Request for Feedback on the Pensions Dashboard

'Identity Approach'

April 2021

Acknowledgments

PASA is grateful to the authors of this response and members of the PASA Identity Working Group (IWG), the PASA Dashboard Working Group (DWG) and all members' employers.

PASA Identity Working Group

Gary Evans (Board Sponsor)	**Hymans Robertson LLP**
Mark Little (Chair)	**LNRS UK&I**
Casper McConville	**Baker Mckenzie**
Gary Raynor	**LCP**
Adam Smith	**LNRS UK&I**
Luke Davies	**LNRS UK&I**

PASA Pension Dashboard Working Group

Kim Gubler (Board Sponsor)	**PASA Board Director**
Chris Connelly (Chair)	**Equiniti**
Kenneth May	**Origo (Expert Partners)**
Richard Smith	**Independent pensions professional**
Karl Lidgley	**Hymans Robertson LLP**
Stuart Reid	**Hymans Robertson LLP**
Geraldine Brassett	**Capita**
Andrew Short	**Capita**
Chris Batts	**Equiniti**
David Rich	**Accurate Data Services**
Francesca Parnell	**Allen & Overy**
Ian Dack	**Mercer**
Ian McQuade	**Muse Advisory**
Ranjit Shoker	**Deloitte**
Sonya Purkayastha	**Rothesay**
Nick Green	**Criterion**
Phillip Cork	**Aon**
Amy Regler	**West Midlands Pension Fund**

The group is also grateful to the following for their input:

Lucy Stone – liaison at The Pensions Regulator

Kristy Cotton – Chair of the PASA Data Working Group

Request for feedback to the Pensions Dashboards Programme Identity Approach

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?**

a) We do agree with the assertion to an appropriate standard but, **we do not agree with the central digital identity**, if by a 'central digital identity' we mean a single identity provider. We are concerned such centralisation creates a **single point of failure, a single point of attack, limited capacity and a commercial monopoly** that will not enable the open market required to sustain the pensions dashboard ecosystem into the future.

b) We also believe an open market approach to identity is more sustainable and commercially viable. To this end, MaPS should consider aligning with the government's UK Trust framework initiative* designed to create an open identity market.

c) We suggest onboarding and identity verification should start with the pensions dashboard provider (PDP) free to adopt identity services of their choice, which provide the best user experience and critically meet the standards laid down by GPG45. PDP's could utilise users' reusable-identities, if they have one, which meet the standard and are interoperable with their CIAM systems. If PDPs are trust marked through an appropriate trust scheme*, they could also create re-usable Identities on registration which can be used with other organisations, easing the identity verification workload for the user and the ecosystem as a whole.

d) Additionally, from an ecosystem design perspective, identity services should plug directly into PDPs which will then register consent and authorisation with the 'consent and authorisation' (C&A) server/module in order to aggregate and orchestrate those consents were a user to switch PDPs. Critically, we assume the C&A server to be under the strict governance and responsibility of MaPs.

* Affiliated to 'UK Digital Identity Trust and attribute Framework released' (Alpha released February this year).

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?**

Yes, we have a view:

a) Dashboards will often be mobile apps which can be challenging for users to trust, so requiring an appropriate level of confidence in verification and authentication is essential. For the release of pension information at least, we believe a **medium level of verification and assurance** is workable and more inclusive, helping adoption of pension dashboards and in alignment with 'Check your State Pension'.

b) However, while a medium level of verification and authentication may be appropriate for the release of pension information, we **do not** believe it is appropriate for transactions or the movement of funds. If, in future, functionality for transactions or movement of funds is provided by pensions dashboards we recommend a 'step-up' authentication to a **high level of confidence** is necessary and will be expected by users.

c) Although we believe a medium level of confidence for verification and authentication works for information access, we recognise the importance of 'Checking the identity belongs to the person who's claiming it'. Consequently, we would recommend very close attention is paid to dynamic knowledge based verification (KBV) questions and GPG45's (Score 2) guidance on this.

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?**

Feedback repeated from question 2.

Yes, we have a view:

a) Dashboards will often be mobile apps which can be challenging for users to trust, so requiring an appropriate level of confidence in verification and authentication is essential. For the release of pension information at least, we believe a **medium level of verification and assurance** is workable

and more inclusive, helping adoption of pension dashboards and in alignment with 'Check your State Pension'.

b) However, while a medium level of verification and authentication may be appropriate for the release of pension information, we **do not** believe it is appropriate for transactions or the movement of funds. If, in future, functionality for transactions or movement of funds is provided by pensions dashboards we recommend a 'step-up' authentication to a **high level of confidence** is necessary and will be expected by users.

c) Although we believe a medium level of confidence for verification and authentication works for information access, we recognise the importance of 'Checking the identity belongs to the person who's claiming it'. Consequently, we would recommend very close attention is paid to dynamic knowledge based verification (KBV) questions and GPG45's (Score 2) guidance on this).

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

a) Although there are a range of trust frameworks which also set similar levels of assurance including eIDAS and NIST it makes **NO sense** to move away from the rest of the country's focus on GPG44/45, if we are looking for an interoperable outcome for digital identities under the UK trust and attribute framework.

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?

a) PASA has no comment on this question beyond the standards set by GPG44/45

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.

Feedback repeated from question 1:

a) **No, we do not agree with the central digital identity**, if by a 'central digital identity' we mean a single identity provider. We are concerned such centralisation creates a **single point of failure, a**

single point of attack, limited capacity and a commercial monopoly which will not enable the open market required to sustain the pensions dashboard ecosystem into the future.

b) We also believe an open market approach to identity is more sustainable and commercially viable. To this end, MaPs should consider aligning with the governments UK Trust framework initiative designed to create an open identity market.

c) We suggest onboarding and identity verification should start with the pensions dashboard provider (PDP) free to adopt identity services of their choice, which provide the best user experience and critically meet the standards laid down by GPG45. PDP's could utilise users' reusable-identities, if they have one, which meet the standard and are interoperable with their CIAM systems. If PDPs are trust marked through an appropriate trust scheme, they could also create re-usable Identities on registration which can be used with other organisations, easing the identity verification workload for the user and the ecosystem as a whole.

d) Additionally, from an ecosystem design perspective, we suggest identity services could plug directly into PDPs that will then register consent and authorisation with the 'consent and authorisation' (C&A) server/module in order to aggregate and orchestrate those consents were a user to switch PDPs. Critically, we assume the C&A server to be under the strict governance and responsibility of MaPs.

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 Identity approach

Answer to a)

The programme's approach to an 'acceptable identity standard' should start with the existing standards and regulation which relate to digital identity and security. The approach should not conflate or intermingle elements borrowed from existing standards or regulation into a 'new' standard just simply quote an existing standard whether GPG44/45, ISO, NIST, or otherwise. Any further standards requirements particular to pensions dashboards, administration or the related ecosystem should be minimised and purely 'additive'. We are sure the programme recognises companies already involved or looking to join the dashboard ecosystem already run on a comprehensive portfolio of standards, regulatory compliance and are very sensitive to any changes in their liabilities. So, it will be important to optimise barriers to entry for attractiveness and security to ensure a flourishing market for pensions dashboards is achieved.

Answer to b)

Do not create another cross-industry approach or Trust scheme, **if** there is already one being developed which fits the bill for the industry (e.g. TISA scheme). If a new trust scheme specific to pensions is necessary, ensure it is closely aligned with other schemes through alignment with the UK Trust framework (already mentioned) and through cross-scheme liaison (see OIX's proposed cross scheme WG).

Additionally:

Please also note we have a number of other questions relating to Identity and data protection we would like the Programme to answer before being able to give approval. We have added these at the end of our response.

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?

Fraud is mentioned just once in the 'Identity Approach: call for input': item 35 'check if the claimed identity is at high risk of identity fraud'. However, background fraud checks must be integrated at **multiple points in the customer journey** and, where feasible, during the movement of data throughout the ecosystem (pension-finder and data provider/ISP included). Given individuals substantial wealth is at risk, fraud checks should be carried out at both the proofing stage and at the authentication stage with possible additional risk monitoring besides particularly when funds or transactions come into play.

Additionally, the ecosystem could 'fall-down' if the underlying data processors and controllers are unable to successfully match the identity request to an internal record. To this end we believe the degree of assertion to each data item needs revisiting. We would push back on the proposal the NI Number is only asserted by the end user and not checked at any point as part of the verification. NI Numbers are a vital part of the data which data processors will use to match.

Finally, some form of recognisable and verifiable certification (e.g. Identity scheme trust mark), would help with the adoption of trust marks.

Further questions from PASA :

1. Who will be the data controller of the dashboard and the special personal data? Where and with whom will individuals exercise their rights?
2. In addition, this is likely to result in automated decision making and profiling – who will be responsible for the DPIA and related security controls?

3. We would need to understand spans of controls and who owns which liabilities at specific points of the data flow map.
4. The identity checks performed to provide a medium level of assurance are not guarantees. As Data Processors who aren't in charge of the security aspects, we would also want to know (alongside the Data Controllers) who would be responsible if a data breach occurred as a direct result of a dashboard data exchange where the identity had passed the central security check?
5. If secondary dashboard legislation compels Data Controllers to provide data to dashboards, but the controller in question does not consider GPG 44/5 Medium safe enough and so refuses, where does this lead us? Which legislation wins out? Compulsion or GDPR?
6. Will there be continued engagement during the Data Protection Impact Assessment process? Publication of the results would also aid demonstration of compliance with DP regulations.

PASA

assess | aspire | achieve

Get in touch:

info@pasa-uk.com

www.pasa-uk.com

PASA is a Community Interest Company and our full name is Pensions Administration Standards Association CIC.

Company number: 6597097