Pensions Dashboards Programme (PDP) Digital Architecture Webinar Q&A

Request for Information (RFI)
Webinar question responses

Webinar Date 7 July 2020

Background

On Tuesday 7th July we hosted a webinar, with panellists Raman Dhaliwal, David Reid and Rahat Khalil.

The session was an opportunity for interested participants to seek clarification on information provided within the market engagement documentation.

Please note, the panellists' clarification responses are provided as early guidance for suppliers rather than a final position of how the programme intends to deliver the Pensions Dashboards Service. This will be informed by further market intelligence information being provided by participants in their RFI questionnaire responses. Final technical requirements will be published as part of the future formal procurement opportunity.

Questions

Questions asked during the webinar, with responses from the panel.

Q1. There will be some minimum Personally Identifiable Information (PII) that the pension finder service may have to send to pension schemes to get customer's pension data. Where would such PII data be stored?
The PFS should not persist PII – Primary personal data is not retained within the PD ecosystem – it is used (transiently) for identity verification and for data matching to pension entitlements at pension providers.

Q2. Please elaborate on the governance register features. Would such be limited to service SLAs?
A 'governance register', consisting of both organisational processes and online IT components, controls which organisations and which software instances can participate in the ecosystem. It may also provide central reporting, technical monitoring and similar services.

Q3. Which aspects of the 3 services (pension finder, consent and authentication) will be governed within the governance register?
The governance register maintains a directory of participants including providers, dashboard instances, integrated service providers, identity services, etc. It will provide public key

infrastructure and key rotation for the authorisation server. Key services will include registration / onboarding of new participants.

Q4. Would PDP be responsible for assessing data quality of the pension scheme service?

PDP will propose data quality metrics and assist in facilitating by sharing data cleansing best practice. The regulators will be responsible for establishing data quality metrics / benchmarks and any assessments.

Q5. For pension schemes to match the pension with the customer, there may be some minimum PII, pension schemes may need. How would such search parameters be gathered from customer and shared with the pension schemes?

Where suppliers anticipate a need for PII (e.g. minimum matching details), please propose a secure design for the dashboards service to pass into the central services.

Q6. Will the successful supplier of the PDP infrastructure be allowed to offer commercial frontend Dashboards and/or an ISP service solution?

This is yet to be decided, but there may be commercial conflict and segregation of duties implications which need to be considered.

Q7. What is the expected duration of the formal procurement exercise, and what is the target date for the Alpha to commence?

Also, what lag to you anticipate between contract award and Alpha go-live?

The formal procurement exercise timescales depend on which route to market we take i.e. via an existing framework agreement which will result in a shorter exercise, or direct European tender which could take in excess of 12 months to conclude. We will be able to identify our options once we assess the RFI questionnaire responses and see how the interested suppliers are positioned.

Regarding the Alpha commencement date, this will entirely depend on the route to market, how quickly future bidders are able to mobilise, what existing technology they are able to offer, and their experience of delivering similar digital project requirements.

Q8. Is the proposal that there are 43,000 APIs that share the member data with the providers 43,000 times to establish if there is a match? Is that not a security risk too, equal or higher than having a central database of minimum data?

We welcome proposals to mitigate the security risks whilst adhering to design principle stating "There should be no aggregation of user information (the storing of multiple users' data) in any of the components in the dashboard's ecosystem other than by the pension scheme, or an Integrated Service Provider operating on behalf of the provider."

Distributing identity data under consent to however many endpoints for a specific very short term process (matching) is considered to be a much lower risk to privacy and to information breach than an alternative design based on centralised permanent data repository of pension details correlated with that personal information.

The residual risk of misuse of identity data in matching must be mitigated in the design. Additionally, the Pensions Dashboards Programme will ensure that the governance arrangements enforce suitable control measures.

Q9. Going back to the previous question. Are you expecting the pension provider to search manually for a match?

While there may be some limited support for offline search of smaller providers (if they are not exempted) most providers are expected to offer digital find interfaces or contract with integrated service providers to do so on their behalf.

Q10. Does that mean that the data will be shared with companies where a match is not found? Have you considered the risk and control of the data being sent to a company where there is no match and then what is done with that data and how the end user has control of their data?

Initial threat modelling was conducted during secure system design and the risk of exploitation by a third party with the following mitigations suggested: Strong privileged access controls, Protective Monitoring, Audit, Business change control. We would welcome further proposals to mitigate this risk.

Q11. You mentioned the pension provider may outsource the searching aspect. How will the end user manage their data and where it goes?

End users will be given the option to limit and select the providers that are searched. Pension Finder requests will only be forwarded to pension providers according to consent and authorisation policies.

Q12. The "aim" previously included the phrase "in a place of their choice". Is this a deliberate omission or a change in policy following amendments proposed in parliament?

There is no change in policy, the digital architecture that the PDP is delivering will support multiple dashboards.

Q13. Is there a preference for technical components that exist today or are you open to considering bespoke solutions that meet the architecture requirements?

Bespoke and existing technical components will be considered together on their merits.

Q14. If consent and authorisation being held in PFS will this not hold personal data to be able to identify them?

Consent and authorisation records will need to be associated with user accounts and credentials. PII data usage should be minimised in line with Data Protection by Design principles.

Q15. Please could you provide a link that details how to engage with you, from a dashboard provider perspective?

We are presently developing the scope of the Dashboards Usability Working Group. Once that is agreed we will publish it on our website. Please contact us on mailto:infopdp@maps.org.uk if you are interested in being part of the group.

Q16. Can you speak about the overall timeline for the PDP? i.e. when do you anticipate pension providers will have functioning APIs? when can the first user expect to use the dashboard?

The Pensions Dashboards Programme is planned and managed according to the Agile phases identified in the RFI and will be flexed in response to engagement and readiness of the pension providers.

Q17. The ecosystem diagram shown this afternoon describes a consent and authorisation component. This component us not described in the diagram in the RFI document. Please can you confirm if this new component is in the scope of the RFI or will it be covered in the IPV market engagement scheduled for Nov 2020?

In the ecosystem diagram, the Consent and Authorisation Service is indeed separated from the PFS. It is in scope of the RFI and it remains entirely possible (perhaps even desirable) that the user perceives that the 'PFS' and the 'Consent and Authorisation' services are the same thing, but note this is a user experience design issue.

Q18. Who will be responsible for data failure, or the wrong user getting other people's data?

Without prejudging the liability model design, it is likely that the existing data controllers will remain responsible for compliance with data protection, disclosure and records keeping regulation. Matching criteria must be carefully designed by pension providers to ensure that false positives are minimised (and wrong users getting other people's data).

Q19. Without storing or caching the user identifiable information would the customer have to do the pension search every time when they login to the service?

User identifiable information will not persist within the ecosystem. Once users have verified their identity to the required level of confidence, they will only need to authenticate to the service. They may choose to search again or refresh their pension entitlement details. We welcome recommendations to efficiently reunite users with their pensions and proposals on pension search service interaction.

Q20. Does this structure mean that all dashboards and all pension providers have to use the same system to send the requests for data and the customers data to the receiving party? If so, surely this will be an uncompetitive system which is likely to drive up costs and drive down efficiencies?

A single PFS is our starting position while the architecture is developed and tested. The existing architecture does not preclude multiple PFSs in the future if the need arises.

Q21. The design rationale provided in Candidate Architecture 2.2: Why does the DWP Architecture have central services?

The 'middle tier' of the infrastructure enables some key features that are critical for the architecture. These are listed below:
- A uniform interface for pension providers/schemes (and ISPs).
- No requirement for pension providers/schemes to develop their own online presence, nor implement their own customer facing authorisation and consent capability.

- Provide standard assurance levels as providers/schemes do not have standard assurance levels (even for any which do offer online accounts).
- User Managed Access (UMA) APIs and consent and delegation management: It is unlikely that those providers/schemes which do have online accounts are running User Managed Access (UMA) API services, nor related consent processes which are scoped to include external lower assurance software or manage delegation (to IFAs or MaPS guidance specialists).
- Provide a level of assurance which enables all participating to meet legal obligations and duties, irrespective of which dashboard an individual is using to find and view their data.
- A simple user journey.
- Find pensions where no details are held or known by the user.

Q22. Are you able to share outputs of the Discovery phase?

The feasibility work that DWP undertook in 2018 was the discovery phase for this project. DWP then led a consultation exercise and published the Government's response to the consultation in April 2019. You will find the link in papers accompanying the RFI questionnaire.

Q23. The programme advises that the proposed digital architecture will enable multiple parties to be connected in a secure ecosystem that delivers for individuals. The Ecosystem diagram shows at a high-level the different parties involved and how they are connected. For the work to date, is there a defined EA architecture and available artefacts, for example:

- Architecture Vision & standards.

We have shared a proposed architecture which was introduced by DWP in their consultation response. The Consultation response states the vision and outlines some key principles and requirements.

- Business Architecture & standards.

To be developed.

- Information & Data Architecture & standards.

To be developed through the Data Working Group.

- Technology Architecture & standards.

Some specified on the consultation response and others to be developed and tested.

Q24. Relating to Q1 of the RFI: "Please state which element(s) of the Pensions Dashboards Service central digital architecture ecosystem your organisation will be interested in bidding for." Does this question relate to all the elements (Pension Finder Service, Identity Service, Governance Register, MAPS Dashboard + other) or just the RFI related elements (Pension Finder Service and Governance Register)?

This market engagement exercise is focussing on the Pension Finder Service, consent and authorisation, and Governance Register. The Identity Service will be dealt with separately – however, happy to take any input at this stage which we will use to inform the IDV market engagement.

Q25. We understand that you are looking for possible product accelerators to support the Pensions Dashboards Services. Can you confirm what other services you would like to

include? Such as any involvement in setting up governance and standards with industry/ regulators, industry/end customer research, PDS service design, setup operation/service model and operational support services for Pension and Dashboard Providers?

Please indicate additional services you are able to provide or support in your response. It will help us to assess what is available out there.

Q26. Relating to Q2 of RFI: "One of the contractual models we are considering is for a Design, Build, and Run service for the Pensions Finder Service and Governance Register. In your view, are there any alternative commercial / delivery models you believe can help deliver these requirements in the best and most economical way?"

Is the "Design, Build, and Run service" limited to technology, or will this include operational and support services for Pension Provider and Dashboard providers?

We are currently only focusing on the procurement of the central architecture to support the Dashboards Service operate – which is mainly limited to technology, standards and operation of the central architecture. Any operational or support services for pension providers and dashboard providers is outside the remit of this exercise or of the programme. However, the programme will look at the future operating model and governance of the ecosystem, which will naturally provide a peer group for support.

Q27. Relating to Q7 of RFI: "To assist us in understanding and benchmarking the potential cost of delivering the architecture solution for a Pension Finder Service, and Governance Register, how much do you estimate it would cost to:

a) Stand up the Alpha (testing) phase for each element?

b) Deliver the overall final product / service requirements for each element based on your proposed commercial / delivery model?"

Does the scope of work include any aspects of defining the open standards and ecosystem governance framework?

PDP Open Data Standards will be developed by the Data Working Group in close collaboration with pensions providers and schemes. The ecosystem governance framework will be developed in due course. We expect successful bidders of the infrastructure to be involved in further development of the standards and governance framework alongside regulators and others.

Q28. Please provide findings of the Pensions Dashboards Prototype Project e.g. has the ABI prototype been built as an evolutionary prototype built on a target state technology architecture?

Please refer to the link provided in the RFI supporting document for further information.

Q29. Does the scope include a Pension Finder user interface for consent (as mentioned in Q24 of the RFI?)

The Pension Finder Service needs to interact with the Consent and Authorisation service to enable the Pensions Dashboards users to initiate the search for their pensions.

Q30. Please confirm if the estimated cost of delivering the architecture solution for a Pension Finder Service should include live data for the Alpha phase.

Please include a breakdown of estimated costs for Alpha phase testing including provision of synthetic / pseudonymised test data and end-to-end interface testing.

Q31. Relating to Q13: "What technical and business challenges do you foresee from creating and consuming services from a wide number of pensions providers?"

Please clarify who will take ownership of the on-boarding process for pension providers.

The phasing and staging will be guided by legislation and input from pensions providers.

Q32. Relating to Q15: "Please confirm that all core functionality of your proposed solution would be exposed programmatically via some form of API? This approach provides integration and interoperability flexibility should that be required."

Please also confirm the definition of 'interoperability', in terms of with whom and for what purposes. We understand that working to open standards implies this, however, could you please clarify further?

At present we are referring to interoperability between the various features of the architecture but in the longer term keeping Open Finance in mind.

Q33. Relating to Q17: "What experience does your organisation have with the adoption of open common government platforms?"

Please clarify if 'open government platforms' refers specifically to the gov.uk platforms (for example verify, notify, pay etc.) or does this mean generally building platforms to meet open government standards?

This is about your experience of building platforms that meet open government standards.

Q34. Relating to Q20: "The architecture depends on a central Consent and Authorisation service. When fully functional, we expect Pensions Dashboards to have a high number of users. In your response please cover the following:

a) What evidence do you have that your service will scale to support the likely load?

b) How will you design, plan and assure for this requirement?

c) Provide examples of any specific technologies or frameworks used."

Please confirm if an identity services has been selected and if not, how many there might be?

Identity services suppliers will be identified in a separate market engagement planned to commence in Nov 2020. Once completed, we will then be in a position to advise if, and how we will commence any required procurement process.

Q35. The requirements document states that the Pension Finder Service "acts as a trust anchor, providing critical assurances for other elements within the ecosystem. For example, it initiates user authentication and manages user consents and permissions therefore, the consent and authorisation process are a part of this requirement."

It also states that the Identity Service "allows users to authenticate themselves (prove they are who they say they are) so that they can access other elements of the ecosystem."

Please can you confirm what elements of identity verification and ongoing user authentication are in scope for the RFI and future procurement exercise? Specifically, is the method of ongoing user authentication (i.e. how a registered user logs in to the dashboard) in or out of scope?

Identity verification and authentication is not part of this market engagement exercise.

Q36. Could you clarify whether the intention is for the Pensions Dashboard to make use of existing identity services e.g. GOV.UK Verify?

No decisions have been made. We will undertake market engagement for the Identity Service later in the year.

Q37. The RFI document states that the Pensions Dashboards Prototype Project "demonstrated most of the requirements needed for the architecture but did not include the following elements: Trust framework or delegated access; Use of open standards"

Please could you expand on this point and give any insights to the trust frameworks or open standards you are considering as part of the PDP?

We are considering User Managed Access 2 (UMA2) for delegated access. The open standards to be used will be selected based on the underlying data requirements and therefore, the most applicable data standards if one exists. The same will be true of the APIs used to form the integration layer.

Q38. Is there a preference, at this stage, for the PDP Digital Architecture to be provided as a completely managed solution, or delivered into an existing 'internal' data centre / Cloud infrastructure?

PDP Digital Architecture can be delivered and managed on a Government Digital Service standards compliant infrastructure. Please recommend service management solution proposals from your experience.

Q39. And if delivered into an internally managed infrastructure, again, is there a desire to have this 'fully managed' or managed by trained internal resources?

We have yet to decide on service management. Please make recommendations in your RFI questionnaire response.

Q40. Can you please comment on the anticipated timescales for all envisioned elements/phases of the project?

This is covered in the webinar presentation slide deck which is available on the PDP website.

Q41. Is there a vision to create a 'standardised' format for incoming data streams from the UK's 43,000 pension provider sources?

And if so, is there a vision to mandate preparedness and connection with this format, and in what timescales?

We are exploring this, and the work will be led by the Data Working Group who have launched a Call for Input into data standards for dashboards on 6th July 2020.

Q42. Is Our understanding is that the desired infrastructure will ideally store no personally identifiable information and act purely as an 'information exchange', connecting independent pension dashboards, with the pension provider community. Would any consideration be given to using the new central digital architecture to store customer-consented information, if taking that approach could be shown to offer a broader set of services to end customers, and the chance of a more successful level of end user adoption?

The central digital architecture will not hold any customer related personal information – with or without their consent.

The RFI Questionnaire is available to <u>complete online</u>.

The deadline for submitting the RFI Questionnaire is: 17:00 Friday 31st July 2020.

Unfortunately, we will not be able to consider any responses received after this deadline.

Please note, information gathered during this process including any RFI responses, will not be scored or used to pre-select or prohibit suppliers from participating in any future formal procurement process. Any competitive tender opportunity will be advertised as per the Public Contracts Regulations (PCR 2015) guidelines through a compliant route to market.