Pensions Dashboards Programme

Identity verification approach market engagement

October 2020

Contents

Background

1. The Financial Conduct Authority (FCA) recommended, in its Financial Advice Market Review in 2016, that industry should make pensions dashboards available to individuals to make it easier for them to engage with their pensions, a view which the government echoed in its budget that same year.

2. An industry-led project, set up in 2016 sponsored by HM Treasury and managed by the Association of British Insurers (ABI), developed and demonstrated a prototype for the dashboard in 2017. The project continued independently of government, publishing its findings in October 2017, which included the call for a government-backed delivery authority to drive the completion of the project.

3. In December 2018 Government launched a consultation, engaging widely with stakeholders across the pensions industry, to identify issues and options for delivering the service. In April 2019 it set out its position in a response document stating that:

   "Government will legislate to compel pension schemes to provide their data; and

   The Money and Pensions Service (MaPS) will have responsibility for enabling delivery of the dashboard service working with the pensions industry"

4. The Pensions Dashboards Programme is responsible for developing the pensions dashboards ecosystem which will enable individuals to view their pensions data via their chosen dashboard. The widely shared aim for pensions dashboards is to enable individuals to access their pensions information online, securely and all in one place, thereby supporting better planning for retirement and growing financial wellbeing.

5. The consultation response set out some overarching design principles which indicated that all dashboards should:

   - put the individual at the heart of the process by giving individuals access to clear information online;
   - ensure individuals' data is secure, accurate and simple to understand - minimising the risks to the individual and the potential for confusion;
   - ensure that the individual is always in control over who has access to their data.

6. At the heart of the design is the need for a trust model, which enables all parties to operate within the system, with complete confidence that other participants are identifiable and have authority to act in the way that they are. Within this framework, users are required to evidence their identity through a digital identity solution, which will mandate that a minimum level of confidence is established.

7. The government response to the consultations states:

   "To enable a sufficient level of trust in the service, the department expects a standard level of identity assurance for all users (individuals and delegates) that satisfies the National Cyber Security Centre's Good Practice Guide 45 on 'Identity Proofing and Verification of an Individual'.

   Our conclusion: the delivery group must agree on a standardised level of identity which complies with the National Cyber Security Centre's Good Practice Guide 45[1]"

[1] https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual

8. This paper presents the basis of an identity process and requests input from identity providers.

9. The PDP are keen to understand the nature of services that identity providers currently support and feedback on indicative standards proposed.

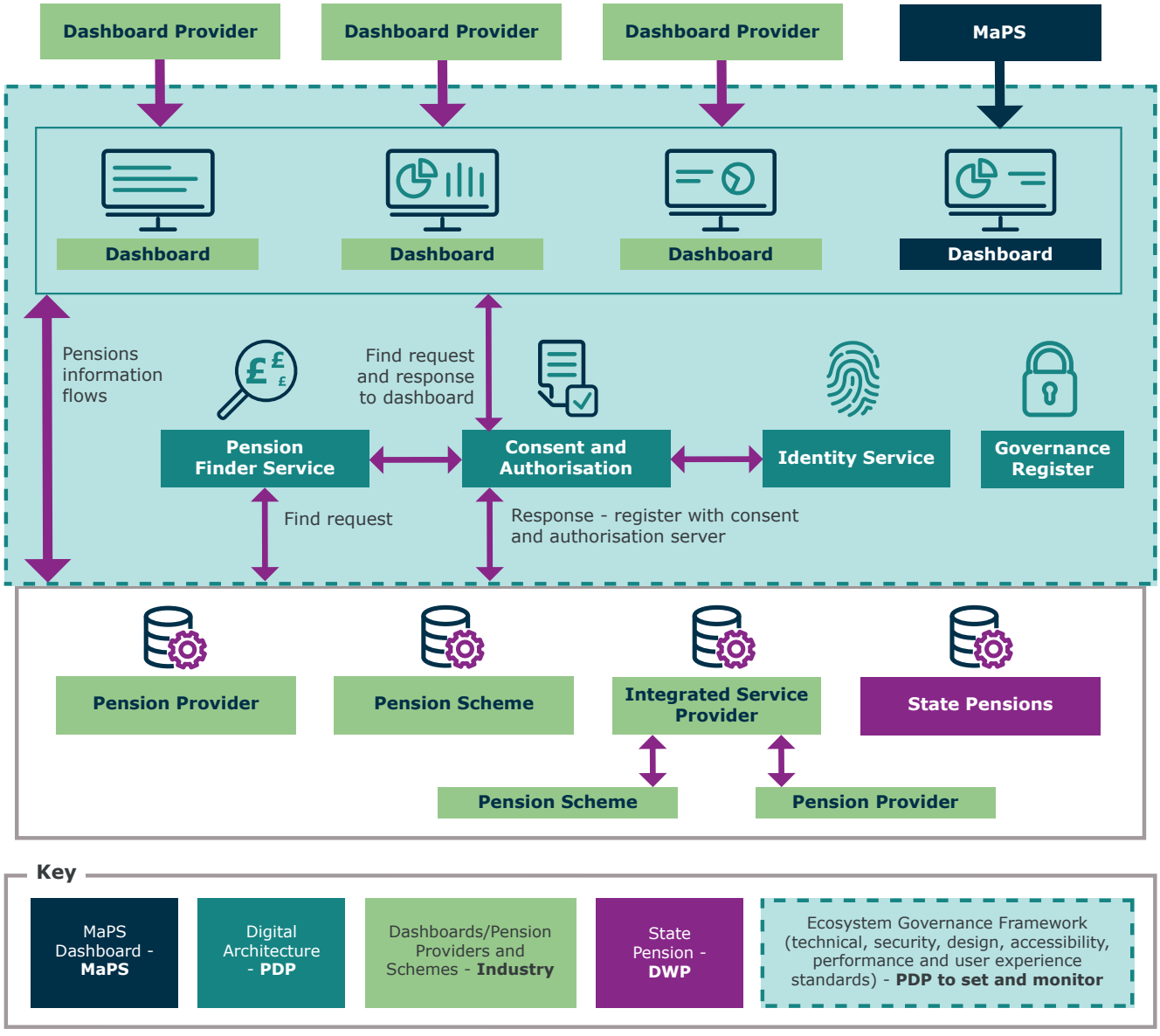
10. We invite feedback from parties that may be interested in providing all or part of the identity service, or that can contribute to our ongoing work to define appropriate standards for the dashboard ecosystem.

Architecture and identity service

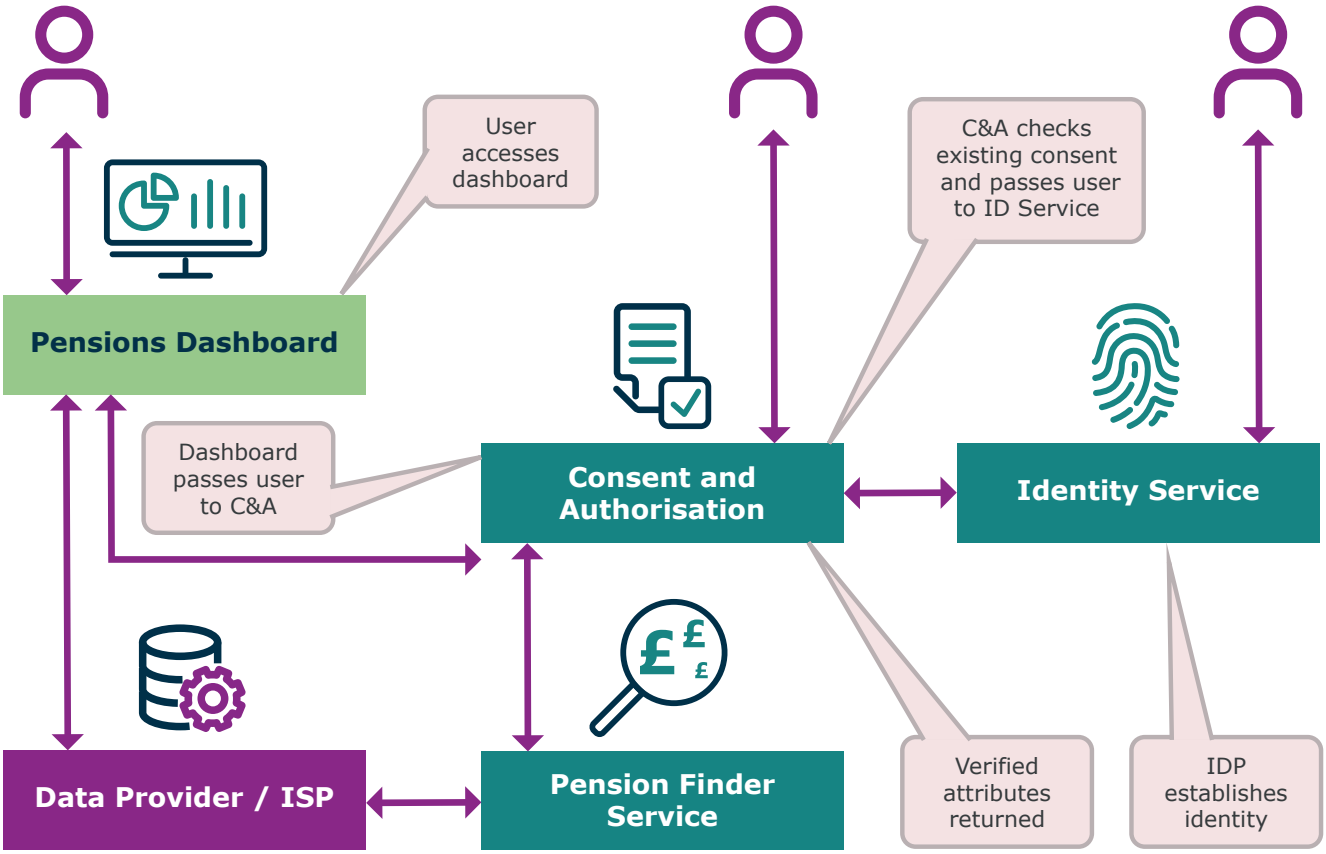
11. Key components of the central architecture, that the PDP is responsible for delivering, have already been the subject of a separate market engagement exercise.

12. The digital architecture includes an identity service at its core.

Proposed digital architecture - overview of the Ecosystem



13. The user will be passed from the dashboard of their choice to the consent and authorisation module, which will manage their consent and pass them to the identity service.



14. Data providers (i.e. pension providers, schemes, trustees etc), as data controllers, retain the responsibility for incorrect disclosure of data. It is vital that they have confidence that the party to whom they are releasing data is who they say they are and has authority to receive the information.

15. Data providers should consider whether the level of assurance of identity is sufficient to prevent identity impersonation (based on creeping change of personal details) to discover the existence of a pension asset and the registered personal identity information, sufficient to mount a fraud attack directly on the PP by other means, especially for entitlements valued below the threshold for which an adviser must be engaged.

16. Before the user can find their pension entitlements, the identity service will prove their identity to a standard acceptable to the ecosystem as a whole.

17. Data standards that are being developed to support the ecosystem, include a matching data set, which will provide information that pension data providers can use to identify a user's entitlement.

18. The user will be asked to consent to an identity provider validating their identity and confirming the following attributes:

    a. first name
    b. family name
    c. date of birth
    d. address

19. Additionally, the user may be asked to provide the following, which may not be validated by the identity provider:

    e. national insurance number

    f. address history

    g. previous names

    h. email address

    i. telephone number

20. The PDP is currently working with pension providers to understand the breadth of information required to enable them to locate a pension entitlement.

21. Verified attributes, from ID service, and user asserted attributes (highlighted in 18 and 19 above) will be provided to the PFS, which will co-ordinate communication with data providers.

Trust framework / model

22. All components of the architecture, including dashboards and data providers, are covered by a trust model that is based on mutual and federated trust.

23. All organisations abide by legal conditions and standards that support a common 'root of trust'.

24. This role is performed by the governance register which maintains all affiliations within the ecosystem e.g. dashboards, data providers, ID suppliers, and each component is registered in the governance register and managed accordingly.

25. Trust is assured and enforced by services acting as trust brokers, on behalf of other services: e.g. the identity service authenticates a dashboard user, and the consent and authorisation module authorises release of pension data based on the user's consent.

26. By the common root of trust, each service may in turn trust each other, e.g. the implicit trust of a relying service (pension data provider) to return data to an authorised requesting service (pension dashboard).

27. All services within the ecosystem, including the pensions dashboards and the pension providers, should explicitly trust each other within the common trust framework.

28. The consent and authorisation module is the trust anchor for identity, authentication and authorisation: it enforces user authentication by the identity service, provides identity attributes to the pension finder service, and access authorisation to the pension providers.

29. The pension providers can rely on and implicitly trust the consent for the user to access an individual's pension entitlement data by virtue of their trust relationships within the framework.

30. MaPS, or an appointed organisation, will monitor, audit and enforce compliance with common standards, operational practices and levels of assurance, under the governance terms to be determined within the agreements between all parties involved.

31. The PDP is currently defining a liability model that supports the contractual arrangements that will be applied to support the trust framework.

32. The identity service will be relied upon to provide strong authentication credentials of a user and identity verified to a defined level of confidence.

Identity standards and approach

33. As indicated in the background section, the response to the consultation has dictated that the identity standard should comply with good practice guide (GPG) 45.

34. National Cyber Security Centre's good practice guides are a framework that supports definition of standards for identity to suit the purpose of the service being provided. In this case that purpose is for the release of pension information to an individual.

35. An identity standard under the good practice guides (for the purposes of the Pensions Dashboards Programme) concentrate on two elements:

    a. confidence in the identity

    b. confidence in the authentication approach

36. Under the good practice guides, identity services provide a level of assurance (LOA) that can be used as a measure of the strength of the identity asserted by an individual.

37. GPG 45, which reflects level of confidence in an identity, should be considered alongside GPG 44[2], level of authentication credential.

38. Level of confidence provides a view of the evidence provided by the user and attributes values across five measures.

39. Level of authentication credential assesses the method by which an identity service proves the person requesting access is the same person as previously permitted.

Good Practice Guide (GPG) 45

40. As documented in GPG 45, an identity is a combination of characteristics that identifies a person. A single characteristic is not usually enough to tell one person apart from another, but a combination of characteristics might be.

41. The process of checking an identity takes characteristics included in a 'claimed identity', provided by the user with consent, (in line with the attributes required for the matching process) and validates them against five criteria / steps:

    - get evidence of the claimed identity
    - check the evidence is genuine or valid
    - check the claimed identity has existed over time
    - check if the claimed identity is at high risk of identity fraud
    - check that the identity belongs to the person who's claiming it

42. Building an identity over a period of time allows for more experience and verifiable sources to become available. Each element of the checking process builds a score, which contributes to an overall level of confidence.

43. The level of confidence depends on:

    - how many pieces of evidence are collected
    - which parts of the identity checking process are undertaken
    - what scores each part of the identity checking process attain

44. Scores can be combined in a number of ways, based on the identity criteria, to provide an overall level of confidence. These are measured as:

    - low confidence
    - medium confidence
    - high confidence
    - very high confidence

[2] Good Practice Guide 44 - Level of Authentication Credential

45. Full details of how these levels of confidence are attributed are incorporated in GPG 45.

46. PDP, with the assistance of identity providers and data providers, will need to determine the appropriate level of confidence required to support the release of information.

Good Practice Guide (GPG) 44

47. Level of assurance through GPG 44, takes into consideration the ways in which the user is authenticated.

    'You might need to know if someone has already used your service before you give them access to it. This is called 'authentication' and can be useful if users need to sign into your service more than once'

48. There are different types of authenticators. An authenticator will usually be one of the following:

    - something the user knows (often referred to as a secret)
    - something the user has
    - something the user is

49. Services can be protected by using a combination of two or more authenticators =- '2 (or multi) factor authentication' (2FA).

50. 2FA should, but does not need to, utilise two different types of authenticator, as this will reduce the risk of two similar types of authenticator being compromised, which is more likely than two different types.

51. An authenticator can be low, medium or high quality. The quality of an authenticator will depend on how secure it is.

52. Examples of low, medium and high-quality authenticators can be found in the GPG 44 document.

53. PDP will need to determine the approach to authentication which provide an appropriate level of control, while not adding unnecessary complexity to the user journey.

Identity requirements

54. In making this proposal on the approach to the identity service, PDP recognises that feedback from identity providers and the pensions industry may suggest alternate approaches.

55. The identity service will be required to prove identities of individuals that may be a user viewing their own pension entitlements or representing a regulated financial advice company or a guidance body, with delegated access rights.

56. In addition to assuring the identity of a user with delegated access, the ecosystem will be required to ensure their registration / professional accreditation is appropriate and valid.

57. At present PDP is not determining whether the identity service will support a **single or multiple identity providers**.

58. Similarly, no decision has been made as to whether the service would directly integrate with multiple providers or whether the use of a **broker / hub** would be more appropriate. This will depend on the responses received during this market engagement and on the cross government and private sector identity landscape at the relevant time.

59. PDP would look to define the API's and communication protocols once the approach to identity has been

further clarified and other elements of the architecture baselined.

60. In order to enable future development and innovation, it may be desirable for the identity service to support interoperability with other markets/ schemes.

61. In accordance with the outcome from the consultation response highlighted in the background to this paper, the PDP is currently focussing on GPG 45 (supported by GPG 44) as the appropriate framework from which to derive a standard.

62. Under GPG 45, PDP indicatively proposes to the pensions industry that **medium level of confidence** might meet their requirements for assurance of identity prior to information release relating to find and view.

63. It is believed that a **low level of confidence** will not be sufficient to provide the level of assurance pensions Data Providers will require.

64. In the event that there is compelling evidence that a lower level of confidence is adequate, PDP will review the option to adopt it, following consultation, even if it does not match the GPG45 defined levels of confidence, but follows the principles.

65. Under GPG 44, PDP similarly propose that a **medium level of authentication** might meet the requirements of the pensions industry. This should incorporate a minimum of 2 factor authentication and attendant security of credential lifecycle and transaction monitoring.

66. Compelling reasons to support a different level of authentication will be considered, under consultation with Data Providers.

67. It is proposed that on initial identity assertion, the Consent and Authorisation module will issue a token that will have a defined life.

68. This approach will streamline the user experience such that there will be no need to re-authenticate until the token has expired. No defined life has been determined yet and proposals will be welcomed. We note Open Banking has set an expectation of 90 days between strong re-authentications.

69. The identity service will need to reach a high proportion of the UK population. One of the key challenges will be to support members of the public that do not have access to Government issued identity documents such as passports and driving licence or have limited credit history.

70. PDP will be seeking feedback from Identity Providers on suitable approaches to broadening the reach of the identity service.

71. The eco-system will be the only relying party supported by the Identity Service – the Consent and Authorisation module will orchestrate transmission of asserted attributes, with the Users consent, on successful validation of the user's identity.

Request for Information

To support the ongoing development of the requirements for the pensions dashboards central identity service, the PDP is looking for information associated with the above requirements and in relation to the intentions of identity providers within the commercial marketplace.

This Request for Information runs from **21st October** to **27th November 2020**

Please answer each of the questions provided in 200 words (each question) and provide supporting evidence where indicated.

Complete the questions online.

1. Company name
2. Contact name
3. Contact email address
4. Contact phone number
5. Please describe the service your company provides and if you partner with any other organisations to deliver this service.
6. Please advise whether your firm can prove identities in line with GPG 45.

   7a - If yes, can you support levels of confidence low and medium.
7. Do you agree that GPG 45 level medium is the correct approach for the pensions dashboards service to pursue for a find and view pensions function?
8. If not, please explain why and what alternative you would propose.
9. Would your service support a level of confidence between low and medium if it were deemed appropriate?
10. Please provide details on how you would achieve a medium level of authentication for users in line with GPG 44.
11. Please indicate whether you agree that GPG 44 level medium is the correct approach for the pensions dashboards service to pursue for a find and view pensions function.
12. If not, please explain why and what alternative you would propose.
13. Please describe how your service would meet the requirements defined above.
14. Please indicate whether you would you be prepared to share details of your standard interfaces.
15. Please indicate whether you could provide an indication of the number of identities your service has currently verified.
16. Please advise your daily, monthly and annual capacity for identity verification.
17. Please advise your success rate for identity proofing at both low and medium levels of confidence and define the population to which that success rate applies (e.g. UK adults).
18. Can you confirm typical elapsed time taken to establish an identity through your service?
19. Please provide an indication of charges for the identity verification service.
20. How would those charges vary with:

    a. Volume

    b. Re-usability
21. How does your company support users with no photo-id, thin files, or are otherwise difficult to prove?
22. At present, it is unclear whether all of the attributes included in the proposed matching data set (as indicated in the above) can be validated and verified. Please provide an indication of which data elements you can authenticate.
23. For those attributes that you cannot validate and verify, what would you propose to resolve the gap?
24. What is your organisation's approach to staying up to date with developments in digital identity?

Commercial aspects

25. Please state which element(s) of the identity service (as set out in the supporting document) your organisation will be interested in

bidding for (services, software product, or end-to-end solution)

26. Please state if you are intending to bid for both the PDP main architecture solution and the PDP identity service requirements.
27. Please advise if your organisation is available through any of the existing Crown Commercial Service (CCS), or any other public sector digital and technology related framework agreements?
28. If yes, provide the full title and reference number of each framework agreement you are awarded to in your response.
29. If your organisation is not on the CCS digital frameworks, would your organisation be open to entering commercial partnerships with suppliers available through the following CCS digital frameworks to bid for the identity service requirements?

    a. Digital Outcomes & Specialists 4
    b. Technology Services 2
    c. G-Cloud 11

30. If yes, please state your partnership options.
31. Which legal jurisdiction does your company fall under?
32. To assist us in understanding and benchmarking the potential cost of delivering the identity service, how much do you estimate it would cost to:

    a. stand up the Alpha (testing) phase
    b. deliver the overall final product / service requirements over a four-year contract period

33. How would your solution approach support our goals of complete flexibility with respect to ongoing intellectual property rights (IPR) ownership? For example, we may require that the IPR of the whole service is vested in such a way to enable a future change of suppliers of the maintenance, enhancement and operational system.
34. Please state if you intend on using your own product, open source or a commercial off the shelf (COTS) product to meet our requirements.
35. If applicable, please state what user licensing model you would propose for the identity service product (enterprise, organisational, user, etc).
36. At a high level, describe how you will support our requirement to move to another supplier if, and when that situation arises?

    The scope of this could include future development and/or support arrangements.

37. What, if any, technology related challenges do you foresee in the legal and regulatory areas? At a very high level describe your proposed approach and experience to overcoming these.

Pensions Dashboards Programme