Pensions Dashboards Programme

Code of connection guide

January 2022

This scoping document outlines what we will include in the code of connection.

pensionsdashboardsprogramme.org.uk

Money & Pensions Service

1 Introduction

1.1 About the code of connection

The Pensions Dashboards Programme (PDP) will combine the security, service and operational standards into a code of connection.

The code will provide the standards and guidance to participants connecting to the pensions dashboards ecosystem, particularly with relation to security. These detail:

1. technical standards - such as implementing an assured barrier between the two organisations
2. procedural standards - such as ensuring that all incidents are reported to PDP
3. physical standards - such as ensuring the physical security of assets
4. people standards - such as ensuring that all staff involved have appropriate background and identity checks or appropriate education, training and awareness

The Pensions Dashboards Programme (PDP) will develop these standards in partnership with:

- The Pensions Regulator (TPR)
- the Financial Conduct Authority (FCA)
- the Department for Work and Pensions (DWP)
- the suppliers of the central technical architecture and identity service
- industry participants

The code of connection will be relevant to both data providers and dashboard providers, with some elements specific to one participant group.

1.2 Why the code of connection is important

The code of connection gives us a level of assurance that your systems, which connect to the pensions dashboards ecosystem, are managed and controlled to acceptable levels.

If a participant in the ecosystem does not follow the code of connection, they could be suspended, as this would pose a threat to the ecosystem. PDP would then work with the participant to rectify the problem or escalate it to the regulators.

2 Scope

Security - to ensure the ecosystem is secure, participants will need to conform to the appropriate security requirements to connect:

- technical (security conformance, standards compliance and resilience)
- procedural (security arrangements, eg pen test)
- physical (locations of people and equipment)
- people (key security personnel)

Service – participants will need to meet the minimum service levels and associated response times along with expected behavior:

- technical (response times and interoperability)
- procedural (maintenance, outage handling both planned and unplanned, process for raising issues and monitoring issues to resolution and service reporting)
- physical (environment details (test & live))

Operational - processes required in order to connect to the ecosystem:

- onboarding (prerequisites, procedure for onboarding - including transition to live)
- BAU operational control (dispute management process, remediation routes for service level failure, escalation process, contact management (starters/leavers etc) and failure to comply process)

3 Security

Current thinking on the type of security requirements. This is not an exhaustive list and will be refined over the next few months with our partners.

	Description	Standards and guidance
Technical		
1	TLS v1.2 as a minimum	While the minimum requirement to connect to the ecosystem is TLS v1.2, there is a strong preference for participants to use TLS v1.3
2	mTLS on all TLS channels	It is advised that all external channels use mTLS, but provided all channels connected to the ecosystem use mTLS this is acceptable

3	UMA 2.0	UMA is an open standard (managed by Kantara). We require you to use version 2.0, to securing the ecosystem and ensure interoperability
4	Money and Pensions Service (MaPS) technical standards v0.6 as a minimum	The technical standards (managed by MaPS). The minimum version we require you to support is v0.6. Later versions can be implemented provided they adhere to the compatibility requirements of the ecosystem
5	MaPS data standards v1.2 as a minimum	The data standards are (managed by MaPS). The minimum version we require you to support is v1.2. Later versions can be implemented provided they adhere to the compatibility requirements of the ecosystem
6	Use of AES-256 encryption as a minimum for data storage	We would advise that all data should be encrypted using AES-256, but encrypting all data used in the ecosystem using AES-256 is acceptable
Procedural		
7	You must alert PDP of any security incident that might impact the ecosystem as soon as you become aware of it	To ensure the security of the ecosystem, all participants must highlight to PDP any security issue that could either affect the ecosystem or other participants in a timely manner
Physical		
8	Inform PDP of your endpoint location	This is to monitor regions for specific threats
9	Inform PDP of your main operations location	This is to monitor regions for specific threats
People		
10	Provide contacts for your security function	PDP will require a contact within your security function to discuss security related issues. This could be as a result of a security threat or as consequence of a breach of security from your firm

4 Service

Current thinking on the type of service requirements. This is not an exhaustive list and will be refined over the next few months with our partners.

	Description	Standards and guidance
Technical – service level agreements (SLAs)		
1	Your live system must be available 99.5%	This is a 24/7 service, so participants will be expected to be always connected unless they have declared a planned outage
2	Your live system should be able to flex to support concurrent users in the range x to y	Estimated figure for accessing the dashboard indicates it is likely that participants can expect requests concurrently from between x to y users
3	Data provider response to find with an ack/nack should be five seconds	In order to provide certainty that a find request has been received, a response is required within five seconds
4	Registering of a PeI should be within five seconds	While the ecosystem will allow the registering of PeIs after five seconds, it is an online experience and as such the consumer will expect to access their details almost immediately
5	View data must be returned within five seconds	In order to provide an online service, data providers must return view data within five seconds after receiving a valid view request
6	Value data within view exceptions	Where a relevant value has not been calculated or provided on a benefit statement within the last 12 months, schemes will have three days to return value data except for: I. non-money purchase schemes, which have 10 days, and II. hybrid schemes, where the benefit value is produced with reference to both money purchase and non-money purchase calculations, which will also have 10 days
Technical		
7	Provide information about the number of endpoints you intend to connect (including test and live)	We need to know this information in order to manage endpoints
8	Inform PDP whether you or an ISP will host and manage your endpoint(s)	This is to ensure that if using an ISP, they have gone through appropriate onboarding

9	Inform PDP who will be responsible for carrying out integration and API testing	We need to know who will carry this out to ensure we have the correct contacts and information during the service testing phase
10	Provide and keep up to date the matching criteria you will use	This information helps monitor data quality and the effectiveness of matching
Procedural		
11	All planned outages must be communicated to PDP at least 10 working days prior to the outage	This is so that the central technical architecture can efficiently manage endpoint outage
12	Provide information on the measures you have put in place to tackle service level failures	Procedures for service level failures are being developed over the coming months. Participants will be expected to follow these procedures
People		
13	Provide contacts for your service contact	PDP will require a contact within your service function to discuss service-related issues. This could be as a result of a service level breach

5 Operational

Current thinking on the type of operational processes required. This is not an exhaustive list and will be refined over the next few months with our partners.

	Description	Standards and guidance
Onboarding		
1	State the measures you have put in place to follow PDP's onboarding procedure	Procedures for onboarding are being developed over the coming months. Participants will be expected to follow these procedures
2	Provide information on who will host and manage your endpoint	Procedures for onboarding are being developed over the coming months. Participants will be expected to follow these procedures
3	Provide contacts for your administrator and their deputy	As part of onboarding, a primary administration user and deputy will be required
4	Provide contacts for the individual who will represent your company on the ITWG	As part of onboarding, participants will be expected to actively participate in the integration and technical working group (ITWG)
Business as usual (BAU)		
5	Describe the measures you have put in place to tackle service level failures	Procedures for service level remediation are being developed over the coming months. Participants will be expected to follow these procedures
6	Explain the escalation process you have put in place	Procedures for escalation are being developed over the coming months. Participants will be expected to follow these procedures
7	Provide information on the process for ensuring contact information will be kept up to date	In order to maintain up to date contact information PDP requires participants to make updates to any contact information in a timely manner. Ideally this will be embedded in your personnel changes, starters and leaves process
8	List the measures you have put in place to support dispute management and resolution	Procedures for dispute management and resolution are being developed over the coming months. Participants will be expected to follow these procedures
9	Provide information on how you plan to support the testing of new releases of software impacting the ecosystem	From time-to-time participants will be required to test new releases of software. Procedures for testing of new releases developed over the coming months. Participants will be expected to follow these procedures