OPEN IDENTITY EXCHANGE

White Paper

OIX WHITE PAPER DESCRIBING THE TISA DIGITAL IDENTITY PROJECT AND THE ASSOCIATED USER JOURNEY EMULATION

By Jim Lound,

Experian

Executive Summary

In light of the relatively high levels of friction that UK consumers encounter when acquiring new financial products and the TISA mission to improve the financial wellbeing of UK consumers, it was decided to embark on the TISA Digital ID project with a view to allowing consumers to utilise a federated identity as part of the onboarding process to attain a new product and thereby improve the user journey in terms of the time taken and the amount of friction encountered.

Background

Takes longer to open a savings account than apply and receive a pay day loan

Current processes not conducive to the digital journey

Market research suggests that citizens would be prepared to use their GOV.UK Verify identity with the financial services sector or a new digital identity brand

Conclusion that organisations would not expect their new customers to attain a GOV.UK Verify Level of Assurance 2 as part of an onboarding process, but do need them to attain an LoA appropriate to AML guidelines.

TISA Mission

To develop policy, services and infrastructure that promotes consumer's financial wellbeing and the strength of the nation.

Through this approach TISA creates an environment for UK financial services to flourish.

TISA Digital ID project

Based upon the background and TISA mission, it was decided to create a TISA Digital ID project.

A TISA Digital ID Standards group was set up to establish an appropriate level of identity assurance to satisfy the TISA members in relation to the use of a federated identity to satisfy their AML KYC obligations and to provide an appropriate level of

authentication when the customer uses their federated identity credentials to access the organisation's products & services.

In order to bring the concept to life a user journey emulation was created to show the user experience when using a Digital ID and bank account verification to open an investment account. This emulation was extended to include the additional information that might be required from a digital ID as part of developing access to a portable fact find.

The emulation was shown at the 2016 TISA Conference and at the TISA Digital ID.

TISA Digital ID emulator

The emulator is designed to demonstrate the following inherent features

1. The ability for the relying party (RP) organisation to engineer the Digital ID into their business process
2. The ability of the RP to align the level of identity assurance required with the level of risk of the associated financial product
3. The ability of the RP to pre-define the personal attributes that will be requested from the consumer
4. The consumer is re-directed from the RP to the Digital ID Hub
5. The consumer chooses which digital identity to utilise
6. The consumer authenticates to the relevant identity provider
7. The personal attributes requested by the RP are presented to the consumer
8. The consumer has the ability to include missing personal data or edit existing personal data and retain this for future use
9. Where there are multiple values for a specific data item, the user has the ability to utilise the default value or select an alternative
10. The consumer agrees to the personal attributes being returned to the RP
11. The consumer is re-directed back to the RP
12. The RP receives confirmation of the level of assurance attained and the consumer's personal attributes
13. The consumer see their personal attributes pre-populate the RP data entry fields

Two key findings from the feedback received are: -

- The RP's logo should persist throughout the user journey in order for the consumer to retain the context of what they are doing.
- Consumers prefer the consent to return personal attributes to the RP to be at a more granular level in order for individual data items to be declined and not returned where appropriate.

TISA Digital ID Standards group

This group analysed the publicly available GOV.UK Good Practice Guides which define the standards associated with the levels of assurance, LoA1, LoA2, LoA3 & LoA4.

The objective of this group was to consider the current AML KYC standards as described in the JMLSG guidance and determine how these could be aligned to the LoA2 level of assurance.

Having analysed the components of the Identity Processing & Verification process in relation to an LoA2, this was decomposed to a lower level of assurance that was judged by the group to be in line with the JMLSG guidelines.

This lower level of assurance was defined as an LoA AML, in order to follow the spirit of the GPG standards LoA1 to LoA4.

The group also identified that low risk investment savings products may require a lower LoA in relation to the LoA AML required for higher risk products.

TISA Digital ID Working Group

The Working Group considered the requirements of the TISA members in relation to the: -

1. Need for an appropriate level of identity assurance to satisfy the AML KYC requirements
2. Ability to accept an existing GOV.UK Verify identity when presented by the customer in order to assert their identity to the organisation for AML KYC purposes.
3. Need to check the Sanctions & PEP data for matches against the customer's personal details
4. Requirement to receive identity attributes as part of the assertion in order to utilise these in the onboarding process
5. Requirement to receive verified personal attributes to satisfy other AML requirements, for example, verified source of funds details e.g. verified bank sortcode and account number
6. Requirement to receive self-asserted personal attributes to satisfy other regulatory requirement, for example, the customer's self-asserted NINO. This

makes the customer more productive when required to provide personal attributes already associated with the customer's digital identity.
7. Requirement to receive current identity attributes as part of the authentication process in order to identify changes to personal data e.g. name, address

The group determined that a representation of how a Digital ID could be utilised was required in order to convey the principle to the TISA membership.

It was agreed that in the absence of a GOV.UK Verify LoA AML identity, a Financial Services Digital ID was required to satisfy those customers that did not have a GOV.UK Verify digital identity.

It should be noted that the term Financial Services Digital ID was selected as a working title for this new digital identity to be made available via the TISA members.

A proof of concept was developed that demonstrated the user journey starting at the TISA member's website, allowing the customer to: -

1. Identify an existing digital identity that they already hold i.e. a Financial Services Digital ID or an existing GOV.UK Verify identity
2. To create a new Financial Services Digital ID as part of the onboarding process with the TISA member and thereby removing the need for the customer to drop out of the TISA member's process to set one up
3. Provide a Bank Account as the source of funds for the investment. Verify the person owns that back account using commercially available bank account verification tools
4. To add additional personal attributes to the identity assertion and allow these to be utilised again in the future: a Portable Fact Find.
5. To allow additional personal attributes to be conveyed to the TISA member in association with the customer's use of an existing GOV.UK Verify digital identity
6. To allow personal attributes to be verified where appropriate
7. To allow the customer to consent to their identity and personal attributes to be presented to the TISA member as part of the assertion

The TISA Digital ID prototype was demonstrated at the 2016 TISA Annual Conference.

The next step is a live pilot using a Digital ID of an appropriate LoA, along with source of funds verification, to open an investment account.