Pensions Dashboards Programme

Code of connection

Draft version: November 2022

pensionsdashboardsprogramme.org.uk

Money & Pensions Service

Contents

Introduction *2*

Summary *2*

Background *2*

Purpose 2

Audience 3

Jurisdiction 4

Use/evidence 4

Version 4

1. Security standards *5*

2. Service standards *8*

3. Operational standards *13*

Introduction

Summary

1. The code of connection comprises of the security, service, and operational standards. These standards set out the requirements that must be met to connect to the pensions dashboards ecosystem and the requirements that must be met to remain connected.

Background

2. Pensions dashboards are apps, websites or other tools which will help individuals view their pensions information online. They will bring together all an individual's pensions they haven't yet taken, including their State Pension as well as any occupational and personal pensions (including those with an insurer), to support better planning for retirement and growing financial wellbeing.
3. This standard is issued by the Money and Pensions Service (MaPS). MaPS set up the Pensions Dashboards Programme (PDP) in 2019 to design and create the pensions dashboards ecosystem and the supporting governance framework.
4. The pensions dashboards ecosystem contains the central digital architecture that will make pensions dashboards work. It will connect millions of individuals to their information across thousands of pensions, via multiple pensions dashboards. For more information about the pensions dashboards ecosystem and its components, see https://www.pensionsdashboardsprogramme.org.uk/ecosystem/.
5. MaPs is also responsible for operating its own dashboard.
6. Standards are separate from, but designed to complement, the Financial Conduct Authority's (FCA) regulatory framework for pension dashboard service firms. Firms which operate a qualifying pensions dashboard service (QPDS) will need to be (or become) FCA authorised, get the regulatory permission to undertake this new regulated activity and meet any Handbook rules and guidance that the FCA may introduce for firms undertaking this activity.

Purpose

7. The code of connection provides assurance that the systems and services 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.
8. 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.

9. 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 dashboards ecosystem	to deliver a secure service 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

Audience

10. This standard and guidance applies to the trustees or managers of occupational pension schemes and the managers of stakeholder and personal pension schemes and insurers -(pension providers and schemes) connected to, or are required to connect to, our pensions dashboard ecosystem. However:
    a. due to the connection staging profile the dashboard duties will apply at different dates to different categories of pension provider or scheme.
    b. schemes with less than 100 members are exempt unless they voluntarily connect.

11. The term dashboard is used interchangeably with QPDS as this may also include the MaPS dashboard even though this standard does not apply to the MaPS dashboard. MaPS will be adopting it to ensure technical interoperability with the pensions dashboard ecosystem. Most of the standards and guidance apply equally to both QPDS as well as pension providers and schemes. Where the standard/guidance applies only to pension providers and schemes or QPDS, this is highlighted.

12. Third parties (such as administrators or software providers) may apply our standards and guidance on behalf of their pension provider, scheme or QPDS clients. As the standards and guidance apply to the pension provider, scheme or QPDS, they remain responsible for compliance with them, even if implementation is delegated to a contracted third party.

Jurisdiction

13. This standard and guidance applies to all United Kingdom QPDS and pension providers and schemes subject to the dashboard duties in the Pensions Dashboard Regulations 2022 (the Regulations) and FCA regulatory framework.

Use/evidence

14. Standards are mandatory requirements and, therefore, compliance by pension providers and schemes as well as QPDS is compulsory.
15. Statutory guidance requires pension providers or schemes to have regard to it when complying with their relevant dashboard duties. Should they depart from the guidance, it would be sensible to have a good reason (including being able to demonstrate how the same outcome has been achieved under an alternative path).
16. General guidance contains recommendations to enable optimal user outcomes.
17. Standards and guidance may be admitted in any proceedings relevant to pension provider's, scheme's or QPDS's compliance with their dashboard duties – this also applies to the obligations owed by any other party (for example, a sponsoring employer or administrator). It will be the decision of the body hearing the proceedings (including any regulatory proceedings conducted by the FCA or The Pensions Regulator (TPR) to assess the evidential weight to be attached to any standard or guidance admitted.

Version

18. This is the November 2022 version of the code of connection. Please refer to the changelog for updates since the last publication.

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 pension providers and QPDS: https://www.ncsc.gov.uk/

Standard reference	Applies to	Requirement	Reason for the requirement or guidance	Recommended guidance
1.1. Technical security standards				
CoCo1.1.1	pension providers and schemes[1]; QPDS	must implement at a minimum and must always support Transport Layer Security (TLS) encryption profile 1.2 for all ecosystem communication where a connection is successfully established between both parties using v1.3, they must not fall back to 1.2	BSC	recommend implementing TLS v1.3 in addition to v1.2 where possible – ie should initially attempt communication via v1.3 and establish a connection via 1.3 where both parties to the interaction support v1.3, but retry using v1.2 if the other party does not support v1.3 (NSCS advise v1.3 is designed to be more secure than previous iterations)
CoCo1.1.2	Pension providers and schemes; QPDS	must implement Mutual TLS (mTLS) encryption for all system-to-system communication within the ecosystem	BSC	recommend that all external channels use mTLS, but provided all channels connected to the ecosystem use mTLS, this is acceptable

[1] to reiterate, for the avoidance of doubt, in all cases where this document refers to pension schemes and providers as the entities on whom the obligation applies, while they are legally accountable for compliance, if the pension scheme or provider elects to connect via a contracted third party rather than connecting directly to the ecosystem, the third party will implement the requirement on the pension provider or scheme's behalf

CoCo1.1.3	pension providers and schemes; QPDS	-	BSC	recommend encryption of data at rest in accordance with industry best practice: recommend implementation of encryption standard AES-256 for data at rest within pension provider/QPDS systems (eg view data cached temporarily at a QPDS; pension identifiers stored on a QPDS user account; transaction identifiers/audit logs stored by pension providers/QPDS)
1.2. Procedural security standards				
CoCo1.2.1	pension providers and schemes; QPDS	must undergo an initial IT Health Check carried out by an independent third-party scheme accredited by Council of Registered Ethical Security Testers (CREST) on interfaces to the ecosystem must cover as a minimum scope the new infrastructure introduced in order to connect to the ecosystem (PDP security working group will verify this scope) must report IT Health Check results to PDP and attend the PDP security working group to present evidence and receive PDP approval must evidence that IT Health Check results either: (a) identify no critical, high or medium defects (minor defects are permissible), or (b) show any critical, high or medium issues identified have been addressed (medium-level defects should be fixed prior to connection, but PDP may allow reasonable exceptions, if a valid case can be made and approved by PDP that the threat can be adequately mitigated through other	BSC – NCSC mandate an independent external IT health check by a company registered on a recognised industry scheme provides confidence and assurance of system security and protects infrastructure used to connect to the ecosystem from unauthorized access or change and do not provide an unauthorized entry point	PDP reserve the right to request to see plans to address minor issues

		controls) must evidence a remediation plan, approved by the CREST-accredited IT Health Check assessor, for addressing any minor defects identified within a year, and to have resolved them by the subsequent re-test (as per 1.2.2.)		
CoCo1.2.2	pension providers and schemes; QPDS	must annually re-take a CREST-accredited IT Health Check, covering at a minimum the infrastructure and services used to connect must ensure any critical, high or medium defects are addressed immediately (PDP may allow reasonable exceptions for medium defects, if the threat can be adequately mitigated through other controls) must keep evidence of IT Health Checks and remediation plans for 2 years: parties must have the previous IT Health Check results and remediation plan (if relevant) as well as the current IT Health Check results in order to be able to evidence that any defects identified at previous IT Health Check have been addressed by the subsequent test	BSC maintains the security and integrity of the ecosystem	whilst participants are not required to submit evidence from every subsequent annual IT Health Check, PDP reserve the right to spot check and request evidence of IT Health Checks

2. Service standards

Standard reference	Applies to	Description of requirement	Reason for the requirement or guidance	Recommended guidance
2.1. Technical service standards				
CoCo2.1.1	pension providers and schemes	must acknowledge receipt of find requests by the find interface, by means of ACK (as per technical standards https://www.pensionsdashboardsprogramme.org.uk/standards/technical-standards/) in <2 seconds (99.9% of ACK responses to acknowledge receipt of a find request to be returned in <2 seconds) ACK response time is the time lapse between receiving the find request from the PFS and sending the ACK	effective traffic management ACK is an asynchronous automatic response to confirm receipt of the find request	recommend that the target for ACK responses should be 250ms
CoCo2.1.2	pension providers and schemes	must complete responses to find requests, including registering any pension identifiers (as per technical standards [https://www.pensionsdashboardsprogramme.org.uk/standards/technical-standards/]) for positive matches (including both matches made and possible matches; negative responses are not required) with the consent and authorisation service in <60 seconds following sending of the ACK	user experience – finding users' pensions is designed to be an in-session experience efficient traffic management pension provider or scheme architectural optionality – 60 seconds does not require a particular architectural solution and supports searching across distributed systems as well as centralized architectural	recommend that the target for completion of matching and registration of pension identifier(s) should be 15 seconds

			solutions pension provider or scheme burden – registration of matches in response to find requests is a synchronous response, requiring pension providers and schemes to undertake matching and register a pension identifier for any found pensions	
CoCo2.1.3	pension providers and schemes	must respond to view requests in <10 seconds (99.9% of view data payloads retrieved from systems and returned to the dashboard that issued the view request returned in <10 seconds) view request response time is the time lapse between receipt of a dashboard view request and return of the view data payload (this includes the authorisation call to the consent and authorisation service to check authorisation of the view request) view response time applies regardless of the view data payload - ie whether the values are returned immediately in response to the view request, or whether a 3/10 working day calculation period (as per legislation) applies – if the pension provider uses the permitted 3/10 working day period to calculate the values, the initial view response (comprising of the administrative data and signpost data) must still be <10 seconds	user experience – viewing pensions information is designed to be an in-session experience architectural optionality – 10 seconds supports return of real-time data by means of APIs to retrieve data from pension provider/administration platforms return of view data is a synchronous response	recommend that, the target for view request responses should be 2 seconds where 'static' values are available, rather than calculated in real time
CoCo2.1.4	pension providers and schemes	must restore service within 2 hours in the event of an endpoint outage, without loss of data ACKed before the outage.	user experience – pensions dashboards are a digital service	

			efficient traffic management	
CoCo2.1.5	pension providers and schemes	must be available 99.5%, 24/7, measured on a monthly basis for clarity, 99.5% availability means 0.5% unavailability for whatever reason	user experience – pensions dashboards are a digital service the central digital architecture will be available 99.5% 24/7	
CoCo2.1.6	pension providers and schemes; QPDS	must generate, send, receive and retain unique transaction identifiers and timestamps in audit logs for all API interactions between ecosystem parties. transaction identifiers must be generated by the party initiating the transaction in accordance with the technical standards [https://www.pensionsdashboardsprogramme.org.uk/standards/technical-standards/], issued to the other party to the transaction via the relevant API in accordance with the technical standards, and retained in the audit logs of both parties to the transaction for 6 years	ecosystem audit – enables correlation of business audit logs across parties to support forensic investigation	
2.2 Procedural service standards				
CoCo2.2.1	pension providers and schemes	must give a minimum of 5 days' notice in advance of a scheduled service unavailability service unavailability includes any gap in service due to the service being unavailable or impaired	effective service management	wherever possible patches and upgrades should be applied without any service outage, but reasonable exceptions where updates require a short outage to re-boot to

				apply upgrades may be allowed, with advance notification (such outages nonetheless count towards the 0.5% downtime permissible)
CoCo2.2.2	pension providers and schemes	-	UK GDPR user experience – ensures users do not have possible matches showing on their dashboards where these have been resolved as no match or which cannot be used to retrieve pensions information	in the event of no match being made against a find request received (including when a possible match is resolved not to be a match, or is not resolved), the find request should be deleted – or, alternatively, pension providers and schemes may investigate whether they can store a hash of some of the details used in the search so that when a subsequent search is initiated by the same user within a given period, a repeat search against a known no match is not needed
CoCo2.2.3.	pension providers and schemes	-	effective management of the ecosystem	pension provider matching processes should support multiple concurrent possible matches: matching may identify multiple potential

				matches for different users for the same pension
CoCo2.2.4	pension providers and schemes	must notify PDP as soon as possible if a pension identifier for a match made must be de-registered (because the member has ceased to be a relevant member as defined in the legislation), but the protection API access token has expired, and the pension provider is therefore unable to de-register the pension identifier using the pension identifier registration API must immediately cease serving view data for any view requests against pension identifiers that have been de-registered with the consent and authorisation service, or that have been flagged to PDP as requiring de-registration, but the provider is unable to de-register due to PAT expiry	effective management of the ecosystem	
CoCo2.2.5	QPDS; pension providers and schemes	-	effective management of the ecosystem	should notify PDP of any threats to the performance or security of the ecosystem as soon as they are known and contribute intelligence relating to ecosystem security to the PDP security operating centre, as well as receiving and acting appropriately on any security intelligence received from PDP
CoCo2.2.6	pension providers and schemes	must notify PDP in the event of any find data loss due to technical/other issues as soon as this is identified	user experience – mitigates the risk of find requests not being processed without the user's knowledge, resulting in pensions not being found	

3. Operational standards

Standard number	Applies to	Description of requirement	Reason for the requirement or guidance	Recommended guidance
3.1. Onboarding operational standards				
CoCo3.1.1	QPDS; pension providers and schemes	must nominate and provide PDP with contact details for the following: • prime business contact • prime technical contact • security lead • test manager • service manager	effective management of the ecosystem	recommend sufficient staff are assigned to the required roles to cover routine absences – the PDP connection portal allows the addition of multiple users for a single required role, allowing deputies to act for the required key roles where the primary contact is unavailable
CoCo3.1.2	pension providers and schemes	must provide data required to register with PDP (MaPS) as a pension provider: (part) scheme name, customer-facing name(s), regulator-issued registration code, regulator number, regulating body, holdername (see technical standards [https://www.pensionsdashboardsprogramme.org.uk/standards/technical-standards/]), holdername view endpoint, and details for the pension provider or scheme find endpoint, view endpoint, PAT refresh endpoint	ensuring connection of legitimate parties only	
CoCo3.1.3	QPDS	must provide data required to register with PDP (MaPS) as a QPDS: regulator-issued registration code, regulator number, dashboard redirect	ensuring connection of	

		URL, dashboard UMA claims redirect URL	legitimate parties only	
3.2. Business as usual operational standards				
CoCo3.2.1	QPDS; pension providers and schemes	must have a defined remediation route for service level failures	effective management of the ecosystem	recommend following ITIL service incident and problem management processes best practice guidance
CoCo3.2.2	QPDS; pension providers and schemes	must have internal escalation frameworks and processes and ensure staff know how and to whom internally issues should be escalated and when	effective management of the ecosystem	recommend following ITIL service incident and problem management processes best practice guidance
CoCo3.2.3	QPDS; pension providers and schemes	must have a framework for raising issues and monitoring issues to resolution	effective management of the ecosystem	
CoCo3.2.4	QPDS; pension providers and schemes	must make all reasonable efforts to support forensic investigation where required, including supporting mediated access to business audit logs	effective management of the ecosystem	
CoCo3.2.5	pension providers and schemes	must ensure that any contracted third parties managing connection to the ecosystem on behalf of the pension provider or scheme severs the connection of the pension provider or scheme if directed by PDP (eg because the pension provider or scheme ceases to have any relevant members, or if the provider ceases to be registrable with the regulator)	ensuring only relevant pension providers and schemes remain connected to the of the ecosystem	

CoCo3.2.6	QPDS; pension providers and schemes	must keep key contacts (as per CoCo3.1.1.) up to date at all times via the PDP Salesforce platform and communicate any key personnel changes to PDP immediately	effective management of the ecosystem	
CoCo3.2.7	pension providers and schemes	must keep pension provider registration data (as per CoCo3.1.2) up-to-date at all times and inform PDP immediately of any changes eg as a result of mergers and acquisitions	effective management of the ecosystem	