Pensions Dashboards Programme

Code of connection

July 2022

pensionsdashboardsprogramme.org.uk

Money & Pensions Service

Contents

What is the code of connection and what is it for?

This document sets out how the trustees/managers (in the case of occupational pension schemes) or authorised persons (in the case of personal/stakeholder pension schemes) (together pension providers) and qualifying pensions dashboard services (QPDS) are to connect to the dashboards ecosystem and what they need to do to remain connected. It details the mandatory requirements that must be met, as well as the recommended ways in which participants should implement them.

Standards are separate from, but designed to complement, the Financial Conduct Authority's (FCA) regulatory framework. As the FCA regulates the conduct of firms carrying out an activity, the FCA's Handbook rules will apply to QPDS firms and can impose standards on those firms (aligned to FCA's statutory objectives) when carrying out the qualifying pensions dashboard service. The FCA will consult on its proposed Handbook rules in due course.

In practice, third parties such as administrators or software providers may manage the connection of pension providers into the dashboards ecosystem and take on the responsibility for implementing these standards. However, the legislation will require the pension providers and QPDS to comply with these standards, and they are therefore ultimately accountable, even if they delegate the implementation to a contracted third party.

These standards provide assurance that the systems of all participants in the ecosystem, which access and use the central digital architecture and interoperate with other ecosystem participants, are managed and controlled to the appropriate levels.

Together, these will ensure that the pensions dashboards ecosystem provides a secure, well-functioning, effective service which garners user trust and satisfaction; which facilitates pension providers to comply with their legal duties; and enables multiple dashboards to operate, creating choice for users and scope for innovation.

The code of connection comprises three sets of standards:

Standard type	Description	Purpose
Security	the ongoing technical and procedural standards required to ensure the appropriate level of security for the pensions dashboard ecosystem	to deliver a secure service which ensures data protection, and in which users, pension providers and dashboards can all have trust
Service	the minimum service requirements and required behaviour of participants	to deliver an effective, well-functioning and high-performing service that ensures all participants operate to the same level and know what to

		expect from each other, and that ensures users have a positive user experience
Operational	the minimum operational processes participants must follow to maintain their connection into the ecosystem	to ensure effective ongoing operation of the ecosystem

Categorisation

This document includes:

- standards and
- recommended or best practice guidance

The security, service, and operational standards are strictly mandatory requirements and must be implemented in all cases. These are clearly marked as standards which participants *must* implement throughout. In addition, the tables below include some best practice guidelines. This is *recommended* rather than required and is therefore clearly delineated from the standards. This guidance should be implemented where possible to enable optimal user outcomes, but it is not a requirement.

1. Security standards

The National Cyber Security Centre (NCSC) lead for HM Government on the security of national systems. They have mandated a set of Baseline Security Controls (BSC) for the ecosystem which are to be implemented for both the PDP (on behalf of MaPS) central digital architecture platform and for all connecting providers. https://www.ncsc.gov.uk/collection/device-security-guidance/platform-guides

Standard reference	Description of requirement	Reason for the requirement	Best practice guidance	Applies to
1.1. Technical security standards				
CoCo1.1.1	must implement TLS v1.2 as a minimum	BSC	recommend you should implement TLS v1.3 where possible. Where TLS v1.3 is supported, fallback should be disabled. TLS v1.2	QPDS; pension providers

			fallback shall be denied	
CoCo1.1.2	must implement mTLS on all TLS channels	BSC	recommend that all external channels use mTLS, but provided all channels connected to the ecosystem use mTLS this is acceptable	QPDS; pension providers
CoCo1.1.3	must use encryption standard AES-256 as a minimum for all stored data	BSC	this is the minimum recommended encryption standard	QPDS; pension providers
1.2. Procedural security standards				
CoCo1.2.1	must undergo an initial IT health check (an external penetration test carried out by an independent third-party CREST-accredited scheme) on your interface to the ecosystem and receive PDP approval of the results IT health check scope must cover as a minimum the infrastructure and services you are introducing to connect to the ecosystem. PDP Security Working Group will verify this scope test results must either (a) show no high or medium issues are identified, or (b) show any high and medium issues identified have been addressed. If any minor issues are identified, you must have a plan to address them within a year and must have resolved them by the next annual test	NCSC require an independent external IT health check (penetration test) by a company registered on a recognised industry scheme	PDP reserve the right to request to see your plan to address minor issues	QPDS; pension providers
CoCo1.2.2	must undertake a CREST-accredited IT health check annually and keep evidence of the test and its findings for the duration of your connection	an annual test maintains the security and integrity of the ecosystem	whilst participants are not required to submit every annual IT health check, PDP reserve the right to request to see subsequent annual IT health check test results	QPDS; pension providers

2. Service standards

Standard reference	Description of requirement	Reason for the requirement	Best practice guidance	Applies to
2.1. Technical service standards				
CoCo2.1.1	ACK response to acknowledge receipt of a find request must be <1 second	effective traffic management	recommend that the target for ACK responses should be 250ms	pension providers
CoCo2.1.2	find request response time including registration of Pension Identifier (PeI) with the C&A service (for both matches made and possible matches) must be <60 seconds find request response time is the time lapse between sending the ACK and registration of a PeI	effective traffic management	recommend that the target for completion of matching and registration of PeI should be 15 seconds	pension providers
CoCo2.1.3	view request response time must be <2 seconds view request response time is the time lapse between receipt of a dashboard view request and return of the view data payload	effective traffic management	recommend that the target for view request responses should be 1 second	pension providers
CoCo2.1.4	in the event of non-response by your find interface, after three retry attempts, your endpoint will be deemed to be down. After retry failure, you must restore your service within 2 hours. The backlog of find requests should be processed accordingly.	effective traffic management		pension providers
CoCo2.1.5	service uptime must be 99.5% (i.e. 0.5% unscheduled downtime), measured on a monthly basis	system availability (ability to process and view transactions)	should use best endeavors to restart the service out of hours (core hours are 9am to 5pm, Monday to Friday).	QPDS; pension providers
2.2. Procedural service standards				

CoCo2.2.1	when in response to a find request you identify a match (whether possible or confirmed), when registering the PeI, you must provide PDP with the reason for registration, i.e. whether it is a possible or confirmed match. [Note: it is TBC whether you will only need to record this in your audit logs, or whether this will involve re-registering a PeI with PDP when a possible match becomes a confirmed match]	enabling monitoring and oversight of matching	recommend matching process should support multiple concurrent possible matches: may identify multiple potential matches for different users for the same pension	pension providers
CoCo2.2.2	if the outcome of the process to resolve a possible match is that it is *not* a match (i.e. the user contacts the pension provider, and the pension provider's own verification processes determine they are *not* the pension owner), you must (1) de-register the PeI (if possible – this requires a valid protection API access token) as soon as possible; and (2) immediately cease serving view data for any view requests against that PeI	user experience – ensures users do not have possible matches showing on their dashboards where these have been resolved as no match	recommend that where a possible match is resolved to be no match, you de-register the PeI as soon as is feasible, and at the latest within 24 hours. In the event of no match, you should delete the find request, or store a hash of some of the details used in the search so that when a subsequent search is initiated by the same user you need not run a repeat search	pension providers
CoCo2.2.3	where a match is made and but the user ceases to be a 'relevant member' (as defined in the legislation), the legislation requires you to de-register the PeI as soon as possible. You will need a valid protection API access token to do this. If this has expired, you will be unable to de-register the PeI, but you must immediately cease serving view data for any view requests against that PeI	user experience – ensures users do not have PeIs registered for pensions that no longer exist/are no longer in scope	recommend that where the user ceases to be a relevant member, you de-register the PeI as soon as is feasible, and at the latest within 24 hours	pension providers

CoCo2.2.4	must communicate all unplanned outages to PDP within 5 days after the unplanned outage (NB trustees/managers/authorised persons must notify PDP when your *scheme* is disconnected)	effective management of the ecosystem		QPDS; pension providers
CoCo2.2.5	must give PDP a minimum of 5 days' advance notice of all planned outages/maintenance scheduled	effective management of the ecosystem		QPDS; pension providers
CoCo2.2.6	must share with the PDP service manager relevant issues that may impact on the ecosystem as soon as they are known	effective management of the ecosystem		QPDS; pension providers

3. Operational standards

Standard number	Description of requirement	Reason for the requirement	Guidance	Applies to
3.1. Onboarding operational standards				
CoCo3.1.1	must nominate and provide PDP with contact details for the following: • prime business contact • prime technical contact • security lead • test manager • service manager must keep these contacts up to date at all times and communicate any key personnel changes to PDP immediately	effective management of the ecosystem		QPDS; pension providers
CoCo3.1.2*	must follow the service acceptance and transition to live processes	effective management of the ecosystem		QPDS; pension providers
3.2. Business as usual operating standards				

CoCo3.2.1*	must have a defined remediation route for service level failures	effective management of the ecosystem		QPDS; pension providers
CoCo3.2.2*	must have escalation processes	effective management of the ecosystem		QPDS; pension providers
CoCo3.2.3*	must have measures to support dispute management and resolution	effective management of the ecosystem		QPDS; pension providers
CoCo3.2.4*	must have a process for raising issues and monitoring issues to resolution	effective management of the ecosystem		QPDS; pension providers

* Further detailed requirements to be confirmed.