Pensions Dashboards Programme

Identity approach

Call for Input from data providers

February 2021

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[1], 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. As a result, the Pensions Dashboards Programme (PDP) was created to lead the work of delivering an eco-system, via which members can find and view their pension holdings. 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 that 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 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[2&3]."

[1] Pension Dashboards government response to consultation
[2] Good Practice Guide 45 - identity-proofing-and-verification-of-an-individual
[3] Good Practice Guidelines are published by Government Digital Services (GDS)

8. This paper presents the basis of an identity process and seeks clarification from data providers (ie pension providers, schemes, trustees etc) on what they believe would be an **acceptable identity standard** for them to provide pension information to a user.

9. PDP has recently undertaken a Request for Information exercise with key participants from the identity market which, along with the feedback sought by this Call for Input, will help shape the requirements defined for the identity service.

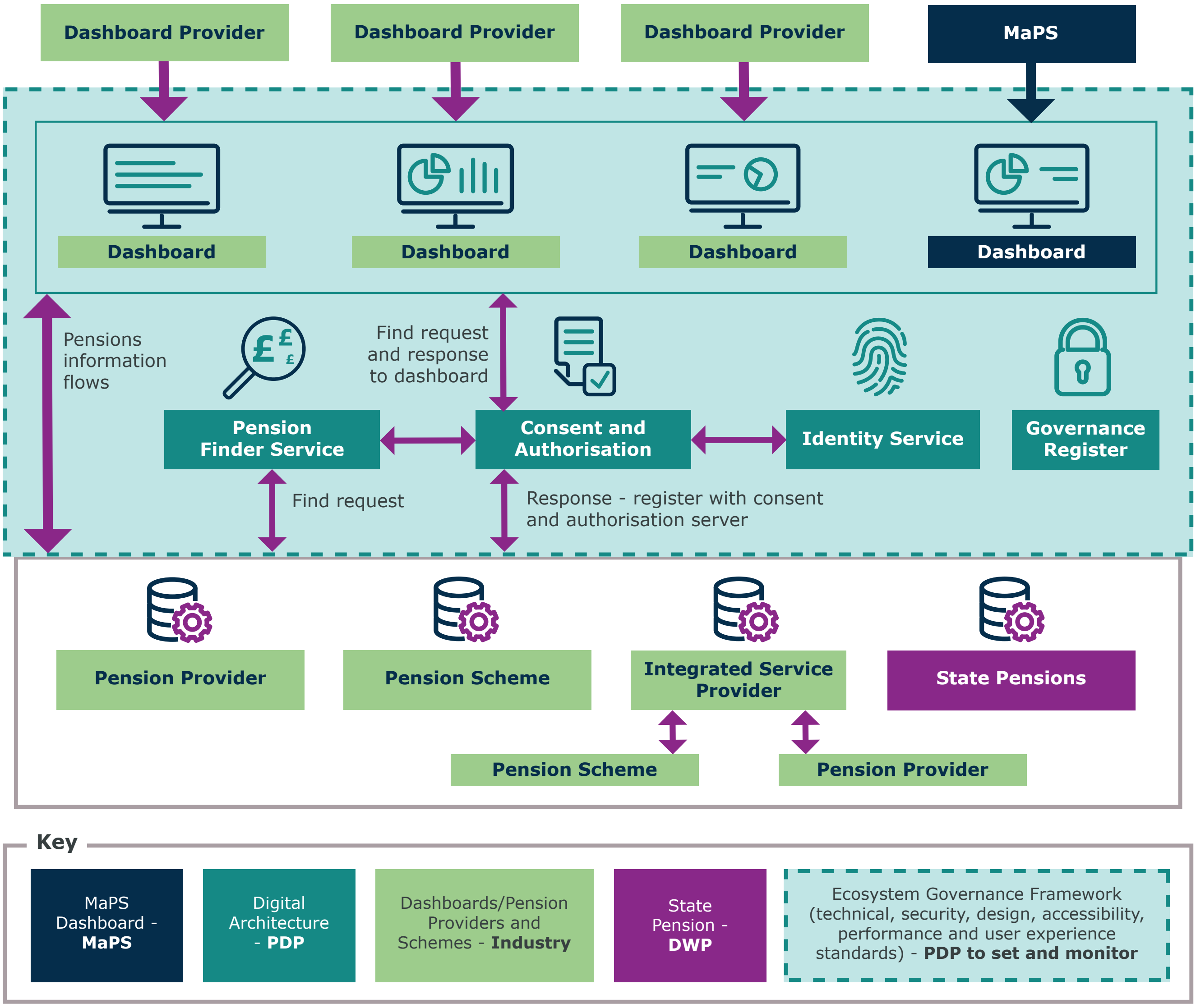
Digital Identities

Why are identities important?

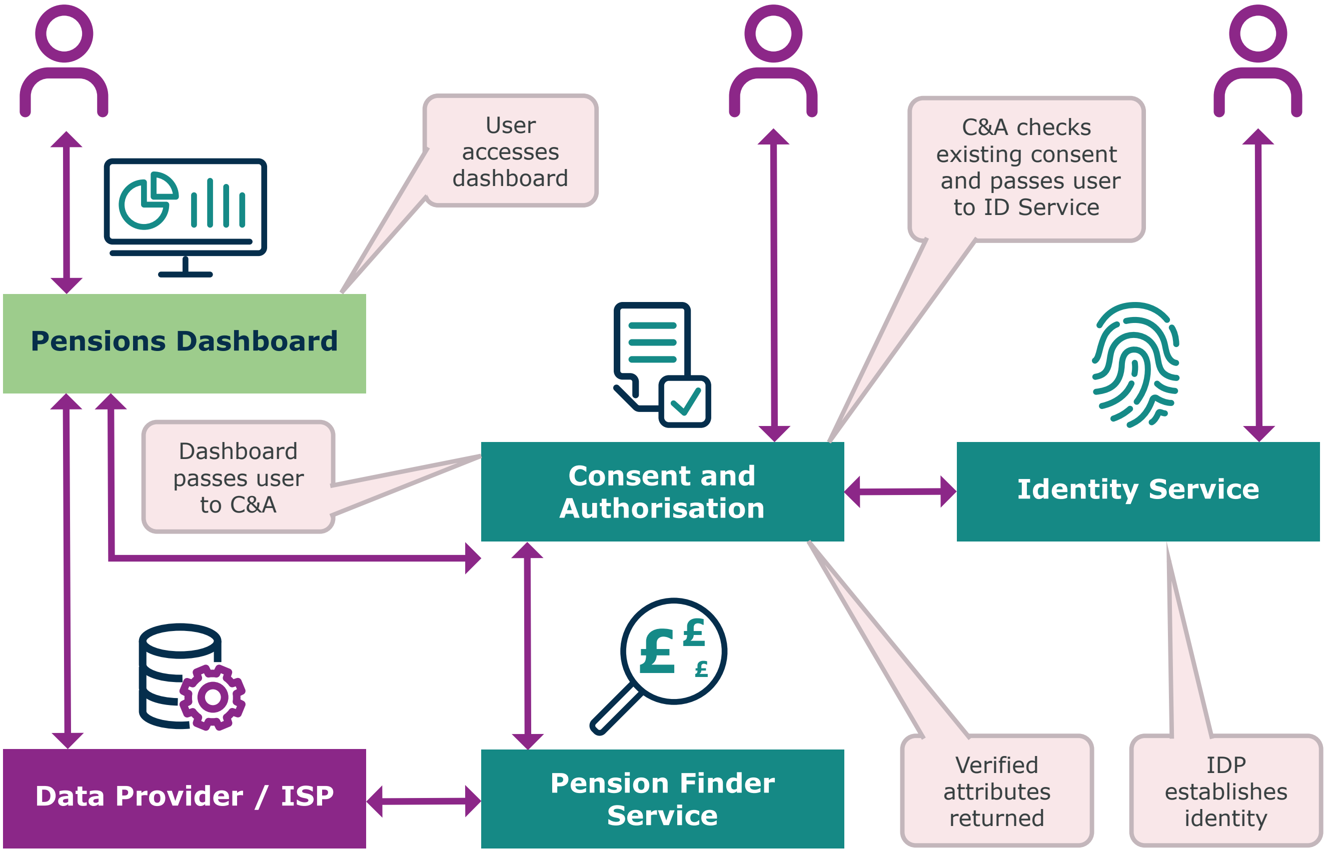
10. Data providers, as data controllers, retain the responsibility for incorrect disclosure of data. It is vital that they have confidence that the party to whom they are releasing data is who they say they are and has authority to receive the information.

11. The digital architecture includes an identity service at its core, which is intended to ensure we can verify the user to an acceptable level of confidence.

Proposed digital architecture - overview of the Ecosystem


Dashboard Provider
Dashboard Provider
Dashboard Provider
MaPS
Dashboard
Dashboard
Dashboard
Dashboard
Pensions information flows
Find request and response to dashboard
Pension Finder Service
Consent and Authorisation
Identity Service
Governance Register
Find request
Response - register with consent and authorisation server
Pension Provider
Pension Scheme
Integrated Service Provider
State Pensions
Pension Scheme
Pension Provider
Key
MaPS Dashboard - **MaPS**
Digital Architecture - **PDP**
Dashboards/Pension Providers and Schemes - **Industry**
State Pension - **DWP**
Ecosystem Governance Framework (technical, security, design, accessibility, performance and user experience standards) - **PDP to set and monitor**

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


User accesses dashboard
C&A checks existing consent and passes user to ID Service
Pensions Dashboard
Dashboard passes user to C&A
Consent and Authorisation
Identity Service
Data Provider / ISP
Pension Finder Service
Verified attributes returned
IDP establishes identity

13. 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.

14. Data standards that are being developed to support the eco-system, include a matching data set that will provide information that pension data providers can use to search for a user's entitlement.

15. At present, the user will consent to an identity provider validating their identity and confirming the following information:

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

16. 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. email address
    h. telephone number
    i. previous names

17. The PDP undertook a data standards Call for Input, which helped our understanding of the breadth of information required by data providers to enable them to locate a pension entitlement.

18. It is anticipated that the identity service will provide verified identity attributes to the pension finder service, alongside user asserted

attributes (highlighted in 15 and 16 above), which will then co-ordinate communication with data providers.

19. Providing a central identity service in the architecture provides certainty in the strength of the identity verification. Within the trust model, it ensures trust persists across the ecosystem.

20. It has the additional benefit of providing an open solution that enables the user to use a single identity to access and manage their consents, even if they view their pensions on more than one dashboard.

21. This supports the principle defined in the consultation response document that users must be able to manage their consent independently of any dashboard provider.

22. The Central Identity Service will manage identity verification and dashboard providers are free to decide whether they wish to implement their own access management service.

23. The matching data from the pension finder service will be provided via a standard API implemented by the data provider. The data provider will use the matching data to locate a user's entitlements based on their own search criteria, which reflects their interpretation of risk.

What is an identity?

24. An identity is a combination of verified attributes about an individual which, when considered in unison, can provide assurance that a person is who they say they are.

25. In simple terms, if you met someone face to face and they provided an identity document from a trusted source (eg passport), if they match the image in the passport, you would have a high degree of comfort that they are who they say they are.

26. This is harder to do online, where visible validation is more difficult to achieve – this is where identity providers and identity standards look to fill the gap.

27. Identity services look to measure a set of data attributes about the claimed identity against known sources and determine the assurance of the identity.

28. The assurance of the identity is benchmarked against a standard, which determines the strength of the recognised identity.

29. Government Digital Services 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 data to an individual.

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

    a. confidence in the identity

    b. confidence in the authentication approach

31. GPG 45, which reflects level of confidence in an identity, should be considered alongside GPG 44[4], level of authentication credential.

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

[4] Good Practice Guide 44 - Using authenticators to protect an online service

33. 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

34. 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.

35. The process of checking an identity takes characteristics included in a claimed identity (typically, but not limited to: name, address and date of birth) 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

36. By doing different parts of the identity checking process, the identity provider can build confidence that an identity is accurate.

37. Identity checking can be completed at a point in time or can be built over a period as more experience and verifiable sources become available. Each element of the checking process builds a score, which contributes to an overall level of confidence.

38. A 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

39. 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

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

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

Good Practice Guide (GPG) 44

42. 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.'

43. 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

44. Something the user knows could be:

- a PIN
- a password
- an answer to a question that only the user knows the answer to - also called knowledge-based verification (KBV)

45. A secret is usually used with either:

- another piece of information, such as a username or email address
- a token, such as a chip and PIN card, single use authentication code or digital certificate

46. A measure of something the user is would normally take the form of a biometric input. Biometric information is a measurement of someone's:

- biological characteristics, such as their fingerprint, facial recognition
- behavioural characteristics, such as their signature

47. Using biometric information means a service can easily tell if the user who is trying to sign in is the same person who created the account. This is because:

- each person's biometric information is unique to them
- it's difficult for biometric information to be forgotten, lost, stolen or guessed

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

49. 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.

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

51. The quality will be informed by how it was:

- created by a user (or a manufacturer if it's something like a physical token)
- managed (including how the authenticator is issued and updated, and what happens when it's no longer being used)
- captured (if it's biometric information)

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

53. An authenticator can protect the service from being accessed by someone who should not be able to use it. How much protection the service needs depends on:

- what information the user needs to use the service
- what information the service gives the user access to
- what the service or user can do with that information

54. Selecting the appropriate authentication options is dependent on how data controllers view risk and the level of protection required to ensure data integrity.

55. The level of protection afforded by the authenticator/s is measured in a range from low, through to very high dependent on the strength and quality of the authenticator/s used.

56. Other considerations which will need to be factored include:

- recovery processes for forgotten, lost and stolen authenticators – enabling the rightful user to recover access
- revocation processes so that authenticators can be cancelled, and access denied
- monitoring of the credential as it is in use to detect misuse or hijack

Trust framework / model

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

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

59. This role is performed by the governance register which maintains all affiliations within the eco-system eg dashboards, data providers, ID suppliers, and each component is registered in the governance register and managed accordingly.

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

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

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

63. The consent and authorisation service 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 data providers.

64. Data providers can rely on and implicitly trust the consent for the user to access an individual's pension information by virtue of their trust relationships within the framework.

65. The PDP, or an appointed operating body, will monitor and audit with common standards, operational practices and levels of assurance, under governance terms to be determined.

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

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

68. Liability under the framework is currently under review and proposals are in the process of being determined. It will be incorporated within the governance framework being defined for the programme and the ongoing solution.

Proposals

69. In making this proposal on the approach for the identity service, PDP recognises that feedback from identity providers and the pensions industry is

important, and may suggest alternate approaches.

70. 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.

71. 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.

72. At present PDP is not determining whether the identity service will include a **single identity provider or multiple identity providers**.

73. 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 call for input and on the cross government and private sector identity landscape at the relevant time.

74. PDP will define the APIs and communication protocols once the approach to identity has been further clarified and other elements of the architecture baselined.

75. In order to enable future development and innovation, our preference is for the identity service to support interoperability with other markets / schemes.

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

77. A Request for Information to the identity industry was broadly in agreement with this proposal.

78. 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, provided it follows the principles.

79. 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.

80. A Request for Information to the identity industry was broadly in agreement with this proposal.

81. Compelling reasons to support a different level of authentication will be considered, under consultation with data providers.

82. It is proposed that on initial identity assertion, the consent and authorisation module will issue a token that will have a defined life.

83. This approach will streamline the user experience such that there will be no need to reauthenticate 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 reauthentications.

84. The identity service will need to reach a high proportion of the holders of UK pensions (regardless of current domicile). 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.

85. The ecosystem will be the only **relying party** supported by the Identity Service – the consent and authorisation service will orchestrate transmission of asserted attributes, with the users consent, on successful validation of the user's identity.

Request for feedback

As we move into the next phase of analysis, ahead of a planned procurement exercise, the direction remains that the identity solution should be based on GPG 45 and authentication on GP 44. This assertion is based on the principle that a consistent, repeatable and comprehensible standard, which can be independently certified, should be applied that will meet the requirements of both government and industry participants.

To validate that assumption and understand any additional requirements that would need to be considered, the PDP would welcome your feedback on the following points, both from your company's perspective and how you think it will be reflected across the industry:

1. Do you agree that finding pensions and viewing pension details via a pensions dashboard should include a central digital identity, asserted to an appropriate standard, in accordance with the GPG 45?

   If no, what alternative approach would you recommend?

2. The proposal includes a **level of confidence in identity** and a **level of authentication**. Do you have a view on the level of assurance that needs to be achieved to provide comfort to release pension information?

   If Yes, what elements do you think are the primary factors?

   If No, what additional information would you need to be able to make an assessment?

3. The suggested levels of confidence (GPG 45) and authentication (GPG 44) are 'medium', which equates to the previous versions of the standard level of assurance two. Do you agree that this is the correct level?

   If No, what would you suggest is the correct assurance level for both proofing of identity and strength of authentication?

4. Is there an alternative to the default levels of assurance from the Good Practice Guidelines and how would you anticipate them being measured?

5. Does your firm have any view on proofing or authentication methods and operate a current internal standard that differs from the GPGs medium level?

   If Yes, could you please provide an overview that could help direct the programme's approach?

6. The architecture includes the central identity service to ensure that a uniform, controlled process exists, and that a user can easily manage their own consents.

   Please provide your thoughts on this approach and any challenges that you may foresee.

7. Are there any specific requirements that you would anticipate the Pensions Dashboards Programme having to meet when seeking:

   a. your firm's approval for a standard approach to identity assurance

   b. a cross industry agreement on a standard for identity assurance

8. What security related controls (other than identity proofing and authentication) do you see as important in your acceptance of the PDP solution for Pensions Dashboards?

Pensions
Dashboards
Programme