the jurisdiction it pertains to. **By default, the ATO expects DSPs to store data onshore.**

Where there is a compelling reason for storing data outside of Australia a DSP must consult with the ATO prior to entering into any offshore data hosting arrangement so that the ATO may satisfy itself that the impact has been adequately addressed. As part of the consultation:

- DSPs must demonstrate they have considered the jurisdictional risks of storing data in a foreign jurisdiction
- the ATO can provide advice on jurisdictional constraints.

The ATO will consider requests to host data offshore on a case-by-case basis.

Additional conditions for offshore data hosting

Consistent with APRAs Cross Industry Prudential Practice Guide CPG 235, the ATO expects the following would normally be applied to the assessment and ongoing management of offshore data hosting:

- enterprise frameworks such as security, project management, system development, outsourcing/offshoring management and risk management
- a detailed risk assessment
- a detailed understanding of the extent and nature of the business processes and the sensitivity/criticality of the data impacted by the arrangement
- a business case justifying the additional risk exposures.

Consistent with APRAs Prudential Standard Guide SPG 231, the ATO expects that DSPs would address the following specific risks and any other identified risks:

- country risk — the risk that overseas economic, political and/or social events will have an impact upon the ability of an overseas service provider to continue to provide an outsourced service to the DSP
- compliance (legal) risk — the risk that offshoring arrangements will have an impact upon DSPs ability to comply with relevant Australian and foreign laws and regulations (including accounting practices)
- contractual risk — the risk that a DSPs ability to enforce the offshoring agreement may be limited or completely negated
- access risk — the risk that the ability of a DSP to obtain information and to retain records is partly or completely hindered. This risk also refers to the potential difficulties or inability of the ATO to gain access to information using ATO information gathering powers
- counterparty risk — the risk arising from the counterparty's failure to meet the terms of any agreement with the DSP or to otherwise perform as agreed.

The ATO expects that an offshoring arrangement would typically include a provision around security and confidentiality of information.

Where you are storing data outside of Australia you must:

- make it clear to your customers that their data is being stored in a foreign jurisdiction
- apply the Australian Privacy Principles
- provide guidelines to your customers, where your customers use your services to collect and store data about other individuals (eg clients of tax practitioners, employees, etc) on where and how their data is being managed.

Identity and authentication

Requirements

Subject to the design and delivery of the Trusted Digital Identity Framework (TDIF) DSPs will be required to either:

- use the current cloud authentication and authorisation (CAA) solution with the addition of a multifactor credential
- consume the government provided TDIF credential, or
- become a TDIF credential provider in their own right and consume their own credential.

In the interim, whilst the TDIF standards and solutions are being developed for use in software products, DSPs must:

- review their security credential risks and develop a plan to manage identified risks
- implement and mandate a multifactor credential solution for all users with access to taxation or superannuation related information or provide assurances that sufficient controls are in place to mitigate the risks.

Note

Many digital products and services perform tasks outside of the tax and superannuation space. User accounts that do not have access to taxpayer or superannuation related information are not required to meet the above requirements.

Implementation

The Framework introduces a number of requirements that DSPs will be required to meet. The ATO recognises that it will take time for DSPs to meet the requirements. In addition, it will also take time for the ATO to adequately assess the evidence that DSPs provide.

To cater for this each requirement has a different commencement date. There is also a strategy to slowly transition DSPs into the Framework. DSPs will be provided time to transition, however planning should be done early to ensure they are able to meet the timeframes.

When does each requirement come into effect?

Certification and assessment

It is recognised that the certification process can take time depending on the standard chosen and the maturity of the organisation. The ATO expects most DSPs will be able to complete the process in 3-6 months however longer timeframes will be required for some. The ATO will work with DSPs on an individual basis to determine an appropriate timeframe.

Existing DSPs will need to commence the process by **1 February 2018**.

New DSPs will need to commence the process before they are granted access to any service.

Access to new services while a DSP is progressing through the certification process will be assessed on a case-by-case basis. Evidence of commitment to undergo certification and satisfactory responses to the security questionnaire will form the basis for this assessment.

Encryption in transit

Existing DSPs will be required to implement encryption of data in transit by **1 February 2018**.

New DSPs will need to commence the process before they are granted access to any service.

Encryption at rest

DSPs will be required to implement encryption of data at rest change by **1 February 2018.**

New DSPs will need to commence the process before they are granted access to any service.

Payload encryption

Design for the payload encryption solution is in development and is expected to be completed by the end of 2018.

Implementing this change requires significant design, development and consultation efforts across industry. The ATO will consult with industry before this requirement comes into effect.

Supply chain visibility

Design for the supply chain visibility solution is in development and is expected to be completed by the end of 2018.

Implementing this change requires significant design, development and consultation efforts across industry. The ATO will consult with industry before this requirement comes into effect.

Onshore/Offshore data hosting

Existing DSPs who store data outside of Australia must notify the ATO and provide evidence of how they meet the requirements and additional conditions by **1 February 2018.**

New DSPs who store data outside of Australia must notify the ATO and provide evidence of how they meet the requirements and additional conditions before they are granted access to any service.

Where a DSP is unable to meet the requirements and conditions of offshore data hosting the DSP will be expected to transition data to Australia within a reasonable timeframe.

Identity and authentication

Design and delivery timelines for the TDIF are yet to be finalised.

DSPs should take a risk based approach to the implementation timeframe for multifactor authentication across their suite of products and services. Tax practitioner products and services generally present a higher risk and as such, DSPs must implement multifactor credentials by **31 March 2018** and mandate their use by **30 June 2018**.

For products and services where users potentially have access to large volumes of taxpayer or superannuation related information (eg payroll) DSPs must implement multifactor credentials by **30 June 2018** and mandate their use by **30 September 2018**.

For all other products and services hosted by the DSP, multifactor credentials must be implemented by **30 September 2018.** Their use will be mandated by **31 December 2018**.

Access to value-added services may be restricted until multifactor credentials have been implemented and mandated.

Audit logging

All new products and services will be required to include this capability. Transition for existing products and services will be discussed on an individual basis with DSPs and it is expected that all will have audit logging capabilities by **1 July 2018.**

Software identifier in message

All DSPs are required to have the software/product identifier in the message header effective immediately.

Personnel security procedures

All DSPs are required to have in place personnel security measures effective immediately.

Transition strategy

The transition strategy assists to identify the priority and order by which existing DSPs will move to the enduring registration and certification process under the Framework.

Staged Approval Process

The process of being approved under the Framework will be done in stages.

All **new** DSPs will need to seek approval under the Framework before consuming an API or web service.

All existing DSPs wishing to consume:

- a new service will be expected to be approved **before** consuming the new service
- PLS services will be expected to commence the approval process by **1 March 2018**
- Single Touch Payroll services will be expected to commence the approval process by **1 April 2018**
- taxation related services will be expected to commence the approval process by **1 May 2018**
- superannuation related services will be expected to commence the approval process by **1 June 2018**
- any other DSP that does not fall into the prior categories will be expected to commence the approval process by **1 Jul 2018.**

DSPs will be able to continue to access 'like for like' services during the transition period, even without meeting all the requirements under the Framework. Later versions of the same service (eg

2018 IITR service compared to 2017 IITR service) are not considered to be new services for the purpose of this transition strategy.

What happens if I can't meet the timeframes above?

The ATO recognises that each DSP is different and the suite of products and services can be complex. If you are unable to meet the timeframes above you should contact the ATO as soon as possible to discuss your situation. The ATO will work with you to develop a tailored transition approach. However, this approach should not be used to gain a commercial advantage.

Framework approval process

The requirements and timeframes outlined within this document are expected to be met by all DSPs seeking approval under the Framework.

The approval process involves a DSP completing a security questionnaire and providing relevant evidence. Once all the relevant information has been provided the ATO will assess the evidence provided and either:

- grant approval
- grant conditional approval
- reject the application.

Conditional approval

Conditional approval may be granted in situations where the DSP is undertaking necessary steps to meet the Framework but does not yet meet those requirements (eg undertaking certification against ISO/IEC 27001). A review date will be set when conditional approval is granted. At this time progress will be assessed and a determination made as to whether the conditional approval will continue or the DSP access will be suspended until such time as they meet the requirements.

Changing circumstances and annual re-assessment

The ATO must be notified via your Account manager of any changes to your business or product environment, in relation to the information you supplied in your questionnaire response. Re-assessments will be conducted annually.

In line with standard industry practice, certification (both independent and self–assessed) must be current. The ATO also reserves the right to undertake ad hoc reviews to ensure DSPs maintain alignment to the requirements of the framework.

Monitoring and information incidents

Monitoring is considered a joint responsibility between the ATO and DSPs. The ATO conducts monitoring at the network, application and transaction layers. If anomalies or areas of concern are identified, we may re-assess your whitelisting suitability. This may include increasing the requirements that you need to meet or introducing additional requirements. The ATO will generally contact you or your representative unless exceptional circumstances apply.

Where you identify a breach through your own monitoring controls you must notify the ATO immediately via your Account manager to ensure appropriate action can be taken.

What happens if I don't meet these requirements?

The ATO expects all DSPs will meet and maintain the relevant requirements of the Framework.

The ATO will endeavour to work through non-conformance issues with DSPs, however failure to address these issues will result in restriction of access to services or de-whitelisting. The SBR Conditions of Use enables the ATO to lawfully suspend or terminate any software product, report or information from access to the SBR channel.

The ATO is committed to the protection of tax and superannuation information and will treat issues of non-conformance seriously.

Glossary

Term	Definition
Accessible	Information that is readily available and easily obtained by the end user.
Application programming interface (API)	An API is a set of subroutine definitions, protocols and tools for building application software.
Application Security Verification Standard (ASVS 3.0)	A framework of security requirements and controls that focus on normalising the functional and non-functional security controls required when designing, developing and testing modern web applications.
ASD approved cryptographic algorithms	Algorithms which have been extensively scrutinised by industry and academic communities in a practical and theoretical setting and have not been found to be susceptible to any feasible attack.
Australian Signals Directorate (ASD)	The ASD produces the Australian Government Information Security Manual (ISM). The manual is the standard which governs the security of government ICT systems. It complements the Protective Security Policy Framework.
Cloud Software	Software that is delivered, stores data and is managed remotely from its users or their technology infrastructure (eg SaaS).
Cryptographic Message Syntax	A process used to provide encryption and digital signature capabilities to any form of digital data.
Data at rest	Data which is in storage and is not actively moving from device to device or network to network.
Data in transit	Data that is actively moving from one location to another for instance device to device or network to network.
De-whitelisting	The process of preventing the ability to transact with ATO production services.
Direct to ATO, product hosted on customer's premise or on customer's IaaS/PaaS Cloud	Software that is loaded and stored on a client's local computer, service (IaaS/PaaS) and/or device and transmits direct to the ATO.
DSP service is running in the cloud	Software that has been developed to run in a cloud environment. Cloud offers the option to provide a SaaS offering direct to end users or provide a SaaS offering to another DSP to consume as part of a supply chain.
ebMS3	A set of layered extensions to the SOAP protocol, providing security and reliability features enabling e-Commerce transactions. ATO is using the eBMS 3 standard with the addition of the AS4 profile.
Encryption	The process of encoding information in such a way that only the person (or computer) with the 'key' can decode it.
Gateway	A digital service provider that facilitates the transfer of compliant electronic data messages.
Indirect to ATO, product hosted on customer's	Software that is loaded and stored on a client's local computer, service (IaaS/PaaS) and/or device and uses a gateway or SSP to facilitate the

premise or on customer's IaaS/PaaS Cloud via gateway	transmission of a message to the ATO.
Taxpayer or superannuation related information	Information that has been stored for the purpose of a taxation or superannuation law and identifies, or is reasonably capable of being used to identify an individual or other entity.
The Information Security Registered Assessors Program (iRAP)	An ASD initiative to provide high-quality information and communications technology (ICT) services to government in support of Australia's security. iRAP provides the framework to endorse individuals from the private and public sectors to provide cyber security assessment services to Australian governments.
ISO/IEC 27001	A family of standards which assist the ATO in managing the security of assets such as financial information, intellectual property or information entrusted by third parties. ISO/IEC 27001 is recognised as the international standard for managing information security.
Large/high leverage user base/ high volumes of taxpayer or superannuation records	A DSP product or service that stores or facilities transmission of, greater than 10,000 unique and accessible individual taxpayer or superannuation related information records (records that relate to the same individual are only counted once).
Like for like services	A service which contains the same functionality, quality and value as one that was previously created.
Sending service provider (SSP)	See Gateway.
Service Organization Control (SOC)2	An audit report which covers operational control systems following predefined criteria around security, availability, process integrity, privacy and confidentiality.
Trusted Digital Identity Framework (TDIF)	A framework which provides the policies and guidelines that will govern delivery of the digital identity solution.
Whitelisting	The process of gaining access to transact with ATO production services.