innovate identity™
experts in id

OIX OPEN IDENTITY EXCHANGE
White Paper

EXECUTIVE SUMMARY:
Exploring Interoperability between GPG45 and JMLSG Guidance

May 2019

INTRODUCTION

It remains frustratingly difficult for customers to prove who they are digitally. Despite the growth of the digital economy, the rapid increase in the number of online transactions and services, and 4 million public sector digital identities having now been created, examples of private sector digital identity solutions in the UK remain lacking. They are niche, they lack interoperability and portability, and are far from accessible for many people.

A number of initiatives have tried to catalyse digital identity use by the private sector, yet the guidance that exists for digital identity on the one hand, and anti-money laundering guidance on the other, remain elusively disconnected.

Until now there has been a lack of definitive research to assess interoperability between Good Practice Guide 45 (GPG45) and the Joint Money Laundering Steering Group (JMLSG) Guidance Notes. This paper answers the need for a conclusive view and looks beyond the immediate future to the factors that may shape a truly interoperable digital identity market in the UK.

REPORT AIMS

1. Assess interoperability between GPG45 and JMLSG Guidance Notes
2. Review the 5th Money Laundering Directive (5MLD) and the digital identity impacts
3. Consider the evolutionary paths of GPG45 and the JMLSG Guidance and influencing factors
4. Create an interoperability map or framework
5. Identify where factors such as guidance and standards may need to be adapted
6. Present a balanced discussion between the evolution of the JMLSG Guidance and GPG45.

WHY ARE GPG45 AND THE JMLSG GUIDANCE NOTES IMPORTANT?

GPG45 on 'Identity Proofing and Verification of an Individual' (v4.0) is guidance produced by the Government Digital Service (GDS) which provides a framework to enable digital identities to be created and shared in a consistent way.

The JMLSG has a range of trade association and industry bodies amongst its membership across a range of regulated sectors. The JMLSG Guidance Notes provide guidance to firms within these sectors how to identify an individual and meet their anti-money laundering obligations. The JMLSG Guidance Notes provide a degree of legal protection, if firms can show that they have followed processes in line with the guidance.

The importance of this research is to connect these two sets of guidance; they have their origins in very different places, and are aimed at very different audiences. But ultimately they both try to successfully establish a person's identity, to a degree of confidence that matches the risks faced by the firm doing business, the relying party.

If the two regimes can be made interoperable this would create a trusted framework to allow digital identities (produced in line with GPG45) to be consumed by regulated firms in line with their obligations. This could give a massive boost for the digital identity market, and provide a method to improve customer onboarding while reducing identity fraud risk.

THE DIGITAL IDENTITY CHALLENGE

The challenge of establishing an individual's identity online has been solved in some countries by developing re-usable digital identity schemes. This is a way to use identity evidence to establish who a person is, digitally, and to check that evidence by carrying out a variety of checks. A person could then be provided with a digital identity that can be:

a) **Trusted** to a level of confidence that is sufficient to satisfy the risk faced by the relying party, and their regulatory obligations.
b) **Re-used**, removing unnecessary friction for the customer, and lowering costs for relying parties.
c) **Federated**, to enable the individual to use their digital identity with a wide range of different organisations, not just one.

THE POTENTIAL VALUE OF DIGITAL IDENTITY

There is a significant body of work examining the potential benefits of expanding the use of digital identities for customers, businesses and the wider economy:

- **Efficient online onboarding**
- **Reduced KYC costs**
- **Reduced financial crime and fraud**
- **Adding value to the digital economy**
- **Improving efficiency**
- **Financial access and inclusion**
- **Enhanced customer experience**

Interoperability is one key to unlocking a market that extends across a range of regulated activities, and across a variety of sectors. Standards are fundamental to interoperability:

- **They enable a common language to be developed amongst identity providers and relying parties.**
- **They enable common definition, categorisation and communication of identity data, which can then be shared and understood in a consistent way across organisations.**
- **They underpin clarity and certainty in the use of digital identities by relying parties – recognised standards underpin regulatory and legal clarity and allow common Levels of Identity or Identity Profiles to be established.**
- **They provide a framework across which trust, governance, oversight and liability regimes can be developed.**

DIGITAL IDENTITY REGULATION: NOW AND IN FUTURE

Regulation sets out the obligations that are reflected in the JMLSG Guidance, and that sets the parameters for how regulated firms identify their customers.

The UK Money Laundering Regulations specify a number of conditions for the use of identity data collected or checked by another organisation, which will be important for shaping how digital identity schemes may be constructed in future. This includes issues such as the need for identity data to be recorded, stored, and made accessible to relying parties if required.

5MLD, if introduced to the UK, would introduce a number of compelling changes to the existing regulation that could significantly help the emergence of an interoperable market.

5MLD AND ITS IMPACT ON DIGITAL IDENTITY

Changes that may be introduced by 5MLD would provide regulatory clarity and greater certainty for potential relying parties when using digital identities:

- Clear and unambiguous support for the use of digital identities to identify customers, with very specific regulatory status given to eIDAS-notified digital identity schemes, or other schemes recognised by the relevant national authority.
- An opportunity to consider the impact of how the current UK legislation interprets the rules on transferring liability; the impact of the regulation is currently unclear, and potentially something that would restrict the use of digital identity.
- The introduction of new UK Money Laundering Regulations would trigger a review and update of the JMLSG Guidance, providing an opportunity to consider acting on a number of the recommendations of this report.

5MLD is not *critical* for digital identity but may provide a catalyst for a digital identity market to emerge.

GAP ANALYSIS: TERMINLOGY AND DEFINITIONS

There is a clear divergence between the language used in JMLSG Guidance Notes and GPG45. This alone makes interoperability more complex; mis-alignment of terminology and definitions creates uncertainty for the end users of both sets of guidance.

While the main report begins to develop an aligned glossary, *it is recommended that a fundamental review of shared terminology takes place to reach a consisten lexicon.*

- As a guiding principle terms more grounded in the digital identity world should be used or cross-referred to in JMLSG Guidance – definitions for terms such as 'validation' and 'identity evidence'.
- Terms more rooted in the language of AML and regulated CDD should in turn be used or cross-referenced in GPG45 – definitions for terms such as 'trusted and independent' sources of information.

GAP ANALYSIS: INTEROPERABILITY ASSESSMENT

Assessing interoperability across two differently structured frameworks provided a number of challenges. GPG45 is based on a specific and detailed scoring methodology, a series of pre-determined and 'risk-balanced' Identity Profiles, and a set of four pre-determined Identity Levels ranging through Low to Very High levels of confidence.

JMLSG Guidance sets out a pure risk-based due diligence methodology, with a less detailed hierarchy of identity evidence types and checking processes than GPG45. To consider any given mix of identity evidence and checks is in the gift of the relying party, balanced on a case-by-case basis to the level of risk associated with the customer and the task in hand.

As such, the research methodology focused on both a granular analysis, examining the equivalence of the detailed stipulations and building blocks of identity in each set of guidance, and a holistic analysis that considers the risk-balanced Identity Profiles in GPG45.

INSIGHTS

- The scoring methodology and criteria in GPG45 are more highly developed than in JMLSG Guidance, and a number of potential benefits if cross-referred to by JMLSG.
- The research also identified a number of mis-alignments in terms of the type, number and relative strengths of the evidence and processes set out in some Identity Profiles in GPG45 compared to the JMLSG Guidance.
- The retention of knowledge-based checking processes in GPG45 and the JMLSG Guidance was questioned, although its use has been recently re-calibrated in GPG45.
- The provision of details to the relying party regarding the specific Identity Profile used, and even the underlying data concerning the creation of the digital identity, may be critical to developing trust the emerging market.
- GPG45 could provide a framework within which specific additional or higher strength pieces of identity evidence or checks could be included to inform a '*step-up'* in an Identity Level or Profile, and the level of confidence attributed to it.

SUMMARY OF KEY FINDINGS

- **The GPG45 scoring framework facilitates a basis for interoperability, but without further amendment to eithet GPG45 or JMLSG guidance the level of interoperability could be limited.**
- **5MLD provides clarity around the use of eIDAS-notified digital identiy schemes.**
- **Language and definitions around shared concepts should be better aligned.**
- **The continued use of knowledge-based processes could be problematic.**
- **Many of the findings are dependent on the Government's Document Checking Service being extended to the private sector. This would enable the GPG45 process to be utilised to its full extent for private sector digital identities.**

RECOMMENDATIONS

1. For **the Government and industry** to establish GPG45 scoring framework as a basis for private sector digital identity schemes.
2. For **the Government** to enable digital identity schemes used in the private sector to utilise the Document Checking Service.
3. For **the Government** to implement 5MLD in line with the EU text and consider the impact of the UK's interpretation of liability rules.
4. For **the relevant National Authority/s (Govt, FCA and Supervisory Bodies)** to recognise suitable schemes in line with 5MLD.
5. For **Industry Groups** to research sectoral CDD needs and the case for additional Identity Profiles and Levels to be recognised.
6. For **JMLSG and GDS** to align the language and definitions used for shared concepts.
7. For **JMLSG** to consider cross-referring to, or adopting, the more detailed evidence weighting and criteria, and the scoring framework presented in GPG45.
8. For **industry and regulators** to ensure that knowledge-based verification processes are high-quality and dynamic.

FUTURE VIEW: FURTHER ISSUES TO CONSIDER

JMLSG Guidance and firms' CDD obligations impact on a wide range of activities, involving a number of regulators, supervisory bodies and trade associations. Ensuring that an interoperability framework between GPG5 and JMLSG guidance can apply across multiple sectors is a vital consideration. The input to the research received from the wider Peer Review Group of cross-industry representatives was therefore critical, and from this the research drew a number of insights.

Developing a system that proportionately matches the identity risks faced by a range of industries may require a more differentiated digital identity output than the four levels of confidence able to be derived from GPG45 Identity Levels Low to Very High.

The Peer Review Group's considerations of what a 'good' future market in digital identity would look like also helped to shape a range of scenarios that were used to examine future issues requiring further consideration.

FUTURE CONSIDERATIONS

- **Consider recognising additional digital Identity Levels or Profiles in addition to GPG45 levels of confidence** – while this must be balanced against the risk of additional complexity or cost, this would allow identities with a more proportionate level of confidence to be used, with benefits including inclusion, and increasing of size of the market addressable by digital identity.
- **Consider standalone use of the GPG45 scoring framework** – the scoring methodology provides a highly flexible framework for interoperability.
- **Consider step-ups, and how to ensure mobility between Identity Levels or schemes** – to have a means to elevate the level of confidence associated with an identity requires clarity on re-usable step-ups for customers, providers and relying parties.
- **Consider standardising trusted events** – while not in-scope for GPG45 at present, establishing a common framework to enable 'trusted events' to be identified, described, recorded and shared is an area for further development.

FINAL CONCLUSIONS

This report's recommendations could ensure that interoperability between GPG45 and JMLSG Guidance is made complete, and would remove many residual points of friction and uncertainty. 5MLD will be a big help if implemented fully, and the report presents a detailed analysis of the issues that can shape interoperability in the future digital identity market.

Ultimately, there is nothing that currently provides an absolute barrier to interoperability.

However, taking action on the recommendations and further issues raised by this research could provide further momentum to the emerging market and result in a more complete interoperability framework. This can ensure the future digital identity market will maximise the benefits to all parties concerned – to identity providers, to relying parties, and to regulators and the Government, but most of all to individual persons.