MBR Design Working Group

WELCOME!

The meeting will begin at 1.00pm AEDT

Issues dialling in

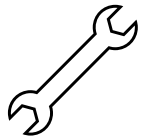
Dial-in: *1800 888 453*

Attendee code: *2652 086 0925*

Meeting password (if prompted): *mbrdwg*

If you are unable to connect to the 1800 number, try one below:

- Adelaide +61-8-7079-0394
- Brisbane +61-7-3067-4844
- Melbourne +61-3-9070-6484
- Perth +61-8-6388-9974
- Australia Toll +61-2-9053-7190



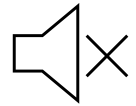
Issues connecting to audio

Hover over the bottom of the webinar screen

Click on the phone receiver button

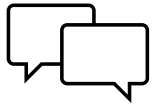
You can choose to connect to the audio:

- using your computer or
- by dialling in using the prompts on your screen



If you cannot hear audio

Check the volume settings on your computer or device



Have your say

You are welcome to take yourself off mute if you have questions, feedback, insights or recognise possible issues. The chat box and 'raise hand' may also be used.

5 October 2022

MBR Design Working Group

Wednesday 5 October 2022

ABRS
Australian Business Registry Services

Welcome and action items

Mary Arrowsmith – Assistant Commissioner, ABRS
Business Registry Design and Delivery

Open action items

Action Item	Status	Who	Action	Update
DWG-41	**Open**	Kylie Johnston	Demonstrate use cases with examples on uplifting certifications because of a change in API risk rating.	Kylie will be demonstrating use cases with examples in the meeting.

ABRS
Australian Business Registry Services

Feedback received and responses

Satyavrat Singh – Program Manager, ABRS Delivery and Integration

Steve Curtis – Program Manager, MBR Program Delivery Integration

Feedback received & responses

Feedback ID	Feedback Date	Feedback Topic	Feedback	DWG Response
DSP-FB-1	10-August-2022	Mandatory Fields	Mandatory elements up in the air. Seems like there are a few things they want to add in but not sure if they're allowed to make them mandatory. All data/info required, happy to build in, just more confidence/certainty as to what's required, makes it easier to build for DSPs.	Mandatory fields are marked with a red asterisk (*) in the Open API specification for ease of DSPs' consumption.
			Significant amount in new mandatory elements being required, upwards of 30-40 elements being added in. Lot of this in system, happy to transmit, don't want to miss things out. Rather than waste time, where missing mandatory elements, have a list of mandatory elements.	OpenAPI Specification provides the necessary mandatory elements indicator and can be leveraged by the DSPs to identify and compare the fields.
			It would be beneficial for the existing DSPs if there was a document that compares mandatory elements from the old ELS to the new system. Even if it was a simple list of new mandatory elements.	
DSP-FB-2	10-August-2022	Data Element	Person names: 'givenName' 'otherGivenName' and 'familyName', but no middle name. Of course, this is open for interpretation, however, 'middleName' would be more standard.	The taxonomy of these fields align to the Government's Standard Business Reporting (SBR) requirements. Other given name is the SBR title. SBR avoids using the position of the name in it's title as it can cause confusion in cultures that have family name in the beginning.
DSP-FB-3	10-August-2022		Date of Birth this should be changed to the ISO format "birthDayofMonth": 0, "birthMonth": "1", "birthYear": 0, this should changed to an ISO date format: for example "birthDate": "1960-12-31" This will be much easier for developers to implement.	The Date format will be updated to use ISO standard Date structure in the form "yyyy-mm-dd".

Feedback received & responses

Feedback ID	Feedback Date	Feedback Topic	Feedback	DWG Response
DSP-FB-4	15-August-2022	Response Codes	Based on the documentation it seems like that the endpoints always return "200 OK" as a response code - even at the time of failures. This gives an inconsistent representation of the underlying status of the requested resource. Though the error status is returned in the response payload, deserializing the response to a respective schema will not be feasible, as the contracts for errors and the requested data differs. To further clarify – the consuming application expecting a contract for 'Provider' resource will fail when it attempts to deserialize the JSON response at the time of failures as the endpoint actually returns a different contract related to "ApiErrorDetails" schema. As a result, there is an overhead to check varied contracts for a single endpoint and there is no easy way to actually identify the underlying reason for failures.	The Open API Specification does cater to with all possible https status codes. i.e, 201, 400, 401, 403, 500.
DSP-FB-5	15-August-2022	Authentication	Documentation around authentication needs better clarification. Dependency on certificates for online service providers introduces the complexity around managing them - especially when it comes to expiry and renewal. As documented, if extracting public and private key is a manual process then automating this at the time of request is an overhead and close to impossible. I have to assume that this is a one-off process and it is the responsibility of the consuming application to manage the keys – need clarity on how to manage client certificates in ATO portal. In-order to reduce this overall complexity, it will be better if the consuming application can use the same keys/token issued by ATO IDP to sign the JWT.	ABRS APIs will follow ATO's established authentication mechanism as published : M2M Client Authentication | ATO API Portal

Feedback received & responses

Feedback ID	Feedback Date	Feedback Topic	Feedback	DWG Response
DSP-FB-6	15-August-2022	Element Format	Regarding the end point format. Why is the first character lowercase? Is there a need for 3 mix of upper and lowercase? A simple approach would be to have it all lowercase.	The format aligns with the Government's Standard Business Reporting (SBR) requirements and how SBR generates it's taxonomy element.
DSP-FB-7	15-August-2022		If the convention is first word lower and abbreviations is uppercase, then in the request body should mIMETvpeCode be MIMETypeCode?	
DSP-FB-8	15-August-2022	Element Data	In the request body, can the sample strings contain characters that are valid, e.g. postcode (which should be postCode??) has 4LHTCSJ-E9ss For public company I believe the registered office should be in Australia (is that correct?) if so the postcode should follow Australian postcode. Some field values contain the word 'string: and others have random characters - are they denoting the same type?	This is caused by a Swagger feature that automatically generates example values based on field type and length. Swagger is a tool created specifically to support the Open API specification.
DSP-FB-9	15-August-2022		e.g. postcode (which should be postCode??)	The format aligns with the Government's Standard Business Reporting (SBR) requirements and how SBR generates it's taxonomy element.
DSP-FB-10	15-August-2022		IncorporationStateCode - in the request example schema I am not familiar with state codes JET, NFK, CXR and CCK	Recent reforms extended the Corporations Act 2001 to Norfolk Island, more information can be found here Norfolk Island Reforms | ASIC The state codes mentioned are Jervis Bay Territory, Norfolk Island, Territory of Christmas Island and Territory of Cocos Islands.

Feedback received & responses

Feedback ID	Feedback Date	Feedback Topic	Feedback	DWG Response
DSP-FB-11	15-August-2022	Element Data	Also in the Schema section your IncorporationStateCode repeats the text "State code of the state where the entity is incorporated.	Accepted, this was a genuine bug and will be fixed as we progress through the development process.
DSP-FB-12	15-August-2022	Data Representation	The schema details has, ShareIssuedNonCash where there is a instanceBinaryObiect string($binary) . Perhaps there needs to be guidance regarding what binary document type, e.g. word or PDF? What is the max size of a binary file?	The treatment of attachments will be discussed in a future DWG.
DSP-FB-13	15-August-2022	DSP support Request	Overall it will be great to get sample code in any modern languages (either in GitHub or part of OpenAPI Specification).	Swagger provides features to generate API Clients based on the Swagger Specification we provide. This feature is supported across various programming languages . This feature needs to be leveraged by the consumers of the API.
DSP-FB-14	15-August-2022	URI Structure	URI parameters consisting of ABN/ACN should be reviewed and Addressed	The API URI path and identifiers will be discussed in a future DWG.

ABRS
Australian Business Registry Services

APIs and retail walkthrough

Satyavrat Singh – Program Manager, ABRS Delivery and Integration

Steve Curtis – Program Manager, MBR Program Delivery Integration

Tim Matthews – Companies Product Manager, ABRS

APIs and retail walkthrough

API0002 – Apply for an Australian Proprietary Company (Round 1)
API0072 – Apply for an Australian Business Number (Round 1)

ABRS
Australian Business Registry Services

API risk ratings

Application to DSP requirements under the Operational Security Framework

Kylie Johnston – Director, Digital Partnership Office

Natalie Hughes – Business Analyst, MBR Program Pipeline Design

Operational Security Framework – Overview

The DSP OSF is a risk scaled model that sets minimum requirements a DSP needs to meet in order to consume ATO services. The risk scaled model is based on the following three factors:

Product Control

API Risk Rating

Volume of Unique Client Records

Some of the **key controls** of the DSP OSF include:

Onshore Data Hosting

Encryption

Certification

Multi-factor Authentication

Audit Logging and Monitoring

All DSPs must **demonstrate compliance** to the Operational Security Framework through the following process:

Complete questionnaire

Provide evidence

Accept terms & conditions

Annual Review

DSP requirements – Dependent on risk

A • DSP controlled, with • Low to High Risk APIs, and • > 10,000 unique client records	B • DSP controlled, with • Medium to High Risk APIs, and • < 10,000 unique client records	C • DSP controlled, with • Low Risk APIs, and < 10,000 unique client records	D • Client controlled, with • Low, medium or high-risk APIs	E • DSP or client controlled, and • No risk APIs
Audit logging	Audit logging	Audit logging	Audit logging	
Authentication - MFA	Authentication - MFA	Authentication - MFA	Authentication - unique login and SFA	Authentication - unique login and SFA
Certification – Independent: ISM (iRAP) ISO 27001	Certification - Independent or self assessment: ISM ISO / IEC 27001 NIST	Certification - Independent or self assessment: ISM ISO / IEC 27001 ISO / IEC 27002 ISO / IEC 27017 NIST SOC2 OWASP ASVS 3.0 or later	Certification - Self assessment: ISM ISO / IEC 27001 ISO / IEC 27002 ISO / IEC 27017 NIST SOC2 OWASP ASVS 3.0 or later	
Data hosting	Data hosting	Data hosting	Data hosting*	Data hosting*
Encryption key management	Encryption key management	Encryption key management	Encryption key management*	Encryption key management*
Encryption at rest	Encryption at rest	Encryption at rest	Encryption at rest*	Encryption at rest*
Encryption in transit	Encryption in transit	Encryption in transit	Encryption in transit	Encryption in transit
Entity validation	Entity validation	Entity validation	Entity validation	
Personnel security	Personnel security	Personnel security	Personnel security	
Security monitoring practices	Security monitoring practices	Security monitoring practices	Security monitoring practices*	
Supply chain	Supply chain	Supply chain	Supply chain	
Third party add-on marketplace	Third party add-on marketplace	Third party add-on marketplace	Third party add-on marketplace*	

*Only applies where a DSP (including in-house developers) has control to implement a solution.

API risk rating – Overview

The characteristics of a service, combined with the potential business risk, can be used to define the overall risk associated with ATO Application Programming Interfaces (APIs) being made externally available to Digital Service Providers. This is based on the risk of data exposure to the wrong person, it does not take into consideration data exposed to the right person through appropriate authentication and authorisation.

The **characteristics** are identified by the following three considerations:

The **type of data** contained in the API and the level of public or protected exposure of the data:

- **Public -** considered to be readily available in the public domain without any privacy or legislative barriers e.g. ABR/ABRS public data.
- **Business or Organisation information** including officeholders/associates, which is **made available through the disclosure framework**^ (Include link when available).
- **Personal, Sensitive, Protected or Private* -** considered to be 'information about an identified individual or entity' which could be used to identify 'who the client is' or used for 'proof of record ownership (PORO)' e.g. - TFN, address, FIA, contacts, non public/protected information from the ABR/ABRS.
- **Registration -** considered to be creating or updating the tax, super or registry profile of the client e.g. applying for a TFN, ACN, ABN, adding or updating a PAYG, GST or Excise registration.
- **Account -** considered to be any financial or non financial data about the tax and/or super profile of the client e.g. reportable income, deductions, payments, offsets etc.

The type of data contained in the **response or outcome.** For example the response contains:

- only data that is **public or made public through the disclosure framework** (Business or organisational information) e.g. successful transmission for an ABN.
- **non interactive message validation** without confirming client data.
- **interactive message validation** confirming client data.
- tax, super or ABR/ABRS **registration** data.
- tax, super or ABR/ABRS **account** data.
- **personal, sensitive, protected or private** data that **WAS** provided in the request or submission.
- **personal, sensitive, protected or private** data that **WAS NOT** provided in the request or submission.

The **resulting action** of the request or submission in the ATO client register, ATO systems or ABR/ABRS. For example:

- Information is only **attached or captured** on the client record e.g. submit a pay event.
- Information is **lodged for processing or updated** on the client record e.g. add contact, update address, lodge a return.
- Information from the client record is **provided or returned** to the user.
- A transaction results in or could result in a **refund, transfer of money (or approval of a transfer).**

The **business risk** can be identified by considering where the action may directly or indirectly lead to fraudulent activity. The result could be used for:

Information gain:

- Identity theft – e.g. obtaining personal or sensitive information to steal or sell an identity.
- Personal gain – e.g. obtaining personal or sensitive information to gain power or knowledge of another person.
- Commercial advantage – e.g. obtaining business information to gain power or knowledge of a competitor.

Financial gain:

- Directly obtaining refund – e.g. updating FIA to obtain a refund.
- Indirect obtaining refund – e.g. adding a tax registration that could lead to a lodgement with a refund.

Destructive behaviour:

- Individual hack – e.g. a malicious actor creates incorrect records on a client account to cause harm or nuisance.
- System hack – e.g. malicious attempt to crash a service or system (denial of service attack).

*Personal information - https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information
^Disclosure framework - TBA

API risk rating – Characteristics of a service based on risk level

4

Characteristics of a **high risk** service:

- Request or submission of the transaction results in, or could result in **updating personal, sensitive, protected or private client data** in the ATO client register, ATO systems or ABR/ABRS.
- Response or outcome of the transaction contains, or could **contain personal, sensitive, protected or private client** data that **was NOT** provided as part of the users request (example - additional information such as TFN, FIA etc is provided in the user response).
- Request or submission of the transaction results in, or could **result in a refund, transfer of money or approval of a request** (e.g. lodgment of an ITR or AS, payment transfer, direct debit arrangement or compassionate release of super).

3

Characteristics of a **medium risk** service:

- Request or submission results in, or could result in viewing **account data** in/from ATO client register, ATO systems or ABR/ABRS (example returning an account/transaction list from an account).
- Response or outcome contains or could contain personal, sensitive, protected or private client data that **was provided** as part of the users request (example -TFN, FIA etc is provided in the users request and is confirmed in the user response).
- Response or outcome provides interactive validation which, by way of receipt confirms accuracy of personal, sensitive, protected or private client data within ATO client register, ATO systems or ABR/ABRS (example - validating a TFN, address or FIA in ATO systems).
- Updating **business or organisation** information made available to the public through the **disclosure framework.**

2

Characteristics of a **low risk** service:

- An initial registration where the request or submission results in **creating registration data** in the ATO client register, ATO systems or ABR/ABRS (this may include personal, sensitive, protected or private data with the initial transaction/submission e.g. ABN application which may contain a TFN of an associate).
- Request or submission results in, or could result in:
  - **Viewing or transmitting registration data** in/from the ATO client register, ABR/ABRS or ATO systems (excludes personal, sensitive, protected or private data).
  - **Viewing business or organisation** information made available to the public through the **disclosure framework.**
  - **Providing account data,** attached/captured in the ATO client register, ATO systems or ABR/ABRS (example lodge STP pay event or dividend/interest report).
- Response or outcome **does not** contain personal, sensitive, protected or private client data nor confirms through interactive validation (examples - user response or outcome does not contain TFN, FIA etc).

1

Characteristics of a **no risk** service:

- Access to data that is intended to be **publicly available.**
- Access to tools and calculators which provide non-interactive or formula based validation.

Scenario – Company maintenance API product suite

Company maintenance		
API	**Risk Rating**	**Rationale**
Maintain Director Details	4	Contains personal, sensitive & protected information including Director ID or information used to complete Proof of Record Ownership (PORO).
Maintain Secretary Details	4	
Maintain Alternate Director Details	4	
Request to correct register	4	
Maintain Proprietary Company Shareholdings	3	Updates business or organisation information made available to the public through the disclosure framework.
Maintain Public Company Shareholdings	3	
Maintain Company Addresses	3	
Maintain Ultimate Holding Company	3	
Maintain General Details	3	
Change Company Name	3	
Apply for voluntary deregistration	3	
General Lodgement	2	Transmitting registration data to ABR/ABRS.
Apply for Entitlements of a Proprietary Company	2	Creates an initial registration on ABR/ABRS with data provided by external user.
Apply for an Australian Business Number for a company	2	
Apply for a Business Name	2	
View Australian Proprietary Company	1	Data is publicly available.
View Australian Public Company	1	
View Foreign Company Details	1	
View Registered Australian Body Details	1	

Scenario – Company maintenance API product suite

Company maintenance

API	Risk Rating	Max Rating
Maintain Director Details	4	4 high risk
Maintain Secretary Details	4	
Maintain Alternate Director Details	4	
Request to correct register	4	
Maintain Proprietary Company Shareholdings	3	
Maintain Public Company Shareholdings	3	
Maintain Company Addresses	3	
Maintain Ultimate Holding Company	3	
Maintain General Details	3	
Change Company Name	3	
Apply for voluntary deregistration	3	
Apply for Entitlements of a Proprietary Company	2	
General Lodgement	2	
Apply for an Australian Business Number for a company	2	
Apply for a Business Name	2	
View Australian Proprietary Company	1	
View Australian Public Company	1	
View Foreign Company Details	1	
View Registered Australian Body Details	1	

Other factors		Minimum requirements for:	
 Product Control	 Unique Client Records	 Certification	 Authentication
DSP Controlled	>10k records	Independent	Multi-factor
DSP Controlled	<10k records	Self assessment	Multi-factor
Client Controlled	>10k records	Self assessment	Single factor
Client Controlled	<10k records	Self assessment	Single factor

Scenario – Company registration and name reservation API product suite

Company registration and name reservation		
API	**Risk Rating**	**Rationale**
Apply for Combined Registration for a New Proprietary Company	2	Creates initial registration on ABR/ABRS with data provided by external user.
Apply for an Australian Proprietary Company	2	
Apply for an Australian Public Company	2	
Apply for Company Name Reservation	2	
Apply for Company Name Reservation Extension	2	
Apply for a Business Name	2	
View Australian Proprietary Company	1	Data is publicly available.
View Australian Public Company	1	
View Foreign Company Details	1	
View Registered Australian Body Details	1	
Check Name Availability	1	
Search Organisation Names	1	

Scenario – Company registration and name reservation API product suite

Company registration and name reservation		
API	**Risk Rating**	**Max Rating**
Apply for Combined Registration for New Proprietary Company	2	2 low risk
Apply for an Australian Proprietary Company	2	
Apply for an Australian Public Company	2	
Apply for Company Name Reservation	2	
Apply for Company Name Reservation Extension	2	
Apply for a Business Name	2	
View Australian Proprietary Company	1	
View Australian Public Company	1	
View Foreign Company Details	1	
View Registered Australian Body Details	1	
Check Name Availability	1	
Search Organisation Names	1	

Other factors		Minimum requirements for:	
 **Product Control**	 **Unique Client Records**	 **Certification**	 **Authentication**
DSP Controlled	>10k records	Independent	Multi-factor
DSP Controlled	<10k records	Self assessment	Multi-factor
Client Controlled	>10k records	Self assessment	Single factor
Client Controlled	<10k records	Self assessment	Single factor

Scenario – Entity search (Free) API product suite

Entity search – Free		
API	**Risk Rating**	**Rationale**
Check Name Availability	1	Data is publicly available.
Search Organisation Names	1	
Search Public Entity Register	1	
Current Company Extract	1	
Current Australian Registered Body Extract	1	
Current Registered Foreign Company Extract	1	
Business Role Search	1	

Scenario – Entity search (Free) API product suite

Entity search - Free		
API	**Risk Rating**	**Max Rating**
Check Name Availability	1	1 no risk
Search Organisation Names	1	
Search Public Entity Register	1	
Current Company Extract	1	
Current Australian Registered Body Extract	1	
Current Registered Foreign Company Extract	1	
Business Role Search	1	

Other factors		Minimum requirements for:	
 **Product Control**	 **Unique Client Records**	 **Certification**	 **Authentication**
DSP Controlled	>10k records	None	Single factor
DSP Controlled	<10k records	None	Single factor
Client Controlled	>10k records	None	Single factor
Client Controlled	<10k records	None	Single factor

ABRS
Australian Business Registry Services

Other business

Mary Arrowsmith – Assistant Commissioner, ABRS
Business Registry Design and Delivery

ABRS
Australian Business Registry Services

Questions?

Raise a ticket in Online Services for DSPs or email us at DPO@ato.gov.au