Open Identity Exchange

Response to proposed JMLSG Guidelines Changes to Support Digital Identity as part of AMLD5

3rd April 2020

Author: Nick Mothershaw, Chief Executive
Email: nick.mothershaw@openidentityexchange.org
Mobile: 07885 618523
1. About the Open Identity Exchange

The Open Identity Exchange (OIX) is a member’s organisation whose goal is to make it easier for consumers, organisations and things to trust each other when interacting online.

OIX’s objective is to achieve an open approach that will:
- Allow individuals to use an ID they already have, with easy step-up trust establishment when required
- Provide service providers with access to millions of trusted IDs
- Allow ID issuers to become a trusted ID provider with minimal effort
- Enable users to understand where they can use their ID
- Make IDs interoperable across sectors
- Ensure security and compliance

OIX achieves this through member working groups, exploratory projects, and the production of white papers and best practise guides for identity interoperability.

In addition, OIX will shortly be publishing an online guide to the Digital ID ecosystem, accompanied by a new Directory of identity services providers, to allow those who rely on identities to understand how ID works and who can help them solve their ID needs.

OIX members include ID component solution suppliers, ID consultants, regulators and other trade bodies. Board members are: UK Government, Microsoft, Google, Barclays, Experian, Lexis Nexis, and International Airlines Group (IAG). OIX also has finance providers as members, including HSBC and RBS, and electronic evidence providers such as GB Group and Trans Union.
2. OIX Comments on the proposed changes

Having reviewed the proposed changes to the JMLSG guidelines to introduce the use of Digital ID OIX has comments that the JMLSG might want to consider in the following areas:

- Ensuring private sector Digital IDs that meet the eIDAS definition of a digital ID are acceptable, not just NOTIFIED eIDAS IDs
- Addressing the fact that a Digital ID might sometimes be established using a single strongly verified photo ID document
- Ensuring the changes for Digital ID do not overwrite existing electronic evidence capabilities leveraged by firms.

2.1 Digital ID alignment to eIDAS

The proposed updates to paragraph 5.3.52 suggest that firms should look for a Digital ID that “... is a notified identity scheme under the eIDAS Regulation4

Private sector Digital Identities that meet the eIDAS definition of a digital identity and comply with other relevant regulation and guidelines should be acceptable to firms for the purposes of Customer Due Diligence, not just NOTIFIED eIDAS IDs

The UK AMLD5 regulation states:

1. “(19) For the purposes of this regulation, information may be regarded as obtained from a reliable source which is independent of the person whose identity is being verified where—
   1. (a) it is obtained by means of an electronic identification process, including by using electronic identification means or by using a trust service (within the meanings of those terms in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23rd July 2014 on electronic identification and trust services for electronic transactions in the internal market(11));

This paragraph points to the definitions for Digital ID (electronic identification means) and Digital Signature services (Trust Services) within the EU regulation. This means that an ID that meets these definitions should be able to be used as electronic evidence for the purposes of Customer Due Diligence.

UK Government wants to create a digital identity market (para 2.279, UK Budget 2020) and it expects this marketplace to be driven by the private sector.

To enable this market to thrive and offer competitively priced services to firms, private sector digital identity suppliers should be able to demonstrate their compliance to the JMLSG guidelines without the need to be a formally-notified EU eIDAS Digital Identity schemes. So far only EU member state governments have been able to notify schemes to the eIDAS framework. In the UK the GOV UK Verify scheme is the only notified scheme. Verify is due to be replaced by the digital identity marketplace referred to above.
The UK Government is working on a Trust Framework for the UK that will allow ID suppliers to comply with best practise in digital identity provision within the UK market. This Trust Framework has not yet been completed and released.

In the absence of any UK legal definition for Digital Identities leveraging the EU regulation regarding the definition of what a digital identity is makes sense. However, this does not mean that a digital identity used in this context has to be a ‘notified’ eIDAS ID.

Private sector Digital ID suppliers should be able to show firms how they comply with:
- the eIDAS framework,
- the UK Digital Identify Framework when released,
- and the JMLSG guidelines,

so that the firm can satisfy itself that the Digital Identities these suppliers offer are fit for customer due diligence purposes.

Or, this compliance could be shown through membership of a Trust Scheme that undertakes a review of digital ID suppliers on behalf of firms. The Investment and Savings Alliance (TISA) has a Digital Identity project that is working with a number of digital identity suppliers and firms to create such a Trust Scheme.

There is no need therefore for the digital identities (or the Trust Scheme via which they are provided) to be a ‘Notified’ eIDAS scheme. This would introduce an unnecessary constraint on the marketplace.

2.2 Establishing a Digital Identity from a single document source

It is possible to establish a high trust Digital Identity using a single document, specifically a photo ID document with a built-in cryptographic chip.

Consideration should be given to the existing wording in paragraph 5.3.50 that says: “An electronic check that accesses data from a single source (e.g., a single check against the Electoral Register, or at a single point in time, is not normally enough on its own to verify identity.”

This could be expanded to clarify that, when using a Digital Identity, a single source would be acceptable provided that it is a Photo ID Document with a chip, and where the chip is read to ensure the documents authenticity, and the photo from the chip is verified to be a photo of the person applying.
2.3 Enabling the continued use of existing electronic evidence services

Today many firms use existing electronic evidence services within highly tuned digital onboarding processes to on-board as many customers within their online journey as possible.

Many of these electronic evidence services are provided by OIX members such as Experian, Lexis Nexis, Trans Union and GB Group.

Several of the proposed changes to the guidelines to introduce digital identity remove, probably unintentionally, some key paragraphs and phrases that these existing electronic evidence services rely upon:

- The change of the term ‘authentication’ to ‘assurance’ in paragraphs 5.3.47 and 5.3.84: the term authentication refers to the scoring mechanisms (e.g. 0-100) used by some electronic evidence providers. Levels of Assurance for digital identities tend to be classifications (e.g Low, Medium, High) rather than scores, so this may cause some confusion.

- The introduction of sentence “and capable of providing an appropriate level of assurance that the person claiming a particular identity is in fact that person” in paragraph 5.3.52: electronic evidence providers may not always provide a Level of Assurance.

- The removal of the bullet point in 5.2.52 referring to credit reference agencies and other accredited or certified bodies: this, combined with the introduction of bullets on digital identity and trust services, has the effect of removing the existing electronic evidence suppliers from the list of features a firm should be considering in their section of a supplier.

- The removal of the sentence “what checks were carried out, what the results of these checks were, and what they mean in terms of”: this evidence storage and provision on demand is a key feature of many of the electronic evidence services provided today.

- The removal of the term electronic sources from paragraph 5.2.82 this, combined with the terms digital identity and trust services, has the effect of removing the existing electronic evidence suppliers from the list of features a firm should be considering in their section of a supplier.