OPEN IDENTITY EXCHANGE
White Paper

Digital ID for Pensions Dashboard

OIX White Paper

Version: ***Final***

Date: ***21/06/2017***

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

1.1 Introduction and Background

Following the OIX UK Alpha Project[1] 'Creating a Pensions Dashboard', completed in May 2016, a further OIX UK project was initiated in October 2016 to implement a private sector Verify Identity Hub for integration with GOV.UK Verify Identity Providers and to consider the Department of Work and Pensions (DWP) requirements for attribute exchange of State Pension data with the private sector.

In late December 2016 some of the contributors to this OIX project were also chosen as Development Partners[2] for 'The Pensions Dashboard Prototype' project being led by The Association of British Insurers (ABI) on behalf of Her Majesty's Treasury (HMT) and 17 companies from the Pensions Industry[3]. The HMT/ABI prototype project was a separate and independent project that provided this OIX project with a key dependency.

This OIX project had a focus on testing the following hypothesis:

"To test how digital identities, which have been certified against government standards, can be used to release attributes from public and private sector sources. For this project we will be using pensions data where the user and their consent is at the heart of the process".

This project had two key objectives:

1. To **design and prove** the integration between a Pensions Dashboard architecture and a private sector Verify Identity Hub and Identity Providers with a focus on the practical aspects of implementation and aligning with Government Digital Services (GDS) standards for GOV.UK Verify.

2. To **design** an approach for integration between a Pensions Dashboard architecture and the DWP for attribute exchange of State Pension data.

This project worked with indicative requirements, supplied by the DWP, for access to State Pension Data. Two requirements that had a major influence on this project were:

1. Consumer and delegate digital identities are verified to a Level of Assurance 2 (LoA2)[4].

[1] http://oixuk.org/wp-content/uploads/2016/09/Creating-a-Pensions-Dashboard_Whitepaper_May-2016.pdf
[2] https://www.abi.org.uk/News/News-releases/2016/12/Pensions-Dashboard-project-announces-FinTech-pioneers
[3] https://www.gov.uk/government/speeches/launching-the-pensions-dashboard-city-ministers-speech
[4] The standards of LoA2 and Good Practice Guides (GPG44 and GPG45) that assure Identity Verification processes are implemented by all GOV.UK Verify Identity Providers

2. The consumer must have control over the consent to access and share their State Pension data with Pensions Dashboards and Delegates (e.g. Financial Advisers).

Increased control over consent to access or share personal data is a topic that has both influential backing and European Union (EU) regulatory drivers. In March 2017 Sir Tim Berners-Lee published an open letter on the World Wide Web Consortium (W3C) web site[5] in which he described three topics that he believes must be tackled in order for the web to fulfill its true potential as a tool which serves all of humanity. **Number one was to regain control of personal data**.

"*The current business model for many websites offers free content in exchange for personal data. Many of us agree to this – albeit often by accepting long and confusing terms and conditions documents – but fundamentally we do not mind some information being collected in exchange for free services. But, we're missing a trick. As our data is then held in proprietary silos, out of sight to us, we lose out on the benefits we could realise if we had direct control over this data and chose when and with whom to share it. What's more, we often do not have any way of feeding back to companies what data we'd rather not share – especially with third parties – the T&Cs are all or nothing*".

The W3C open letter was published on the Web's 28th birthday and was covered by major broadcasters, newspaper publishers and web sites.

The EU General Data Protection Regulation (GDPR) reforms apply from May 2018 and this has an increased emphasis on consumer consent. "A data subject's consent to processing of their personal data must be as easy to withdraw as to give consent. Consent must be explicit for sensitive data[6]".

This OIX UK White Paper provides an update on activities that have tested the hypothesis in line with the objectives stated above:

- The practical experience and key findings of implementing a private sector Verify Identity Hub that supports GDS GOV.UK Verify standards and which is then utilised in a Pensions Dashboard architecture;

- The progress that has been made on a draft design that utilises a **User-Managed Access (UMA)[7]** approach which will meet the DWP indicative requirements and could also be applied to a Pensions Dashboard ecosystem for secure attribute exchange.

[5] http://webfoundation.org/2017/03/web-turns-28-letter/
[6] http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf
[7] https://kantarainitiative.org/confluence/display/uma/Home

UMA is an OAuth-based profile and is designed to give web users a unified control point for who and what can get access to their personal data, content, and services, wherever it lives on the web. Section 5 of this document provides more detail on UMA and the potential pros and cons of using it within a Pensions Dashboard architecture.

1.2 High Level Architecture

Figure 1 below provides a high level architecture context for this project that should be useful in understanding the key findings outlined in section 1.3.

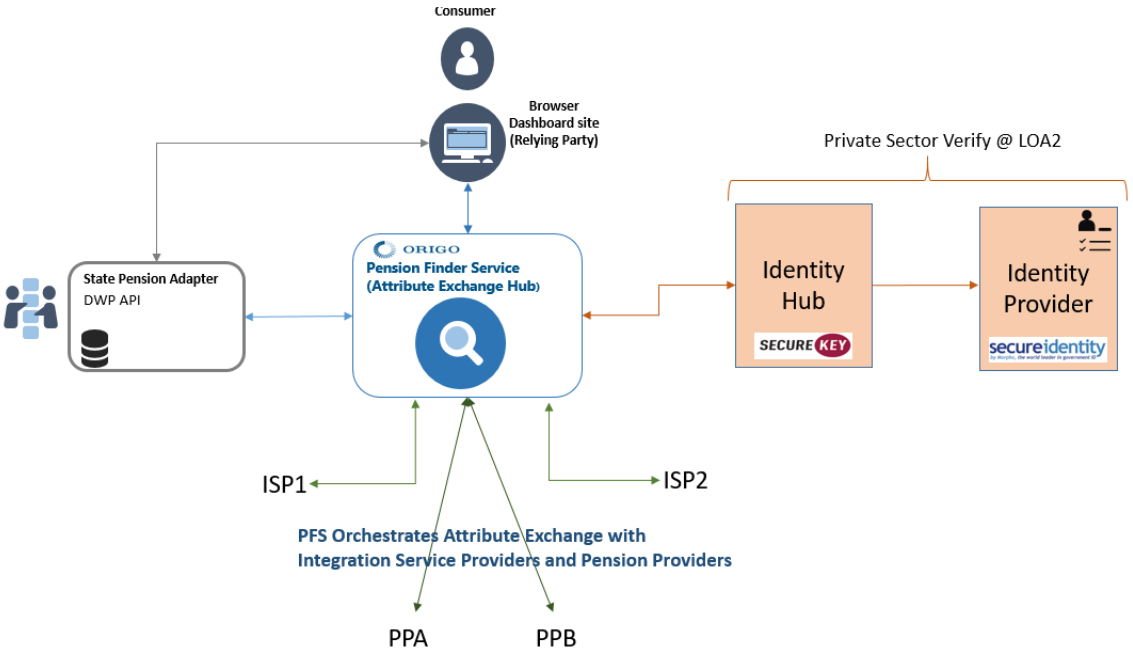

Figure 1: High Level Architecture

A **Consumer** at a Pensions **Dashboard provider (**website or mobile application) wants to view their pensions data. The **Dashboard** provider interacts with a **State Pension Adapter (SPA)** to access State Pension Data and a **Pension Finder Server (PFS)** to access (search for) pensions across all UK private Pension Providers.

The SPA and the PFS interact with a private sector Verify **Identity Hub** to seek authentication of the consumer Identity at a federated **Identity Provider** that can assure the identity of the consumer to the required LoA (as set by industry) before searching for the consumers' pensions data.

For private pensions the PFS orchestrates searches with **Integration Service Providers (ISPs**) who act as technology enablers on behalf of Pension Providers or directly with **Pension Providers (PPs)** who can support direct integration.

The **Origo PFS** can be considered as analogous to (or a foundation for) a Pension Industry **Attribute Exchange Hub (AXH).** The Origo PFS has functional features that align well with those of an AXH. Appendix 1 provides a comparison between Origo PFS features and previous OIX work[8] on defining AXH features.

It is key for a vibrant digital identity and attribute ecosystem to emerge at a national level, that AXHs for various industry verticals, as well as more generic AXHs, are interoperable.

1.3 Key Findings

The two key findings are listed below:

1. ***It is technically feasible to implement a private sector Verify Identity Hub that integrates with existing GOV.UK Verify Identity Providers***. This has been implemented and demonstrated in a Pensions Dashboard context via the HMT/ABI prototype project. The current version of the Identity Hub software supports GDS Verify requirements for the private sector, with further enhancements planned for delivery in Q32017 to support public sector requirements. When these enhancements are delivered this will enable the private sector Verify Identity Hub to support business processes that require access to both private and public sector data, using the same Verify Digital Identity.

2. ***A Pensions Dashboard draft profile for an open standard based on UMA has been developed that meets the DWP indicative requirements for the release of State Pension data attributes.*** The primary focus was access to State Pension Data via a conceptual component called the State Pension Adapter (SPA). However, it is recognised that the draft UMA profile could be applied in a wider context for the release of private pensions attributes and could also be a key feature within an AXH.

1.4 Conclusions

1. This OIX UK project has been a successful pathfinder in progressing and proving the concept of a private sector Identity Hub that can comply with GOV.UK Verify standards. The concept was demonstrated via the HMT/ABI prototype project to government ministers, the press, the pensions industry and the FinTech industry.

2. The Pensions Dashboard architecture has potential to provide a large consumer user base that could increase the number of assured digital Identities that meet GDS

[8] A number of OIX white papers reference various Discovery and Alpha projects on Attribute Exchange and can be found here http://www.openidentityexchange.org/papers/

GOV.UK Verify standards. This assumes private sector Verify is the chosen direction for Digital Identity in the Pensions Dashboard architecture.

3. An UMA based approach for a target architecture meets the DWP indicative requirements and could also be applied in the wider context of the private pensions sector, although this requires more work in conjunction with a Pensions Dashboard governance body. The pros and cons of an UMA based Pensions Dashboard target architecture are outlined in section 5.3.

1.5 Recommendations

1. The current version of the private sector Verify Identity Hub software supports GDS private sector requirements. Further work is planned to fully comply with GDS Standards for public sector requirements. Estimates are that this can be achieved by Q32017. The Verify Sandbox Environment[9] provides an established GDS governance process for tracking this.

2. Further work is required to progress the potential for an UMA based approach within the concept of an AXH that could incorporate a Pension Finder Service. This requires Government and Pensions Industry co-ordination. Implementation options will need to be defined, and decided upon, with the governance function that is assumed will take forward the Pensions Dashboard architecture and standards for a 2019 implementation.

3. The DWP requirements need to be finalised and prioritised to enable a full assessment of security architecture requirements for access to the DWP for State Pension data and the options for implementing and operating the SPA service.

4. The Pensions Dashboard draft profile for UMA was developed with UMA v1.01 standards. UMA v2.0 is expected to be released in Q2 2017. Therefore it will be prudent for any future work on the Pensions Dashboard UMA profile to review it against UMA v2.0 standards.

5. This project has shown that UMA standard and DWP requirements are very well aligned today. However other standards or technical implementations may allow the same level of user control over their attributes. For DWP requirements to be future-proof and allow innovation, they should allow technical implementations following other standards as well.

[9] Verify Sandbox environment - **http://oixuk.org/wp-content/uploads/2016/12/Verify-Sandbox-Environment-Final-Dec-2016.pdf**

2 PROJECT APPROACH

The project had a focus on testing the following hypothesis:

"To test how digital identities, which have been certified against government standards, can be used to release attributes from public and private sector sources. For this project we will be using pensions data where the user and their consent is at the heart of the process".

Face-to-Face workshops and weekly conference calls were held with project contributors to align all tasks and testing activities.

The starting point for the project was to develop integration points that further developed the architecture concepts presented in the OIX Alpha project white paper of May 2016. A conceptual architecture with the integration points for this is depicted in figure 2.

2.1 Project Objectives

It was agreed that the OIX project would have two primary objectives:

1. To **design and prove** the integration between a Pensions Dashboard architecture and a private sector Verify Identity Hub and Identity Providers with a focus on the practical aspects of implementation and aligning with Government Digital Services (GDS) standards for GOV.UK Verify.

2. To **design** an approach for integration between a Pensions Dashboard architecture and the DWP for attribute exchange of State Pension data.

2.2 Project Scope

In Scope

- The scope of the OIX project has been to focus on the practical and technical challenges that are required to test the hypothesis.

Out of Scope

- Consumer research or testing of the user experience was out of scope for this project, although journeys for registration and authentication have been delivered and are demonstrable as part of what has been delivered for the HMT/ABI prototype project;

- Any in-depth considerations of governance or commercial requirements.

2.3 Project Deliverables

The OIX project focussed on the following deliverables:

1. A working Implementation of a private sector Verify Identity hub and Integration with an existing GOV.UK Verify Identity Provider. This would provide a practical assessment of what is required to be in the private sector Verify Identity Hub market, including adherence to GDS Verify standards.

2. Integration of a Pensions Dashboard architecture with a private sector Verify Identity Hub.

3. Produce an initial design option for Attribute Exchange between a private sector Pensions Dashboard architecture and the DWP, based on the DWP indicative requirements for access to State Pension data.

4. Produce an OIX white paper that summarises progress and lessons learnt.

2.4 Project Tasks

The OIX project took an approach of splitting the tasks into integration points depicted in figure 2.

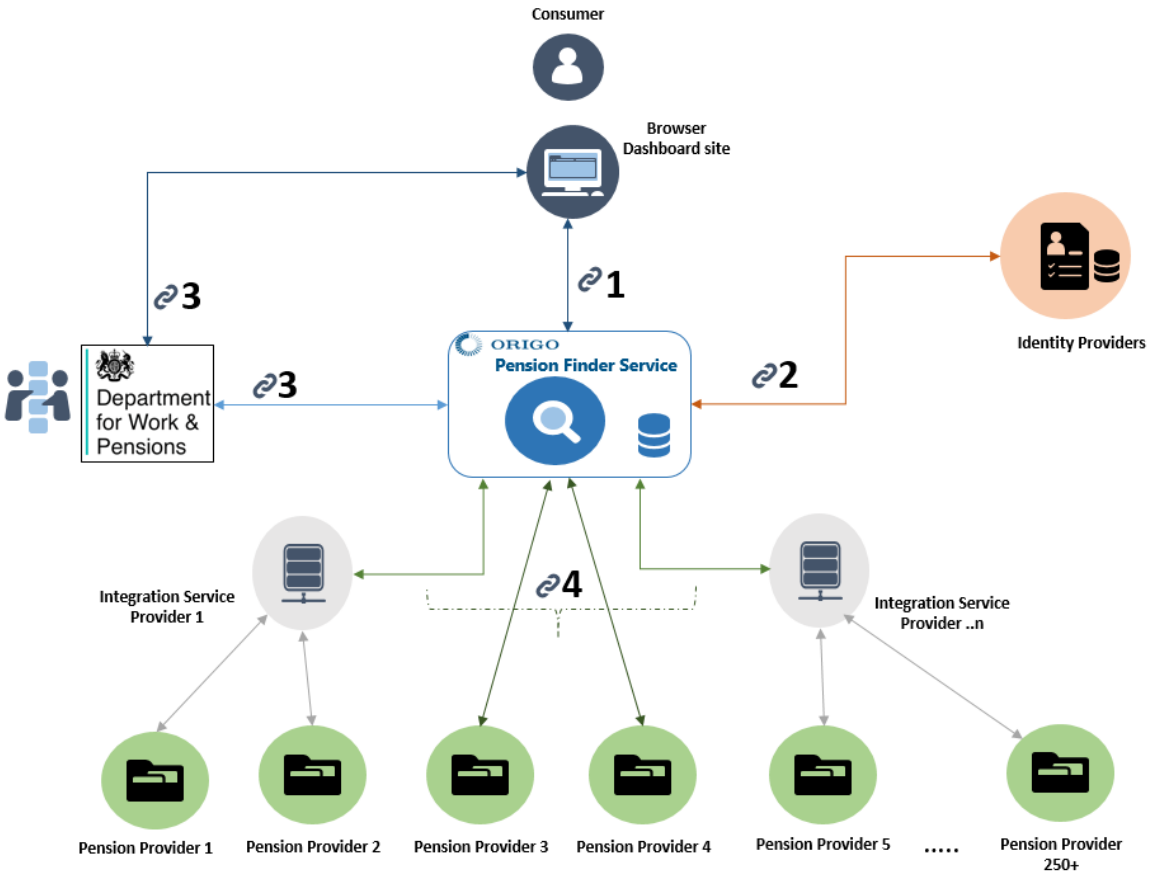

Figure 2. Pensions Dashboard conceptual architecture with Integration Points

- Integration points 1 And 2 were designed, built and tested to align with the HMT/ABI Prototype project timescales;

- Integration point 3 was tackled as a design exercise to produce a Pensions Dashboard draft profile for an open standard based on UMA that meets the DWP indicative requirements via an assumed component called the SPA;

- The OIX project also considered the potential for the UMA profile developed for integration point 3 to be applied for integration point 4. This is described in more detail in section 5 of this White Paper.

2.5 Project Contributors

The project contributors to this OIX project and their roles are listed below:

- **Government Digital Service (GDS):** Sponsor of this OIX project;
- **Department of Work and Pensions (DWP) :** Supplier of indicative DWP requirements for access to State Pension data, and key contributor to the design approach for attribute exchange;
- **Origo:** Project co-ordinator for this OIX project. Origo is the not-for-profit Fintech Company dedicated to improving connectivity between financial services companies. Origo was the supplier of a Pension Finder Service (PFS) and a Pensions Dashboard for this project;
- **ForgeRock**: Supplier of security software components that are within the Origo PFS component architecture;
- **SecureKey:** Identity and Authentication Services supplier; SecureKey provided the private sector Verify Identity Hub software;
- **Safran:** GOV.UK Verify Identity Provider (Morpho Secureidentity). Safran are a global partner with SecureKey.

2.6 Reference Inputs

The UK Government Transformation Strategy[10] published in February 2017 stated that one of its priorities is *"making better use of GOV.UK Verify by working towards 25 million users by 2020 and exploring options for delivery of identity services for businesses and intermediaries".* Not all of these new Digital identities will be at LoA2 but the consumer uptake and use of federated Identity Providers should see huge growth if the Government's strategy succeeds.

[10] https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020/government-transformation-strategy-platforms-components-and-business-capabilities

The project team also referred to previous OIX white papers on attribute exchange and the DWP personnel on this project were contributors to those previous OIX white papers. ForgeRock also supplied software to the OIX Alpha project that produced a technical design for a blue badge digital service which is detailed in an OIX white paper published in August 2015[11] .

Some recent OIX publications also have relevance to this project:

1. The OIX white paper titled 'The value of digital identity to the financial service sector' published in December 2016 explored the potential re-use of GOV.UK Verify identities for financial services and has recognised opportunities and listed some gaps that need to be plugged to enable Digital Identity re-use. The need for Attribute Exchange was one gap in particular and was stated as a key example that requires solutions and mechanisms for delivery to aid the functioning of a UK Identity ecosystem.

2. The OIX white paper titled 'Verify Sandbox Environment' published in December 2016 documents the processes and activities required for private sector Verify Federated Identity Hub providers to be listed in this environment. Safran are listed as one of the Hub providers in the Verify Sandbox.

3. Chris Ferguson, Director of National, International and Research in GDS, provided a foreword section in a January 2017 OIX white paper titled "How Digital Identities which meet Government standards could be used as part of UK Banks' customer on-boarding and KYC requirements"[12]. The foreword states that the UK Government is working with, and across, a range of private industry sectors to explore potential re-use of GOV.UK Verify certified digital identities and that the Verify Sandbox environment will provide a space to engage with the Government on operation and governance of GOV.UK Verify beyond the public sector.

[11] A technical design for a Blue Badge - http://oixuk.org/blog/2015/08/05/a-technical-design-for-a-blue-badge-digital-service/
[12] http://oixuk.org/wp-content/uploads/2017/02/How-Digital-Identities-which-meet-Government-Standards-could-be-used-as-part-of-UK-Banks%E2%80%99-Customer-On-boarding-and-KYC-Requirements.pdf

3 Architecture and build approach

The OIX project was cognisant of the HMT/ABI prototype project deadlines, its high profile, and the resulting prototype is being demonstrated to a wide Government, Pensions Industry, FinTech and media audiences through Q2 2107.

Figure 3 shows who implemented the key components of the architecture.

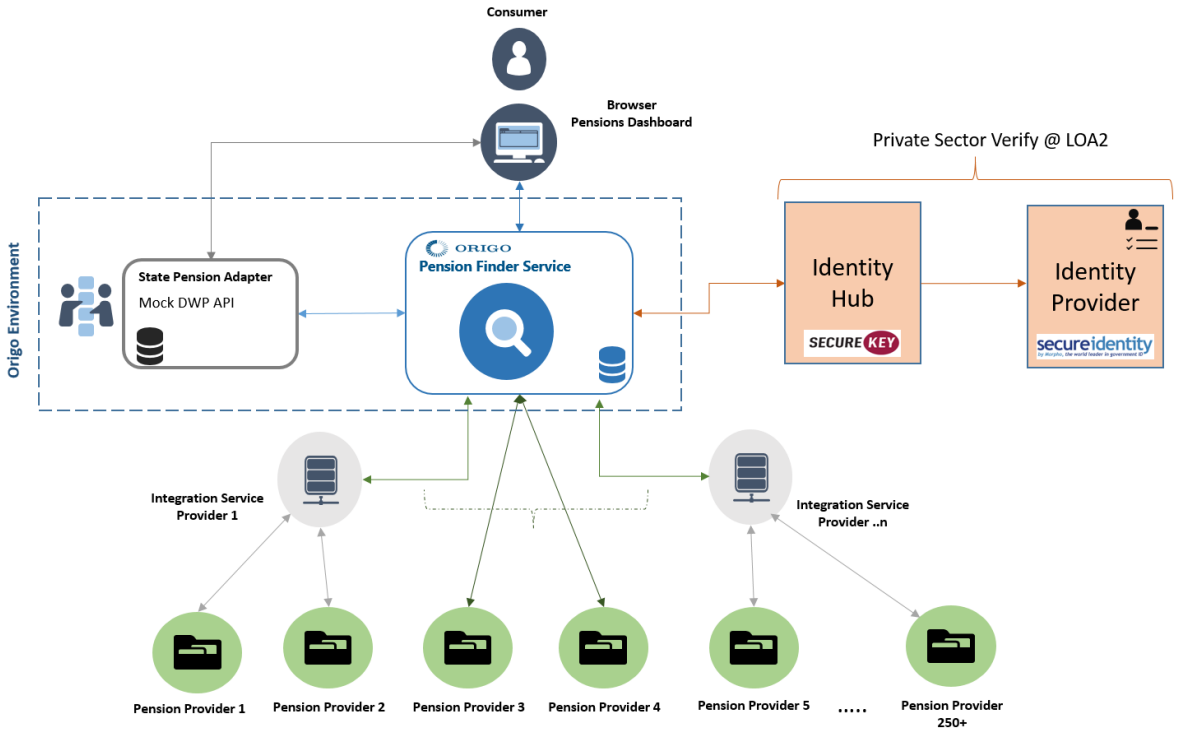

Figure 3: High Level Architecture (showing who did what)

- Origo implemented a Pensions Dashboard to test the security interactions with PFS APIs and a mock DWP API to provide State Pension data from a test database;

- Origo implemented the Pension Finder Service (PFS) which provides public facing "Find" and "Value" APIs and then orchestrates the process across all ISPs and Pension Providers. The Origo PFS includes the ForgeRock software[13] OpenIG to provide an API gateway and OpenAM to provide integration with the private sector Verify Identity Hub and a consumer consent process;

[13] https://www.forgerock.com/platform/

- The SecureKey platform, briidge.net Exchange[14], was implemented as a private sector Verify Identity Hub providing an authentication service between the Origo PFS and the Verify Identity Provider;

- In support of the Verify Trust framework, which requires the Relying Party to verify the asserted identity was supplied by a trusted Identity Provider, SecureKey developed a scheme to enable this. The public sector implementation supports a Matching Service Adapter flow and will be supported by SecureKey as an optional private sector scheme for Relying Parties;

- A test instance of the Verify Identity Provider (Secureidentity) was established by Safran. As mock data for consumers was being used for testing this had multi-factor authentication features (e.g. a mobile pin-code) switched off.

All components, apart from the Origo test dashboard, are also utilised in the HMT/ABI prototype project.

3.1 Dashboard and PFS Security Integration

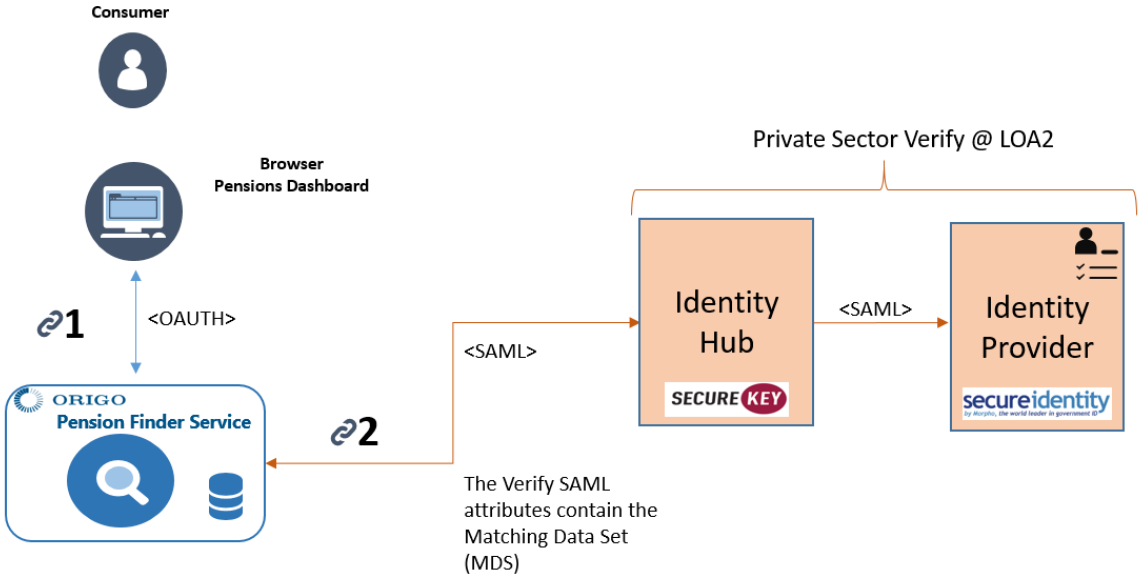

Figure 4: Integration points 1. And 2.

Figure 4 shows the open standard security protocols that were implemented for integration points 1. And 2. Once proven in the OIX project, sequence diagrams and on-boarding guides were then produced for the HMT/ABI prototype project.

[14] Briidge.Net Exchange is an existing Federated Identity Services product from SecureKey that is used in Canada for the SecureKey Concierge service. Concierge enables access to Canadian government digital services using public or private sector digital identities (e.g. bank digital identities). These identities conform to Levels of Assurance as specified in the User Authentication Guidance for IT Systems document (ITSG-31) issued under the authority of the Chief, Communications Security Establishment Canada (CSEC). See www.securekeyconcierge.com

The Origo PFS does not trust the consumer identity assertion at the dashboard. This is consistent with DWP indicative requirements and reduces the assurance effort required for dashboards. Therefore, the PFS seeks an identity assertion from the private sector Verify Identity Hub (which in turn orchestrates integration with the Verify Identity Providers).

The PFS is the Trust Anchor consuming the SAML identity assertion from the private sector Verify Identity Hub. This is done within the ForgeRock OpenAM software that forms part of the Origo PFS.

In more detail:

1. Origo issues each dashboard a client ID and secret via an onboarding registration process. The client ID and secret can last for any duration which would be defined by governance rules, and it is the responsibility of the dashboard provider to keep the secret safe. Dashboard providers must support the use of browser redirects to allow the browser to be directed to the private sector Verify Identity Hub and begin the process of consumer authentication and authorisation. For a target state architecture the OIX project has defined a dynamic client registration process as part of the Pensions Dashboard draft UMA profile.

2. Dashboards must obtain a valid access token via an OAuth2/OpenID Connect (OIDC) “authorisation code flow” to act as a client of the PFS APIs and access data on behalf of a consumer. An access token can be obtained by sending an authorisation code (which indicates the user has authenticated at the Identity Provider and given their consent for the dashboard to access their data) and the dashboard-specific client ID and secret to the PFS authorisation server. This exchange results in an OIDC response being returned to the dashboard that contains an access token and Identity claims data. The OIX project recognises that there are limitations on how identity claims can be utilised by Service Providers (such as the Origo PFS) as per GOV.UK Verify guidelines.

3.2 Consumer Journey

The flow of the consumer security journey is outlined in figures 5 through 8

1. A Dashboard requests access to protected Origo PFS APIs for “Find” and/or “Value” processes. The Origo PFS API Gateway checks for a valid access token. If a token does not exist (or is invalid) then the Origo PFS is now in the role of a SAML service provider, seeking an identity assertion which contains the LoA indicator and identity claims data i.e. the Matching Data Set (MDS). The browser is re-directed to the private sector Verify Identity Hub which is shown in figure 5.

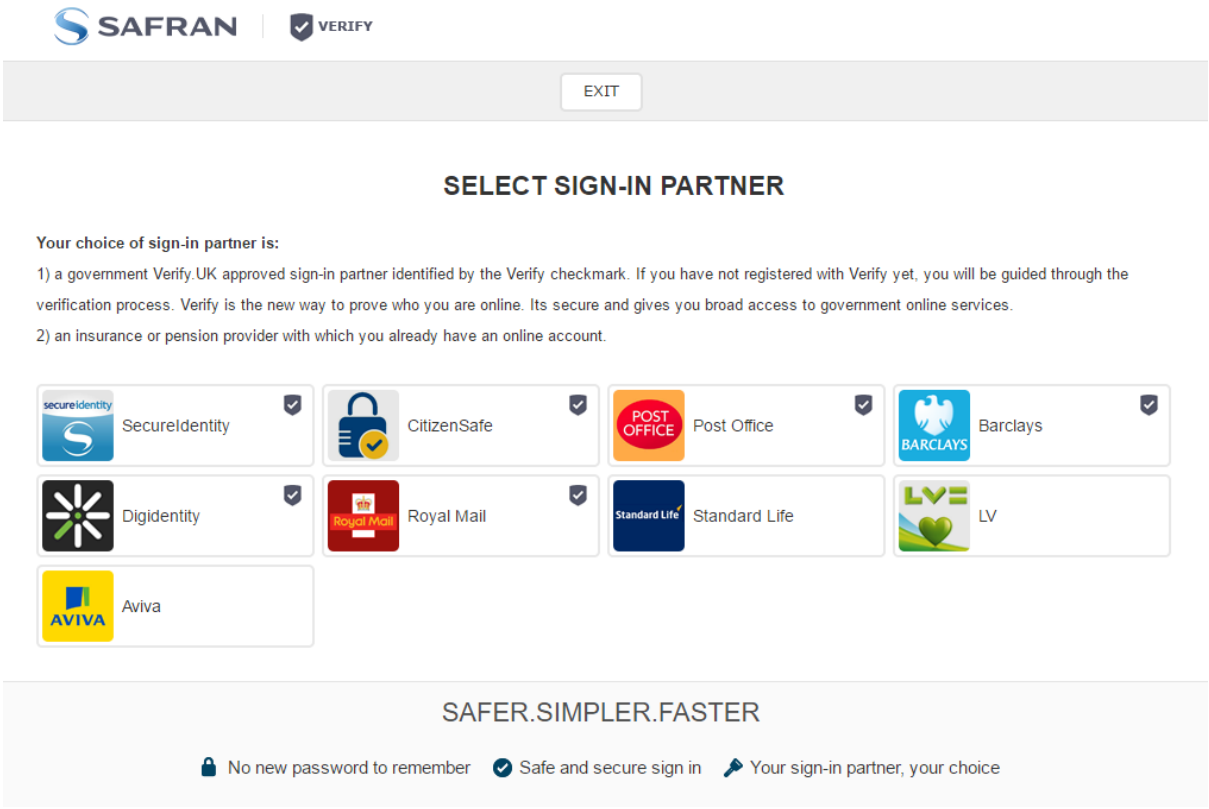

Figure 5 – Private Sector Verify Identity Hub User Interface

2. The consumer selects an Identity Provider via the private sector Verify Identity Hub user interface shown in figure 5. For this project the Identity Provider is Secureidentity.

   Standard Life, LV= and Aviva are pension companies that are not Verify Identity Providers but agreed to be shown on the Identity Hub landing page. This was to show the concept of a trust scheme that utilises major pension brand digital identities[15] as well as Verify Identity Providers.

   On selecting Secureidentity the consumer is re-directed to the Secureidentity User Interface shown in figure 6.

[15] In Canada SecureKey run the SecureKey concierge service which enables Canadian citizens to access Canadian government services with a their Bank digital identities, if the bank is part of the scheme. This project did not explore in any detail the suitability of such an approach for the Pensions Dashboard architecture. It is anticipated that this will be a topic taken forward by any governance function established for the Pensions Dashboard ecosystem.

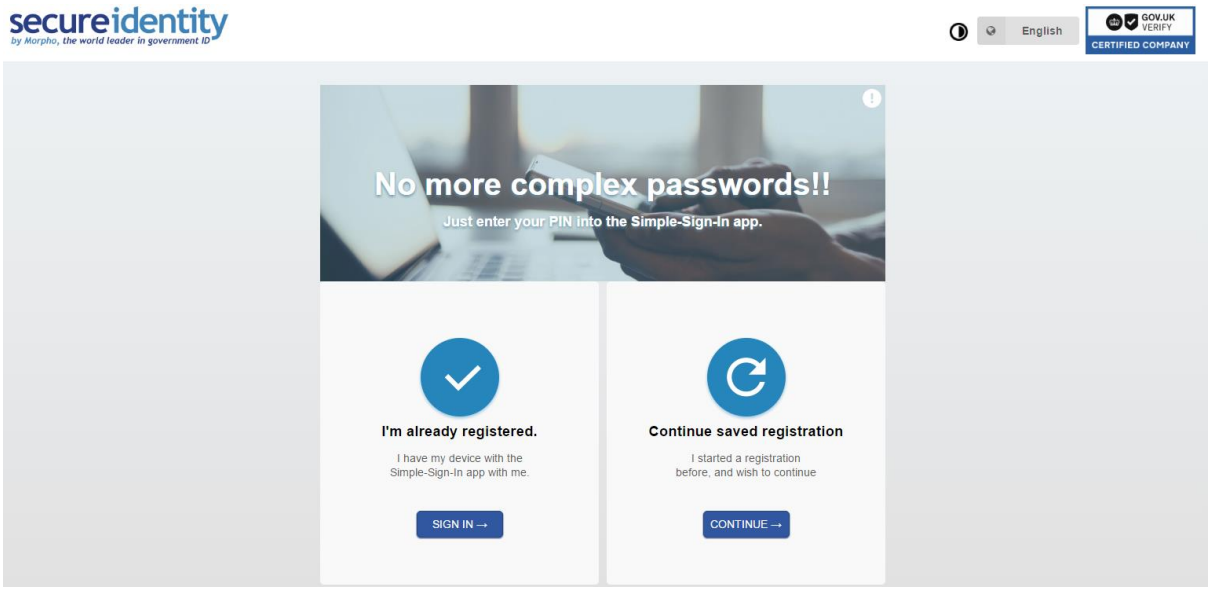

Figure 6: Secureidentity landing page

3. On selecting SIGN IN the consumer enters their authentication details (shown in figure 7).

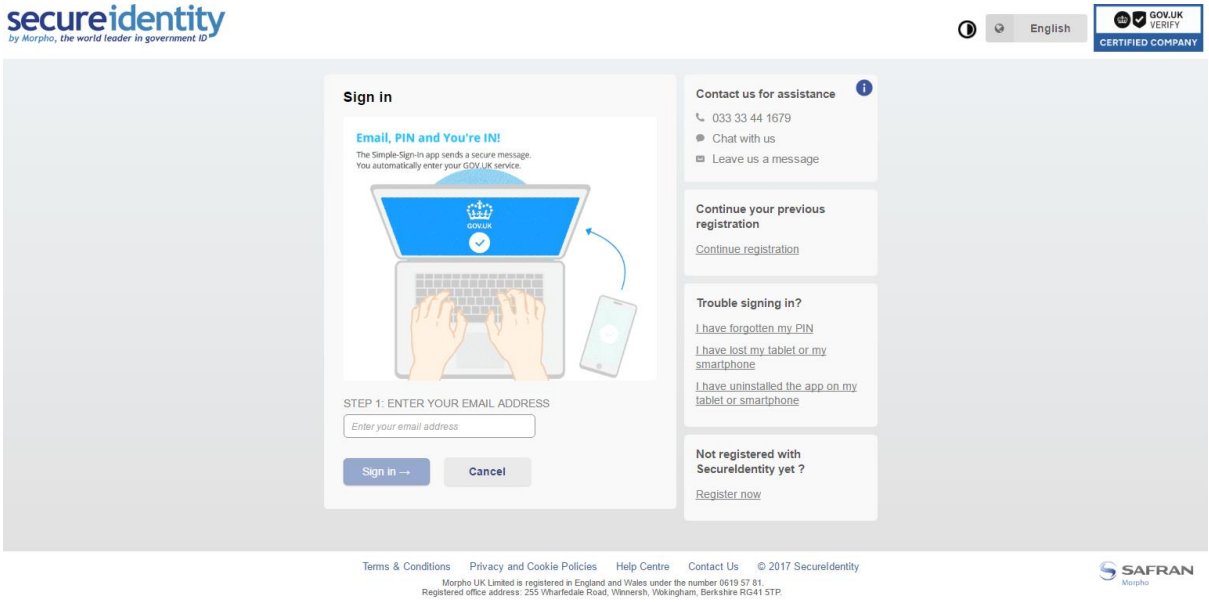

Figure 7: Secureidentity authentication screen

4. On successful authentication the consumer is re-directed back to the Origo PFS, via the private sector Verify Identity Hub, where the SAML assertion is converted to a to an OIDC/OAuth2 authorisation code and the consumer sees the consent user interface shown in figure 8.

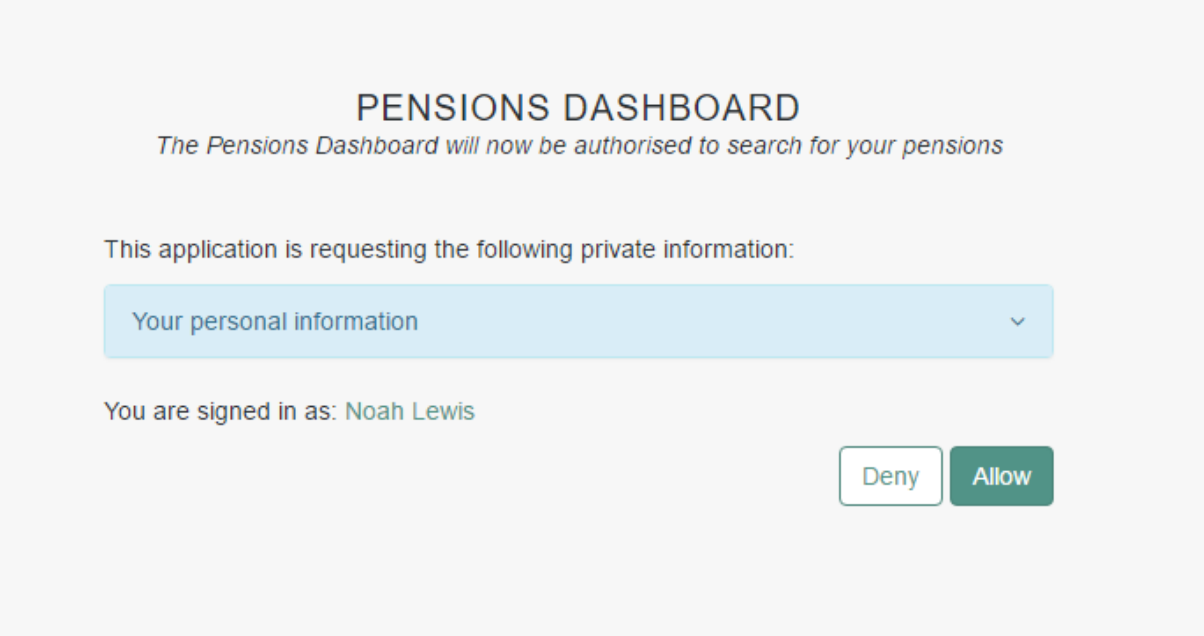

Figure 8: PFS consumer consent screen

5. If consent is granted the browser is re-directed to the dashboard which receives the authorisation code and exchanges it for an access token that can then be used to invoke the protected Origo PFS APIs.

3.3 Lessons learnt in the build phase

The build tasks for this project have proven that:

1. The Origo PFS (as an AXH) can federate consumer authentication to a private sector Verify Identity Hub that then integrates with a federated Verify Identity Provider. After consuming the identity Assertion the Origo PFS then acts as a trust anchor for subsequent Find and Value requests to Pension Providers and ISPs.

2. The use of LoA2 and enabling private sector use of Verify Identity Providers is technically feasible for use within the Pensions Dashboard architecture ecosystem.

3. Understanding and aligning with the existing GOV.UK Verify standards were key discussion topics and took up considerable time and debate e.g.

   How do Verify standards apply in a private sector context?

   I. What expectations are there on a private sector Verify Identity Hub and how does this compare with the GDS GOV.UK Verify hub? For example, the GOV.UK Verify Hub has UI features that ask the consumer questions that help guide appropriate Identity Provider selection for registration.

II. What approach should be taken to matching cycles in a Pension Finder Service where the primary function is to orchestrate matching across ISPs and Pension Providers?

III. What digital branding should be applied to private sector Verify? No private sector Verify branding was available in this projects timescales so the user interaction flow (as shown in figures 5 to 7) still show some GOV.UK Verify branding. This will need to be developed into future releases of Safran and SecureKey products as private sector Verify branding is finalised.

4. Once Standards were understood and the software feature enhancements were made to align with the Verify standards we found that testing integration points was quick.

5. The integration with the private sector Verify Identity Hub and from the Hub to the Identity Providers uses SAML open standards, and the MDS attribute set returned as identity claims in the SAML assertion conforms to the GOV.UK Verify standards for SAML attributes[16].

6. For Public Sector, the project recognises that the identity assertion is normally consumed within the MSA component that is delivered by GDS as part of the GOV.UK Verify standards. This acts as the Trust Anchor for Government Service Providers when utilising GOV.UK Verify.

   For Private Sector, the Relying Party will have a choice of implementation for the trust framework:

   i) Use of a Matching Service Adapter (MSA), supplied by GDS. This will be part of the overall Safran private sector Verify service (based on SecureKey software) by Q32017.
   ii) Delivering Identity Provider assertion as an attribute from the private sector Verify identity Hub service. This scheme was used for the HMT/ABI prototype.

[16] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/458653/Identity_Assurance_Hub_Service_Profile_-_SAML_Attributes_v1.2a.pdf

4 DWP HIGH LEVEL REQUIREMENTS

At this stage it is worth re-stating the hypothesis that is being tested.

"To test how digital identities, which have been certified against government standards, can be used to release attributes from public and private sector sources. For this project we will be using pensions data where the user and their consent is at the heart of the process".

The DWP provided a set of indicative high level requirements for this OIX project that were also provided to the HMT/ABI prototype project. It is anticipated that definitive and detailed requirements will be produced in the next few months and that these would be jointly agreed by the Pensions Industry and the DWP.

In the DWP indicative requirements a component named the **State Pension Adapter (SPA**) is assumed to exist as separate system component which manages access to State Pension data for a consumer at a Pensions Dashboard. The SPA properties are defined as a logically separate functional component that has its own user experience for consent journeys and also has separate assurance and technical boundary. A summary of the DWP indicative requirements is listed below:

1. **Identity**: Customer and Delegate identity shall be LoA2;
2. **Presence**: The Customer shall be 'present' when an initial request for access to State Pension data is presented;
3. **Consent**: The SPA shall manage consumer consent for access to State Pension data. The consumer shall be shown a scope statement prior to giving consent (of which type of data will be shared with which specific dashboard and for how long);
4. **Matching**: The consumer will be able to provide additional claims (e.g. NINO) to assist matching in the DWP service;
5. **Authorisation:** Authorisation will be sought before access to State Pension data (see Consent above);
6. **Technical Trust:** There will be a technical trust infrastructure across the whole dashboard ecosystem;
7. **Assurance:** The DWP will receive formal assurance from an independent authority relating to those aspects of the system which relate to State Pension data and it's handling;
8. **Data Presentation:** Dashboards shall comply with a given standard for presentation of State Pension data to the consumer.

5 UMA BASED TARGET ARCHITECTURE FOR PENSIONS DASHBOARDS

This section of the OIX White Paper intentionally does not attempt to provide a detailed overview (or tutorial) on UMA. Reference material is available online and at the Kantara Initiative website. The purpose of this section of the white paper is to provide an overview of what has been produced as part of this OIX project. In particular:

- How we describe a conceptual UMA based target architecture in the context of a Pensions Dashboard ecosystem and the benefits of this approach;
- Consideration of the implications for the Pensions Industry to adopt an UMA based target architecture approach.

User-Managed Access (UMA) is an OAuth-based profile which defines how **resource owners** (typically a consumer) can control protected-resource access by **clients** (e.g. dashboard software) operated by arbitrary **requesting parties** (e.g. the consumer or an adviser acting as a delegate), where the resources (e.g. personal data) reside on any number of **resource servers**, and where a centralized **authorisation server** governs access based on resource owner policies. The UMA profile concept is depicted below in figure 9 which is taken from the Kantara Initiative website.

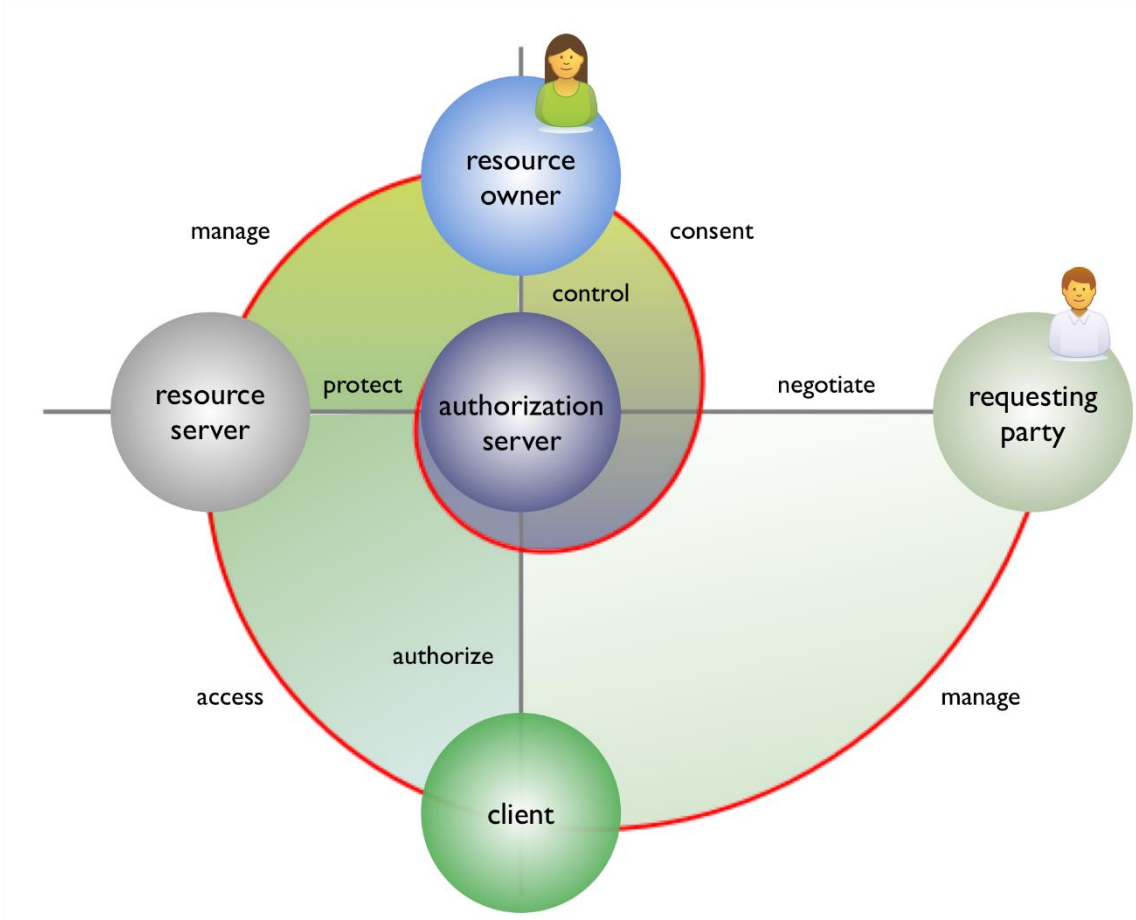

Figure 9: UMA Profile - concept and actors

UMA provides a federated authorisation architecture.

An UMA approach can also enable a centralised console (as part of an authorisation server) for consumers to manage their consent to share data, providing consumers with much greater control over who or what (e.g. advisers, multiple dashboards, IoT devices etc.) has access to their data.

5.1 Pensions Dashboard profile for UMA

The DWP has developed a Pensions Dashboard draft UMA profile. This profile is currently version labelled v0.1 and has been reviewed and refined over a series of OIX project workshops involving the DWP, GDS, Origo and ForgeRock.

An UMA based target architecture aligns well meeting the DWP indicative requirements, the pending EU GDPR reforms for consumer consent and would be a key feature of an AXH.

The profile has been developed to be specifically applicable (but not necessarily limited to) the application domain of the Pensions Dashboard. The profile has also been issued to the UMA Work Group at the Kantara Initiative for feedback and to the OIX Industry Working Group on Attribute Exchange.

5.2 Conceptual UMA based Pensions Dashboard Architecture

Figure 10 depicts a conceptual Pensions Dashboard architecture based on an assumption that both the DWP and Pensions Industry agree to adopt an UMA based approach.

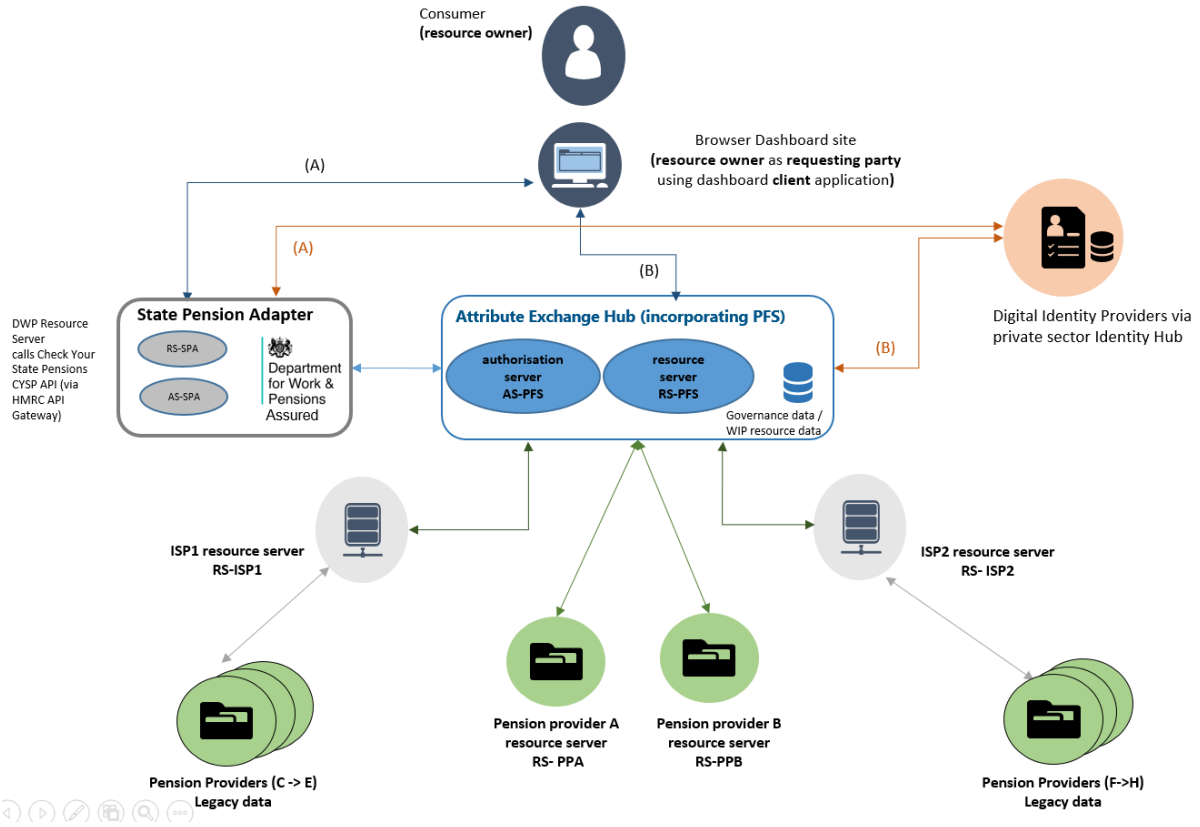

Figure 10: Conceptual UMA based target architecture for Pensions Dashboard

In this UMA based conceptual target architecture a consumers pensions data is a resource protected by a resource server. Resource servers would exist across Pensions Providers, Integration Service Provides acting on behalf of Pension Providers, the DWP, and possibly inside an AXH (see section 6 - Implementation Considerations).

A resource owner ("user") as the requesting party is the consumer using a Pensions Dashboard (client) website or application. When the dashboard makes a first time request for a State Pension resource (route A in figure 10), or to find private pensions resources via the AXH (route B in figure 10) the browser is re-directed to a federated Identity Provider, via a private sector Verify Identity Hub, for step up authentication which provides a digital identity assertion (assumed to be LoA2) to the SPA (route A) or the AXH (route B). The SPA is the Trust Anchor for access to State Pension data and the AXH is the Trust Anchor for the Private Pensions data

A consumer (resource owner) will be prompted to register the resources (data) at the authorisation server and give consent for dashboard (client) to have access to their data via a user interface portal (which could be part of the authorisation server). This allows the

consumer to set access policies on who, what and for how long their personal data resources can be accessed.

In a Pensions Dashboard context, over time, a consumer would have a view of where their data was (i.e. which resource servers) and how many clients (e.g. dashboards or financial planning tools) and requesting parties (e.g. Advisers or other trusted third parties) have access to their protected resources.

There are many UMA case studies[17] which are documented and can be found on the Kantara Initiative website.

5.3 Pros and Cons of an UMA based Pensions Dashboard Target Architecture

This analysis of pros and cons is not an exhaustive list. Instead, it is intended to provide input for assumed future work on the Pensions Dashboard ecosystem architecture;

Pros

1. Consumer consent and authorisation processes can be enabled using open standards that meet DWP indicative requirements and should be relevant to a Pensions Dashboard target architecture for 2019 implementation.

2. Supporting a RESTful API architecture will encourage Pension Providers and ISPs to consider how the data is made accessible and stored as resources that are directly invokable through APIs. This will be an area of investment for the industry that is likely to be relevant for more than just the Pensions Dashboard processes.

3. Once a pension has been found, Pensions Dashboards can design software to request new valuations directly for that pension resource at the ISP or Pension Provider (having first being authorised by an authorisation server which would be part of an AXH (including PFS capability); Arguably, there are merits in using the AXH to orchestrate all attribute exchange requests for ease of integration, centralised logging, reporting and governance features. An AXH could enable a hybrid model of UMA and non-UMA protected end-points which would enable a pragmatic approach to provisioning Pensions Dashboards.

4. Potential for a Pensions Industry Authorisation Service that puts the consumer at the heart of the consent process. This may simplify the trust and legal framework aspects of the ecosystem i.e. the consumer is explicit in their consent and this is recorded at the authorisation server. This is also revocable consent – a key element of GDPR.

[17] https://kantarainitiative.org/confluence/display/uma/Case+Studies?src=contextnavchildmode

5. There is opportunity to implement a capability that would enable an existing digital identity for a consumer at a provider customer portal (e.g. “alice” logs in to portal with existing uid/pw assumed LoA < 2) to be associated with a Verify Identity (e.g. “Alice” logs into Verify IdP at LoA 2).

   This would occur after first time step-up authentication to Verify LoA2. The association could be time configurable using security tokens. **This should be attractive to Pension Providers with existing ID&V infrastructure investments but will still drive the uptake of Verify digital identities.**

   The consumer (“alice”) at the provider customer portal would have the benefit of ‘single sign-on’ experience for subsequent uses of a pensions dashboard within the provider portal**.** This could be for a pre-determined time which would be set as a policy in the authorisation server and could also be configurable per resource server.

6. It is an objective of the Pensions Dashboard initiative to encourage millions of consumers to be more active in their engagement with pensions. This will likely result in a large increase in adviser delegation processes when the consumer seeks financial advice. These processes are not well automated at present. The draft UMA profile for the Pensions Dashboard has been designed to support delegation processes [18].

7. An UMA based approach aligns well with EU GDPR reforms that come into force in May 2018.

8. UMA is a profile of OAuth 2.0 that is complementary to OpenID Connect and will be familiar to any developer already acquainted with OAuth.

9. A process for Dynamic Registration of dashboard client software can be enabled utilising UMA\OAuth 2.0 Dynamic Registration protocol [RFC 7591][19]. This would fit well with a governance process where a dashboard client software provider requires approval from a governance body. The governance body could set the metadata values relating to the client software in a digitally signed software statement. This statement is then evaluated at the authorisation server as part of the dynamic registration request.

[18] The UMA profile assumes that components for delegate Identity will exist and can be utilised in the consent and authorisation processes.
[19] https://tools.ietf.org/html/rfc7591

Cons

1. Awareness of UMA is likely to be low across the Pensions Dashboard / FinTech ecosystem. UMA is relatively new. V1.01 of the UMA standard was produced in December 2015 and v2.0 is expected to be released in Q2 2017. However, it is a profile of OAuth 2.0 which is mature and used extensively in digital web applications.

2. At present there is a limited, but growing, range of technology suppliers who provide UMA capabilities.

3. Consumer experience of using a centralised Authorisation Service UI (portal) is limited.

4. Pension Providers (and ISPs) will be required to develop RESTful APIs that enable access to resources (also a Pro).

6 Implementation considerations

The project has considered an implementation outlook and categorised short term as technically achievable within a 2017 timeframe and medium to long term as achievable to support HMT's objectives for a 2019 implementation for the Pensions Dashboard ecosystem. No commercial or governance aspects have been factored into these considerations.

6.1 Near term outlook - achievable in 2017

From a technical perspective[20] it is entirely feasible to implement a private sector Verify Identity Hub that integrates with existing GOV.UK Verify Identity Providers and utilises LoA2. This has been established and has been successfully demonstrated in a Pensions Dashboard architecture context as part of this project.

The current version of the SecureKey briidge.net Exchange platform can support a private sector Verify compliant scheme that integrates with existing GOV.UK Verify Identity Providers and utilises LoA2. The SPA is a component that would be assured as a public sector Relying Party that uses the private sector Verify Identity Hub for federated identity services. There are additional features planned for both private sector and public sector use including an HMT/ABI solution:

- Support for matching service orchestration at the private sector Verify Identity Hub;

[20] This OIX project did not explore in any detail the governance or commercial framework for a private sector Verify Identity Hub.

- For GDS to provide and support the Matching Service Adapter (MSA) component for private and public sector (e.g. SPA) Relying Party integration;
- As part of the DWP trust framework, persistent session handling is required and would need to be supported by the private sector Verify Identity Hub provider as well as Identity Providers. This feature is currently forbidden in the GOV.UK Verify SAML 2.0 profile (as per GPG), but it is supported in the generic SAML 2.0 standards and is live in other deployments.

Safran are already listed as a private sector Verify Identity Hub service provider (utilising SecureKey software) and also as an Identity Provider in the Verify Sandbox environment[21]. The Safran Sandbox environment is planned to be fully GDS Verify Standards complaint by early Q3 2017.

A new technical specification has been proposed by GDS that, when implemented, enable support for session management at Identity Hub Services. This will enable support for re-assertion of identity claims (from an Identity Provider), and satisfy the requirements for attribute exchange services i.e. this would enable an authorisation service to seek a new identity assertion without the consumer requiring to re-enter login credentials in a set time period, unless other criteria dictated they should. Early indications are that support for persistent sessions is not a major task for Verify Identity Providers. When the session management specification is approved GDS have indicated that it will be embedded within a revised version of the Verify SAML profile specification.

From an UMA based target architecture perspective the Origo Pension Finder Service can be considered as analogous to an AXH. The Origo PFS is built on a leading Integration Platform as a Service (IPaaS) software stack and infrastructure which provides Enterprise Service Bus capability and also utilises the ForgeRock software products OpenIG and OpenAM, which have built in capability to configure and support an UMA based target approach.

A prototype for a centralised authorisation server could be built within a short period of time**.** This would enable:

- A prototype of a SPA component to be demonstrated;
- The private Pensions Industry to assess the potential for an Industry authorisation server providing advanced consumer consent features within the context of an AXH (that incorporates a Pension Finder Service).

To participate in an UMA based target architecture requires a Pensions Dashboard to be an UMA OAuth2 client. It will also require Integration Service Providers, Pension Providers and the DWP to be UMA resource servers. This will involve the creation of RESTful APIs that enable access to resources. A resource being defined as an object with a type, associated data, relationships to other resources, and a set of methods that operate on it.

[21] https://drive.google.com/file/d/0B1L-Y6JCkQeVWTlYd3ZFcWFRWlE/view

6.2 Medium to long term outlook - achievable for 2019 Pensions Dashboard launch

The medium to long term implementation outlook needs to consider in more detail the scalability and **overall** security requirements of a SPA and a potential Pensions Industry AXH.

The DWP have indicated that the assurance scope of the SPA must be as small as possible and will be separately assured physical component. If this exists outside Government infrastructure it will require to comply with security controls that can be audited to comply with ISO27001.

The pace and scale at which Pension Providers would be able to on-board to an UMA based target architecture will also require consideration e.g. A requirement could emerge to support UMA and Non-UMA resource server end-points as depicted in figure 11 with the AXH acting as a proxy (or gateway) UMA resource server for the non-UMA end-points.

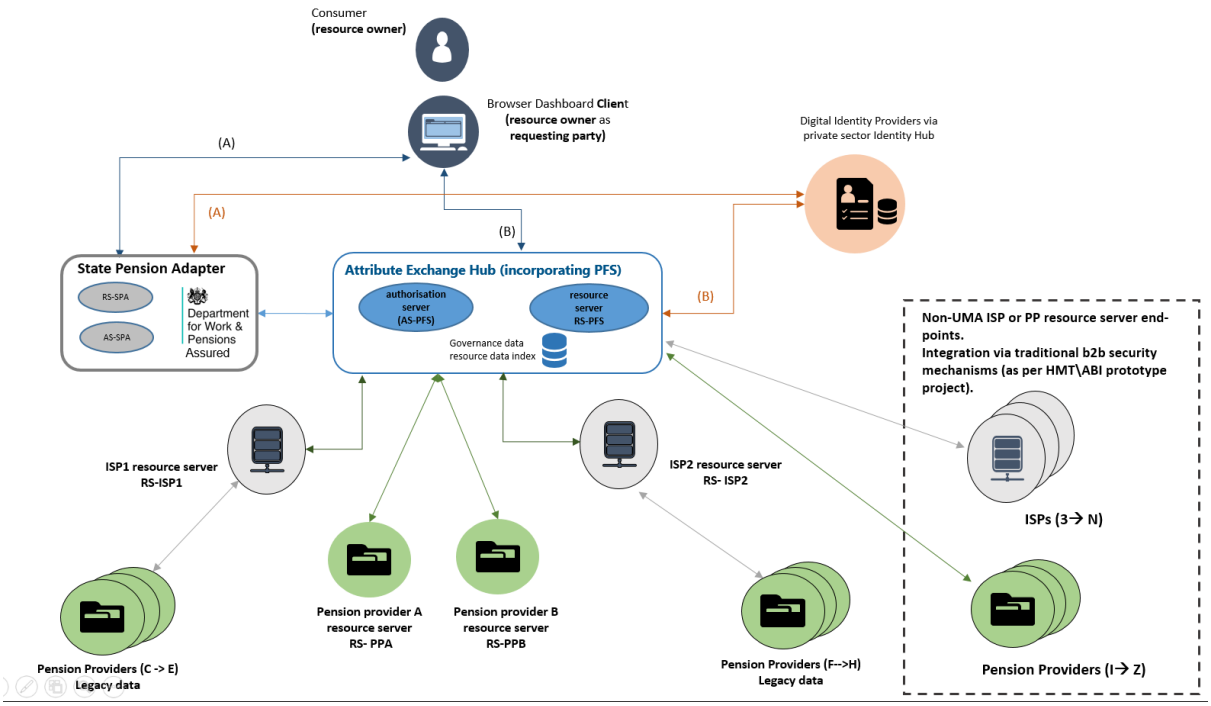

Figure 11: Supporting UMA and non-UMA end-points

7 REFERENCES

1. **OIX Pensions Dashboard Alpha White Paper** - http://oixuk.org/blog/2016/05/28/creating-a-pensions-dashboard
2. **ABI Development Partners announcement** - https://www.abi.org.uk/News/News-releases/2016/12/Pensions-Dashboard-project-announces-FinTech-pioneers
3. **HMT launching the dashboards speech** - https://www.gov.uk/government/speeches/launching-the-pensions-dashboard-city-ministers-speech
4. **OIX White Paper. The value of digital identity to the financial service sector** - http://oixuk.org/blog/2016/12/26/the-value-of-digital-identity-to-the-financial-service-sector/
5. **Can attribute provision together with identity assurance transform local government services** - http://oixuk.org/wp-content/uploads/2016/11/WCC-2-white-paper-FINAL.pdf
6. **Towards an architecture for a blue badge digital** service - http://oixuk.org/blog/2015/08/05/towards-an-architecture-for-a-digital-blue-badge-service/
7. **A Technical Design for a Blue Badge Digital service** - http://oixuk.org/blog/2015/08/05/a-technical-design-for-a-blue-badge-digital-service/
8. **The industry working group on attribute exchange** - http://oixuk.org/blog/2015/10/05/the-industry-working-group-on-attribute-exchange/
9. **Verify Sandbox environment -** http://oixuk.org/blog/2016/12/13/verify-sandbox-environment/
10. **Kantara initiative: User-Managed Access (UMA) profile of OAUTH 2.0 https://kantarainitiative.org/confluence/display/uma/Home**
11. **GOV.UK Verify SAML profile** - https://www.gov.uk/government/publications/identity-assurance-hub-service-saml-20-profile
12. **DWP Indicative High Level Requirements v0.4 Draft** – Available on request
13. **Pensions Dashboard Profile for User Managed Access v0.1 draft and associated sequence flows** – Available on request
14. **Hub Service Requirements for Reassertion of Identity to an Attribute Exchange Hub** – Available on request

8 APPENDIX 1 - Origo PFS comparison with AXH features

The Origo PFS can be considered as analogous to (or a foundation for) for an Attribute Exchange Hub (AXH). This could be aligned with the Pensions Industry which is a Community of Interest (COI) using OIX terminology.

The Origo PFS is built on a leading Integration Platform as a Service (IPaaS) software and infrastructure stack. The IPaaS provides Enterprise Service Bus capabilities that supports multiple forms of integration protocols. The Origo PFS also utilises the ForgeRock software products OpenIG and OpenAM, which have built in capability to configure and support indicative security integration requirements.

A feature comparison between the Origo PFS and those outlined by previous OIX papers on Attribute Exchange and the Industry Working Group (IWG) on Attribute Exchange is described in table 1 below:

No.	Attribute Exchange Hub Feature	Feature Description	Origo PFS Capability Alignment
1.	Attribute data dictionary	A standardised approach to defining attributes, their sources, recency (freshness) and associated levels of assurance	Not explicitly part of the Origo PFS although Origo contributed to defining the data standards and attribute definitions for the HMT/ABI Pensions Dashboard Prototype architecture. It is anticipated that attribute definitions and standards will be maintained as Open Standards by a Pensions Dashboard governance function.
2.	Dynamic and static attribute exchange	Dynamic attribute exchange is the state where the Relying Party does not know who the attribute provider is. The decision on where to source the attribute from is made within the AXH	This is a core and demonstrable capability of the Origo PFS. Onboarding of attribute provider end points is enabled by governance and configuration data and UI tools have been developed that showcase the dynamic search for attributes that is core to the Find process

No.	Attribute Exchange Hub Feature	Feature Description	Origo PFS Capability Alignment
3.	Multiple Consent	The user journey within the Relying Party digital service may need to access more than one attribute provider. To minimise interruption within the user journey flow, permission may be obtained at a single point by the Relying Party from the end-user to access all attribute providers.	This is enabled within the Origo PFS and can be enhanced to support an UMA based approach should the Pensions Dashboard ecosystem choose this for the 2019 target architecture
4.	Open Source and Software protocols	The hub should be capable of converting different protocols employed at the end points.	The Origo PFS utilises Open Source software from ForgeRock for security integration. Origo also utilise a leading IPaaS upon which the dynamic attribute exchange processes are developed. The IPaaS is capable of supporting all mainstream protocols and package integrations. UMA is an award winning Open Standard profile of OAuth and is supported by the ForgeRock technology stack.
5.	Privacy Principles	The Privacy and Consumer Advisory Group (PCAG) Identity Assurance Principles (IDAP) have been written specifically for the identity assurance ecosystem. The Industry Working Group in a September 2015 OIX paper listed some future requirements that it believes need to attached to attribute exchange	The Origo PFS can integrate with a commercial instance of a private sector Verify Identity Hub and the expectation is that this will conform to the same PCAG IDAP principles. Extending or embedding new privacy principles into the Origo PFS for Attribute Exchange can be

No.	Attribute Exchange Hub Feature	Feature Description	Origo PFS Capability Alignment
			developed as they are defined.
6.	Trust Anchor	The trust anchor is the origination point of the trusted identity of the user. The user's digital identity credentials are passed from here to the attribute provider end-point in a "tamper-proof" form.	The Origo PFS is the Service Provider (Relying Party) that seeks and consumes the Identity Assertion from the Identity Hub. This will be enhanced to comply with the Verify Standards for matching and use of the MSA component
7.	Support for Web Browser re-directs (to aid matching and permissions processes)	The Attribute Exchange Hub can request information to support matching based on the status of the match and configuration in the hub. An attribute Exchange Hub may seek permission on behalf of attribute providers. Specifically useful in a dynamic attribute exchange context.	Support for this can be enabled by the Origo PFS. It is anticipated that the approach to matching by seeking consumer asserted attributes will also be driven by enhancements to data standards. An UMA based approach does enable the concept of an industry authorisation service that provides centralised consent features that which could be beneficial for consumers and industry.
8.	IWG Additional Requirements IWG/001-008[22]	The IWG has listed 8 future requirements that it believes should be tackled that expand on the above. These suggest Privacy controls which could apply, enhanced configuration options and some commercial model considerations.	The IWG recognises that the Attribute Exchange market for hubs and attribute providers is new and will emerge. The Origo PFS is analogous to (or a foundation) example of an AXH,

[22] http://www.openidentityexchange.org/wp-content/uploads/2016/11/OIX-IWG-AX-report-Sept-2015-v0.3.pdf

No.	Attribute Exchange Hub Feature	Feature Description	Origo PFS Capability Alignment
			It is anticipated that the Origo PFS will evolve to meet the Pensions Industry requirements as they are set. The Pensions Dashboard ecosystem is a good example of a Community of Interest (COI) that will require Governance and Legal (Trust) Frameworks for Attribute Exchange.

Table 1: Origo PFS to Attribute Exchange Hub Feature Comparison

9 APPENDIX 2 – GLOSSARY

Access token

An access token contains the security credentials for a login session and identifies the user, the user's groups, the user's privileges and, in some cases, a particular application.

Application Programming Interface (API)

It is a means of accessing data based on a standard. The data accessed via an API may be closed, shared or open data.

Attribute Exchange Hub (AXH)

A technology hub that enables exchange of attributes between Relying Parties, Requesting Parties and Attribute Providers. Typically implemented on Enterprise Service Bus/Integration Platform technology stacks.

Attribute Provider

The provider of data. In the context of the Pensions Dashboard Service this will be the pension companies and trustees who supply data to the service and also the DWP for the State Pension.

Authorisation Server / Authorization Server (UMA context)

A server that protects, on a resource owner's behalf, resources managed at a resource server.

Consumer

A person with a form of UK pension entitlement who will make use of a Pensions Dashboard.

Client

An application that is capable of making requests for protected resources with the resource owner's authorisation and on the requesting party's behalf.

Dashboard Provider

The provider of a Dashboard user interface that will use the data generated from the Pensions Finder Service – typically a Financial Services or FinTech company.

Dashboard User Interface (UI)

The user interface which enables an individual to view their information.

Delegate (Delegated Authority)

A Consumer may be able to delegate authority to an adviser or other Third Party to access their Pensions Dashboard attributes that are held by the attribute provides. Authorisation

to act on behalf of another.

Digital Identity (ID) – Consumer

This digital identity of the consumer. The digital representation of an entity that's authenticated through the use of a credential.

GOV.UK Verify

The identity and verification mechanism from Government Digital Services that allows a consumer to prove their online identity for government services.

Governance Register

A pensions dashboard Trust Scheme (or Framework) will require a Governance Register of all approved participants (e.g. pension dashboard providers, pension dashboard client software providers, ISPs, Pension Providers).

Identity and Verification (ID&V)

These checks will be performed on a consumer before access would be granted to their Pensions Dashboard.

Identity Assurance

The ability for a party to determine, with some level of certainty, that an electronic credential representing an entity (human or a machine) with which it interacts to effect a transaction, can be trusted to actually belong to the entity. "In other words, proving you are who you say you are to a certain level of confidence".

Identity Claims

A claim is a statement that one subject, such as a person or organization, makes about itself or another subject. Claims are packaged into one or more tokens e.g. SAML or OIDC\OAUTH) that are issued by an issuer (e.g. Identity Provider).

Identity Provider (IDP)

Private sector organisations paid by the government to verify a user is who they say they are and assert verified data that identifies them to the Relying Party. The organisations are certified as meeting relevant industry security standards and identity assurance standards published by the Cabinet Office and CESG (the UK's national technical authority).

Integration Service Provider (ISP)

Technology enablers who can provide modern real-time access to data on or from the underlying Pension Provider administration systems.

IPaaS

Integration Platform as a Service. Technology that provides development and run-time enterprise service bus capabilities to support a large range of technical protocols and open

standards for real-time and message based integration as well as package integration components. The technology can be deployed in the cloud or in hybrid cloud / company data centre environments.

Level of Assurance (LoA)

The degree of confidence a service requires that a consumer (user) is who they say they are. LoA2 indicates that on the balance of probabilities the consumer is who they say they are and that they are a real person

Local Matching Service (LMS)

The service that matches data from the Identity Provider to the Service Providers (Relying Party) local data store in order to tie the consumers digital identity to their account (if it exists)

Matching Cycles

Matching Cycles - 0,1,2,3 refer to sequence of cycles to match an assured digital identity with a consumers account at the Relying Party (Service Provider)

Matching Data Set (MDS)

The minimum data set of name, address, date of birth and gender sent by the Identity Provider to the Relying Party matching service for the purpose of matching

Matching Service Adapter (MSA)

A software tool provided by GDS that is installed within a Service Providers security domain. The Matching Service Adapter handles SAML requests for matching queries and sends responses to the Identity Hub. The Matching Service Adapter and the local matching service together comprise the matching service.

Open Identity Exchange (OIX)

A non-profit trade organisation of market leaders from competing business sectors driving the expansion of existing online services and the adoption of new online products. Business sectors include the internet (Google, PayPal), data aggregation (Equifax, Experian) and telecommunications (AT&T, Verizon).

Pension Finder Service (PFS)

A core architecture component that deals with the aggregated Find (match) of pensions and orchestrating pension valuation requests for data required for a pensions dashboard.

Pensions Dashboard

Software Client application that provides dashboard User Interface via the web or mobile application to a consumer. Typically implemented by a Financial Services Brand, perhaps utilising a 3rd party FinTech software supplier.

Personal data

Data from which a person can be identified (as per UK Data Protection Act definition). Note: personal data can be closed, shared with specific people or organisations, or made public.

Relying Party

A software application that is reliant on identity claims

Requesting party

A natural or legal person that uses a client to seek access to a protected resource. The requesting party may or may not be the same party as the resource owner.

Resource owner

An entity capable of granting access to a protected resource, the "user" in User-Managed Access. This is typically an end-user (a natural person) but it can also be non-human entity that is treated as a person for limited legal purposes (a legal person), such as a corporation.

Resource server

A server that hosts resources on a resource owner's behalf, registers resources for protection at an authorisation server, and is capable of accepting and responding to requests for protected resources.

Private Sector Verify Identity Hub

Private sector equivalent of GOV.UK Verify Digital ID Hub. This will support features where a Government relying party service can utilise the private sector verify Hub when providing attributes to private sector service providers e.g. Pensions Dashboards.

Service Provider (Relying Party)

A supplier of services e.g. dashboard provider, attribute exchange hub, that can also act as act as a Relying Party for Authentication and Authorisation services.

State Pension

A regular payment from government that you qualify for when you reach State Pension age. The State Pension age for men and women is increasing and will reach 66 by 2020. It’s due to rise further to 67 by 2028.The amount you get depends on your National Insurance record.

State Pension Adapter

The DWP have proposed a component named the State Pension Adapter (SPA) which manages access to the access to State Pension data for a consumer at a Pensions

Dashboard. The SPA properties are defined in the DWP indicative requirements as a logically separate functional component that has its own user experience for consent journeys and also has separate assurance and technical boundary.

"The SPA shall manage consumer consent for access to State Pension Data. The consumer shall be shown a scope statement prior to giving consent (of which type of data will be shared with which specific dashboard and for how long)".

Third Party (Delegate)

An individual or organisation that acts on behalf of the Consumer. This is expected to be a financial adviser although the Pensions Dashboard Service could provide access to other Third Parties e.g. a family member where a Power of Attorney has been granted.

User (typically a consumer)

A user of (and/or account holder of) commercial products or services offered through digital channels. For the purposes of this report these will primarily relate to financial services propositions.

User-Managed Access (UMA)

UMA is an OAuth-based access management protocol standard. Version 1.0 of the standard was approved by Kantara Initiative on March 23, 2015. Version 2.0 is expected to be finalised through Q2 2017. UMA (pronounced "OOH-mah" like the given name) is designed to give a web user a unified control point for authorising who and what can get access to their online personal data (such as identity attributes), content (such as photos), and services (such as viewing and creating status updates), no matter where all those things live on the web.

Verify

The **assumed** top level brand that will be utilised for private sector instances of Identity Hubs.