



# Exploring Interoperability between GPG45 and JMLSG Guidance

May 2019

## PROJECT PARTICIPANTS

The Open Identity Exchange (OIX) is a non-profit, technology agnostic, collaborative cross sector membership organisation with the purpose of accelerating the adoption of digital identity services based on open standards. OIX's broad membership and independent nature have seen it develop a significant body of digital identity research, and it is a significant influencer working towards the development of a digital identity market.

### PROJECT PARTNERS

A number of OIX Board members were central to the development of this project. The breadth of project participants are from amongst the digital identity ecosystem's complex stakeholder environment, comprising government organisations, regulators, trade associations, financial service firms, identity providers, fintechs and technology firms.

OIX has amongst its membership a cross-section of the major constituents in the digital identity ecosystem in the UK, a number of whom were participants in the project:

- Government Digital Service
- Barclays
- HSBC
- Lloyds
- Post Office
- Experian
- LexisNexis Risk Solutions
- GB Group

To reflect the wider range of stakeholders with a clear interest in the project and its findings, a Peer Review Group was established, which included:

- HM Treasury
- Financial Conduct Authority
- Gambling Commission
- Information Commissioner's Office
- Building Societies Association
- Remote Gambling Association
- Association of British Insurers
- Tax Incentivised Savings Association
- FinTech Delivery Panel
- Finance and Leasing Association
- tScheme

Also invited to take part:

- UK Finance
- Open Banking Implementation Entity

## RECOMMENDATIONS

- 1. Establish GPG45 as a basis for private sector digital identity standards.** While GPG45's status is considered to be Guidance, it provides a scoring framework that could be used as the basis for recognised standards within schemes in the UK.
- 2. Extend the use of the Government's Document Checking Service to private sector digital identity schemes.** This would enhance the range of trusted validation processes available to the private sector.
- 3. Implement the 5<sup>th</sup> Money Laundering Directive (5MLD) in full, and in line with the EU text.** This also provides an opportunity to review the intended interpretation of 'Liability' vs 'Responsibility' (Article 39 ML Regs 2017).
- 4. For the relevant national authority/s to recognise standards or schemes in-line with Article 13.1 of 5MLD.** This could be GPG45 Low-Very High, or include additional Identity Levels, based on the outcome of Recommendation 5 below.
- 5. To research sectoral needs and the case for additional Identity Profiles or Identity Levels to be considered by industry representative bodies.** This analysis would inform Recommendation 4 above.
- 6. Align language and definitions for common issues and concepts – this will require close working between GDS and the JMLSG secretariat.** Where JMLSG Guidance refers to issues central to digital identity, to adopt or cross-refer to GPG45 definitions (e.g. verification, identity evidence, credentials, proofing, authentication), and for GPG45 to adopt or cross-refer to the JMLSG Guidance's definitions for established AML-related terminology (e.g. refer to 'independent and reliable' sources).
- 7. For JMLSG to consider cross-referring to, or adopting, the more detailed evidence weighting and criteria, and the scoring framework presented in GPG45.** This would greatly improve interoperability and remove ambiguity for relying parties.
- 8. Consider the future application and suitability of knowledge-based checking, and knowledge-based processes much be high quality and dynamic.** This may be particularly important when it is used as a single-factor, even within a balanced score approach.

## CONTENTS

### PAGE

1	PROJECT PARTICIPANTS
2	RECOMMENDATIONS
3	CONTENTS
4	1: INTRODUCTION: THE DIGITAL IDENTITY MARKET
11	2: REGULATORY ANALYSIS
17	<i>Part 1: Interoperability Analysis</i>
18	3: DIFFERENCES IN TERMINOLOGY AND DEFINITIONS
21	4: GAP ANALYSIS
36	5: CONCLUSIONS AND RECOMMENDATIONS
40	<i>Part 2: Developing an Interoperable Digital Identity Market</i>
41	6: TOWARDS AND INTEROPERABLE DIGITAL IDENTITY MARKET
48	7: FURTHER ISSUES TO CONSIDER
51	REFERENCES

## 1 INTRODUCTION: THE DIGITAL IDENTITY MARKET

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

### THE PROBLEM WITH DIGITAL IDENTITY

The methods we use to establish who we are have their roots in the physical world, not the digital world. Passports, drivers licences, letters from local authorities or utilities companies are all accepted forms of identity evidence we use to establish confidence in our identity with a 'relying party' (such as when opening a new bank account).

This becomes more challenging when we are not physically present; for instance when we try to establish our identity online. Many countries have begun to solve this problem by developing re-usable digital identities – a way to use evidence to establish who we are, and to use this evidence and a variety of checks to create an online identity that:

- a) Can be trusted to a level of confidence, which is sufficient to satisfy the risk faced by the relying party, or their regulatory obligations
- b) Can be re-used without the need to re-establish the identity each time
- c) Can be used by the individual to establish their identity with a number of third parties, not just one.

The digital identity challenge has begun to be addressed for the public sector. Four million re-usable digital identities have been created allowing individuals to access a range of government services via the GOV.UK Verify Identity scheme. However, at present these identities are not widely used to establish digital identities in the private sector.

**Ensuring that digital identity standards are interoperable with the rules governing how regulated firms undertake their customer due diligence will be key to developing an interoperable private sector market in digital identity, and the subject of this report.**

### THE POTENTIAL VALUE OF DIGITAL IDENTITY

Digital identities have been successfully utilised by customers and private sector organisations in a growing number of countries, and there is a significant body of work examining the potential benefits of expanding their use in the UK for customers, businesses and the wider economy. Potential benefits include:

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

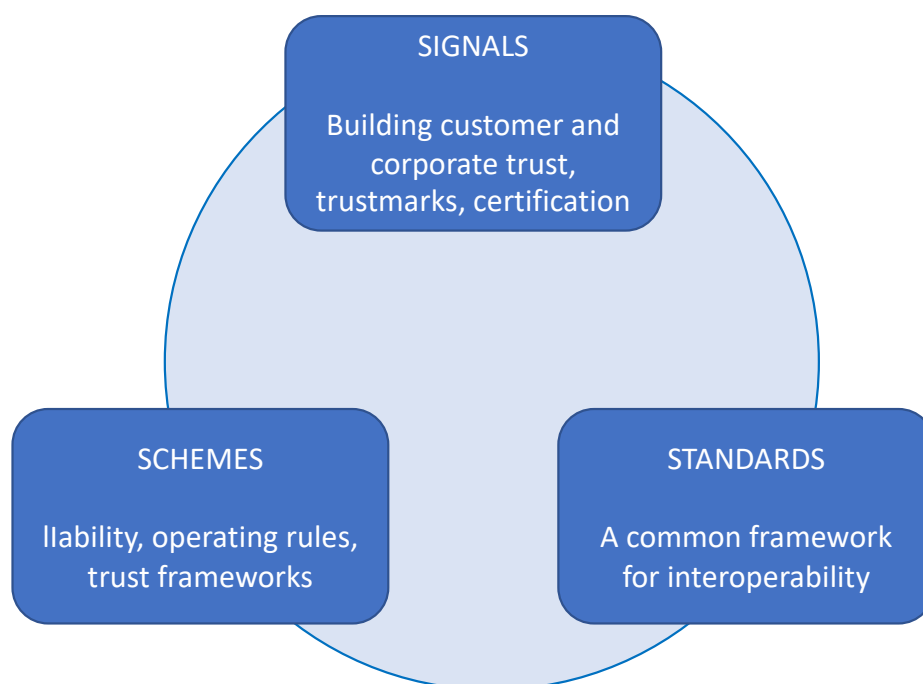
The importance of developing recognised, common standards to provide a framework for the use of digital identities in a regulated environment, and particularly across different sectors, should not be underestimated.

For example, making remote payments became much more trusted and convenient for consumers following the agreement on the relevant standards and the development of the VISA and Mastercard schemes – the same kind of clarity and ease for consumers could be provided by digital identity standards, and future schemes based upon them.

Standards are therefore 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 assurance, or Identity Profiles to be established.**
- **They provide a framework across which trust, governance, oversight and liability regimes can be developed.**

### THREE COMPONENTS FOR AN INTEROPERABLE DIGITAL IDENTITY MARKET



## **IDENTIFYING CUSTOMERS AS PART OF CUSTOMER DUE DILIGENCE**

A range of regulated industries are required by law to undertake a series of checks to identify customers, to an adequately high degree of confidence. This is a process called Customer Due Diligence (CDD), part of a process commonly referred to as Know Your Customer (KYC), which involves performing additional background checks on the customer.

Digital identities are not currently used for mainstream CDD by regulated firms in the private sector. While electronic identity and address checking are commonplace, only a few firms are utilising digital identities.

## **JMLSG GUIDANCE**

Industry guidance is produced by the Joint Money Laundering Steering Group (JMLSG) which interprets the requirements of the Money Laundering Regulations for regulated firms across a number of sectors.

The JMLSG Guidance Notes are updated in line with changing regulation and guidance elsewhere – principally the Money Laundering Regulations, and guidance produced by organisations such as the Financial Action Task Force.

The guidance itself is signed-off by both the Financial Conduct Authority (FCA) and the Treasury Minister and thereby provides a degree of legal protection for firms that operate in accordance with its requirements; for instance, a court must take account of the Guidance in determining whether a person or institution within the regulated sector has complied with the requirements of the Money Laundering Regulations.

This research considers Parts 1 and 2 of the JMLSG Guidance Notes.

## **RISK-BASED CUSTOMER DUE DILIGENCE**

Customer Due Diligence, explored in detail below, is a cornerstone of the anti-money laundering, control of terrorist financing and financial crime prevention regime. Risk-based customer due diligence has been the required basis to onboard customers for regulated firms for many years, across international money laundering regimes.<sup>ii</sup>

The function of the CDD process is to know the individual's identity, and to undertake screening and wider assessment to mitigate identity risk – in addition to other checks undertaken to assess product suitability which are not included in the scope of this research.

The higher the level of identity risk assessed by the relying party, the higher the level of assurance required to 'reasonably satisfy' the relying party that the customer is who they say they are, and that the firm can evidence how this was established.<sup>iii</sup> The degree of confidence a firm must have in a person's identity profile – the level of confidence - should be directly proportionate to the level of assessed risk on a customer-by-customer basis.<sup>iv</sup>

## DIGITAL IDENTITY STANDARDS

Public sector digital identity standards have been established via a Good Practice Guide 45: Identity Proofing and Verification of an Individual (GPG45) <sup>v</sup>, recently updated with the publication of v4.1. If the standards could be used to undertake Customer Due Diligence, then many uses could potentially be developed in the regulated private sector, particularly in Financial Services.

JMLSG Guidance already ‘allows’ digital identity and other digital data to be used in CDD, with a number of caveats. Paragraph 5.3.81 makes this clear:

*“For verification purposes, a firm may approach an electronic/digital source of its own choosing, or the potential customer may elect to offer the firm access to an electronic/digital source that he/she has already registered with, and which has already accumulated verified evidence of identity, and which meets the criteria in paragraphs 5.3.51 and 5.3.52.”<sup>vi</sup>*

This report explores to what extent GPG45 is interoperable with the detailed requirements of the anti-money laundering rules, as set out in the JMLSG Guidance Notes. And if not, what is needed to make interoperability possible?

**PROJECT HYPOTHESIS:** The UK government’s Good Practice Guide 45 Identity Proofing and Verification of an Individual, and the Joint Money Laundering Steering Group (JMLSG) Guidance Notes could be adapted and/or an interoperability framework devised to allow a digital identity, created within a scheme that is using GPG45, to be used within a financial services organisation’s customer onboarding journey, in such a way as to meet the identity verification guidance set out for CDD in the finance industry.

## LANGUAGE AND DEFINITIONS USED IN THIS REPORT

Links to the Glossaries contained in GPG45 and JMLSG Guidance are included in the References at the end of this publication.

For ease of reference, a number of definitions used in this report are set out below, to enable clarity on those used for the purposes of this research. As a general principle, the report takes definitions that flow from the Money Laundering Regulations (in particular the definition of Customer Due Diligence, Simplified Due Diligence, Enhanced Due Diligence, ‘reasonably satisfied’, ‘reliable and independent’ and ‘reliance’) from JMLSG Guidance.

For terms and definitions regarding authentication, validation, verification and assurance (and other common digital-centric terminology or processes, we have used the definitions contained in GPG45.

Where the two definitions vary (verification), we have remained cognisant of the fact, but have referred to the GPG45 definition.



A starting point is to define in more detail what we mean by re-usable, federated digital identities, and the terminology involved.

**Digital identity** is a collection of data, usually which has been verified by trusted parties, which can be used as a digital means of establishing ‘we are who we say we are’.

The level of risk associated with a false identification (the risk posed by regulatory failure, or the financial consequences of fraud, for example) will vary according to the service or product being accessed. For example, the **Identity Level** (the level of confidence in the person’s digital identity) that is required to prove that we are over 18 to purchase alcohol, may be lower than that needed to open a bank account, a much more highly regulated and financially risky type of transaction.

**Reusable** digital identities enable individuals to use their digital identity multiple times, across a range of services from different relying parties.

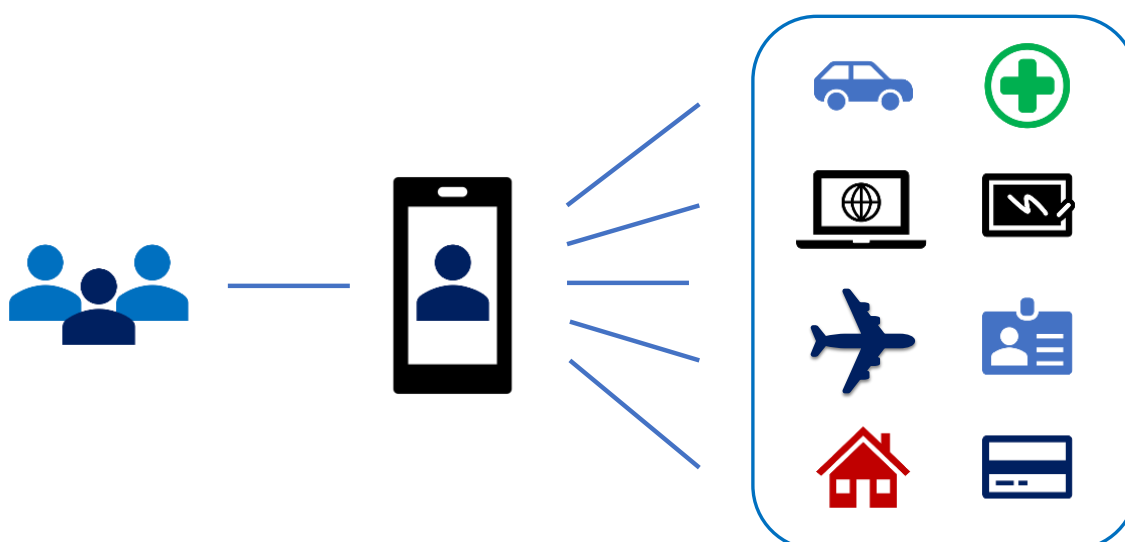
**Trusted** identities carry a degree of confidence that has been ascribed to the identity by a trusted identity provider (IDP). This usually in part reflects the degree to which identity risk has been mitigated by utilising **authoritative sources** for verifying an individual’s identity.<sup>vii</sup>

**Federated** digital identities are those where an identity scheme is recognised by a range of organisations. The digital identities created under the scheme can be used across any of the various participating organisations. This arrangement is usually supported by a trust framework and common standards to support interoperability, as well as other elements.<sup>viii</sup>

## WHAT IS A TRUSTED FEDERATED DIGITAL IDENTITY?

A digital identity that is **created** and **verified** to allow users to access services from one organisation...

... which can be **trusted** to access services from other organisations.



**Verification** is a process undertaken to check that the identity belongs to the same person who's claiming it.

The process of **Validation** is to check that the evidence is genuine or valid.

**Customer Due Diligence (CDD)** is the process whereby a regulated firm takes steps to identify their customers, and to check that they are who they say they are.

**Enhanced Due Diligence (EDD)** requires that the regulated firm takes additional checks or seeks additional evidence of the person's identity, due to the relationship being assessed to carry a higher degree of risk. Such additional checks are potentially much wider than just identity checks, however establishing identity can form an important part of undertaking EDD.

**Simplified Due Diligence (SDD)** is a process used to establish a relationship with a customer where the level of risk is assessed to be low and may therefore require a lower level of confidence in the identity, or for fewer checks to be made. Most Financial Services firms will require CDD or EDD to establish a relationship.

The evidence used to identify a customer is required to be **independent and reliable**, emphasised by money laundering regulation and guidance, including in FATF guidance on undertaking risk-based Customer Due Diligence, the Money Laundering Regulations, and industry guidance such as that provided by JMLSG.<sup>ix</sup>

**Know Your Customer (KYC)** describes the full set of checks that need to be made by a regulated organisation to establish a person's identity and gather all of the various information and undertake checks required to allow access to a product or service. CDD and its variants are part of this process, but KYC as a whole is much broader than just establishing identity.

## THE REPORT

Following an overview of current regulation and the potential future impact of the 5<sup>th</sup> Money Laundering Directive, the report is presented in two parts.

Part One presents the findings of a detailed gap analysis between JMLSG Guidance and GPG45, in terms of the alignment of language and definitions, and their interoperability when considered from both a granular and more holistic perspective. Conclusions and recommendations are drawn from this analysis (page 39, repeated at the start of the report).

Part Two looks forward towards the creation of an interoperable digital identity market, what that might look like, and identifies further challenges and opportunities to consider going forwards.

## PROJECT AIMS

### The agreed aims at the outset of the project were:

1. Review current JMLSG Guidance on CDD with respect to Private Individuals and the approach set out by the UK Government in GPG45, and identify the commonalities and variances between the requirements and industry good practice set out in the Guidance and that within GPG45.
2. Review 5MLD and consider how the inclusion of eID may impact CDD within the UK.
3. Consider the evolutionary paths of the Guidance and GPG45 and the key influencing factors (e.g. risk, standards, principles of design).
4. Create an interoperability map or framework to show how the two standards could work together and be applied to the same digital identity.
5. Identify where factors such as guidance, standards, procedures and design may need to be modified or adapted to enable convergence of the industry guidance and potential use of GPG45 in such a way that allows a customer to use a digital identity in an onboarding journey.
6. Write and publish a white paper that presents a balanced discussion between the evolution of the JMLSG Guidance and GPG45, and is respectful of privacy, security and customer convenience, yet recognises the requirements and intent of the UK Regulations.

### The intended impact of the project is to:

- Identify actions (guidance, amendments) that could establish interoperability, enabling digital identities in line with GPG45 to be used by regulated sectors, including financial services.
- Inform future digital identity standards development.
- Inform potential future amendment to JMLSG regarding digital identity use for CDD.
- Inform 5MLD implementation.

## 2 REGULATORY ANALYSIS

During the course of the research examining the potential for interoperability between GPG45 and JMLSG Guidance a number of contextual regulatory and guidance issues were considered. A range of regulatory issues impact upon the creation of digital identities, and how they may be relied upon, including guidance produced by a number of organisations. Some of the more pertinent are summarised below.

### REGULATORY ENVIRONMENT

**Money Laundering Regulations 2017 (ML Regs)** – the JMLSG Guidance Notes provide a recognised interpretation of how firms achieve compliance with the detailed requirements of the ML Regs. The ML Regs themselves were last updated in 2017, implementing the 4<sup>th</sup> Money Laundering Directive.<sup>x</sup>

In addition to the various requirements that are covered in JMLSG Guidance Notes and which were included in the gap analysis later in this report, there are two overarching elements of the current money laundering regulations that are of particular interest, those being concerning liability, and rules regarding reliance on third party CDD.

- **Liability** – the ML Regs state that liability for CDD cannot be transferred from the onboarding entity to a third party, even when the CDD undertaken by that third party has been relied upon.
  - This is transposed from the Fourth Money Laundering Directive (4MLD). However, 4MLD itself states that ‘responsibility’ (not ‘liability’) cannot be transferred.<sup>xi</sup>
  - Other EU states legally transfer (and in some cases limit) liability via digital identity scheme rules, which may not be permissible under UK ML Regs.
- **Access to electronic evidence providers’ data and process** – reliance on electronic evidence from third party providers to undertake CDD is allowed under the current regulation, but there are specific requirements. These include for the relying organisation to be able to access electronic evidence and process data immediately from providers when required.
  - Data access rights, upon demand, are a legal requirement for any digital identity solution that is relied upon by regulated firms.<sup>xii</sup>
  - The regulation does not stipulate that the underlying data has to be provided in every case, nor does it prevent that.

## GDPR AND DIGITAL IDENTITY

The General Data Protection Regulations (GDPR) impact on how a digital identity may be used. To comply with GDPR the specific purpose for an identity verification must be clearly identified, and any chosen level of verification must be appropriate to that purpose. Potential further implications of this are explored on page 34.

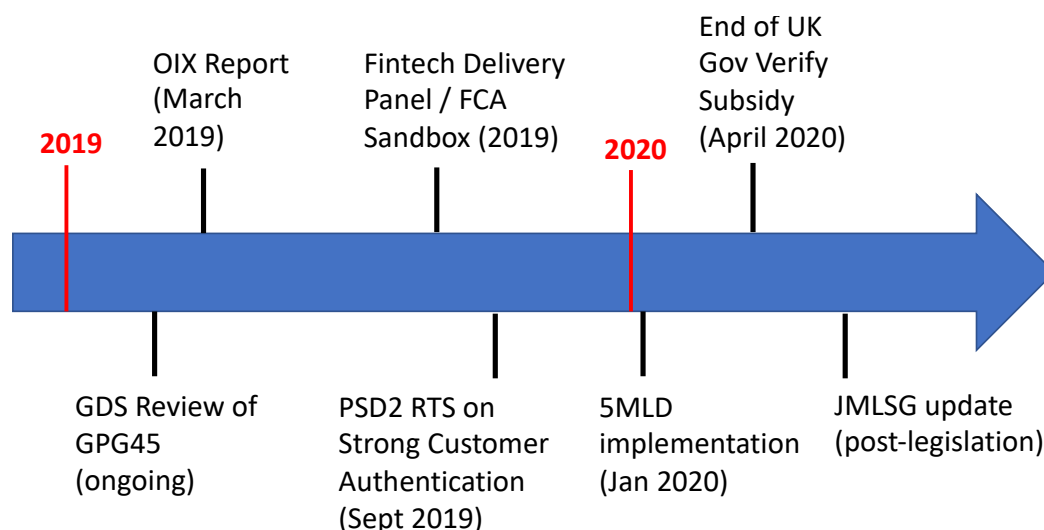
## OTHER RELEVANT GUIDANCE

JMLSG Guidance Notes are part of a range of guidance affecting regulated entities of various types, reflecting the complex regulatory environment governing relationships between customers and regulated firms. Wider regulation such as the Proceeds of Crime Act (POCA), the Payment Accounts Regulations and Payment Services Regulations, to name but a few, also impacts on other aspects of CDD and onboarding processes but are not specifically covered in this report. However, the National Cyber Security Centre (NCSC) guidance is particularly relevant.

One particular change in guidance affecting CDD is the recent update to guidance provided by the NCSC on Multi-Factor Authentication for Online Services<sup>xiii</sup>, which may have wider implications for other knowledge-based processes.

- While not directly focused on digital identity, the guidance's comments regarding the limitations and relative weakness of knowledge-based authentication, particularly when used as a single factor, will shape thinking concerning authentication and verification processes, and the application of knowledge-based checks. This is relevant to the gap analysis later in the report.
- It has implications for the future development and acceptance of digital identity guidance, as GPG45 includes Knowledge-Based checks. Version 4.0 strengthens the knowledge-based requirements and retains them for a number of the Identity Profiles.

## THE FUTURE SHAPE OF REGULATION



## 5<sup>TH</sup> MONEY LAUNDERING DIRECTIVE IMPLEMENTATION

In terms of regulation, the biggest impact will come from 5MLD. The Government's position (stated in a written answer in 2018<sup>xiv</sup>) is that 5MLD will be implemented in the UK.

Even without the provisions that 5MLD could introduce to the UK's Money Laundering Regulations, it is important to stress the ongoing value that GPG45 and the JMLSG Guidance could bring to the emerging digital identity market, and JMLSG Guidance already allows digital identity to be used for CDD, as explored below.

### AN OPPORTUNITY FOR REGULATORY CLARITY

5MLD is an opportunity to provide some further regulatory clarity for digital identity use by the regulated sector, if it is transposed in line with the agreed European Union text.

Some specific amendments 5MLD would make to the current 4MLD regime impacting on digital identity include:

- Specific recognition of digital identity as a means of undertaking CDD
  - specific recognition of eIDAS-notified schemes as a means to satisfy CDD, or
  - an opportunity for national authorities to recognise alternative digital identity processes, and for these to have formal recognition as a means to undertake CDD.
- Potential to reduce CDD risk concerning the customer not being present if a recognised digital identity process is used. The customer not being present, or where their identity has been verified electronically or via copy documents, currently triggers the need for an additional verification check to manage the risk of impersonation fraud.<sup>xv</sup>

### DIGITAL IDENTITY STANDARDS GIVEN MORE SPECIFIC RECOGNITION IN REGULATION

4MLD and the ML Regs already allow digital identity use under certain parameters, and this is already reflected in JMLSG Guidance Notes (Part 1, 5.3.81).

5MLD goes further, and specifically recognises the use of digital identities, or 'electronic IDs' ('eIDs') created in line with the eIDAS Regulations, in the Pre-amble and in Article 13.1(a) – see below. It also allows for alternative digital identity processes to be recognised or approved by the relevant national authority. Regulatory recognition would significantly improve clarity concerning digital identity use for CDD.

The 5MLD preamble states:

*“(22) Accurate identification and verification of data of natural and legal persons are essential for fighting money laundering or terrorist financing. The latest technical developments in the digitalisation of transactions and payments enable a secure remote or electronic identification. Those means of identification as set out in Regulation (EU) No*

910/2014 of the European Parliament and of the Council [in line with eIDAS Regulations]<sup>xvi</sup> should be taken into account, in particular with regard to notified electronic identification schemes and ways of ensuring cross-border legal recognition, which offer high level secure tools and provide a benchmark against which the identification methods set up at national level may be checked.<sup>xvii</sup>

Article 13.1 reinforces the new approach to accepting digital identity as a mainstream method to identify an individual, changing the definition of Customer Due Diligence.

The 4MLD Article 13.1 currently defines CDD but is unspecific regarding the recognition of any particular way of delivering this:

*“Customer due diligence measures shall comprise: a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;”*<sup>xviii</sup>

The revised Article 13.1 in 5MLD widens the CDD definition to more specifically include digital identity (alongside other trust mechanisms such as digital signatures), and recognises eIDAS-aligned schemes and provides for others to be recognised by the competent national authority:

*“Customer due diligence measures shall comprise: a) identifying the customer and verifying the customer’s identity on the basis of documents, data or information obtained from a reliable and independent source, including, where available, electronic identification means, relevant trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council or any other secure, remote or electronic identification process regulated, recognised, approved or accepted by the relevant national authorities.”*<sup>xix</sup>

## **DIGITAL IDENTITY CAN MITIGATE THE ‘CUSTOMER NOT PRESENT’ RISK FACTOR**

A customer not being physically present is currently one of a number of risk factors that prompts a relying party to consider undertaking additional identity verification checks to prevent impersonation. Under 5MLD, where an eIDAS (or otherwise recognised) eID is used, then the customer not being present is no longer a specific risk factor requiring additional checks to be applied; banks will however retain their obligations to control impersonation risks. Under 5MLD, the Annex III text is amended to enable CDD, rather than EDD, where a non-face-to-face transaction includes the use of an eIDAS or other recognised digital identity:

*“Point (c) is replaced by the following: ‘non-face-to-face business relationships or transactions, without certain safeguards, such as electronic identification means, relevant trust services as defined in Regulation (EU) No 910/2014 or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant national authorities.’”*<sup>xx</sup>

## RETAINING DIGITAL IDENTITY RECORDS AND ACCESSING THAT DATA

Article 40, paragraph 1 is amended to extend the current record keeping regime applied to third party CDD to also specifically include providers of digital identity (whether eIDAS notified schemes, relevant eIDAS trust services, or other digital identity processes in some way recognised by the relevant national authority).<sup>xxi</sup>

5MLD retain the requirement that relying parties have ‘immediate access upon demand’ to the data that was used to create and verify the customer by digital identity. This is a requirement for formal reliance on any CDD undertaken using a third party electronic evidence provider.

Article 27, paragraph 2 is replaced by the following:

*“Member States shall ensure that obliged entities to which the customer is referred take adequate steps to ensure that the third party provides immediately, upon request, relevant copies of identification and verification data, including, where available, data obtained through electronic identification means, relevant trust services as set out in Regulation (EU) No 910/2014, or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant national authorities.”<sup>xxii</sup>*

## CAN LIABILITY BE CAPPED OR TRANSFERRED?

Article 39 of the UK ML Regs reads as to require the relying party to retain all CDD liability:

*“A relevant person may rely on a person who falls within paragraph (3) (“the third party”) to apply any of the customer due diligence measures required by regulation (28(2) to (6) and (10) but, notwithstanding the relevant person’s reliance on the third party, the relevant person remains liable for any failure to apply such measures.”<sup>xxiii</sup>*

4MLD Article 25, from which this text is derived, reads in a different way, and requires that the ‘responsibility’ for CDD to be retained by the relying party:

*“Member States may permit obliged entities to rely on third parties to meet the customer due diligence requirements laid down in points (a), (b) and (c) of the first subparagraph of Article 13(1). However, the ultimate responsibility for meeting those requirements shall remain with the obliged entity which relies on the third party.”<sup>xxiv</sup>*

5MLD does not seek to amend the current Article 25. However, the current way the relevant text is transposed into UK regulation could be considered. Liability is an issue usually set out in a contract between two parties, within what is acceptable under law. Other EU states that have implemented digital identity schemes have allowed liability to be capped within the operation of certain schemes such as Norway’s BankID scheme.<sup>xxv</sup>

At present it is unclear if the UK interpretation of Article 25 (4MLD) in Article 39 (ML Regs)’ would prevent such arrangements for a private sector digital identity scheme in the UK. As such, liability is an issue that merits further consideration.



## CONSIDERATIONS FOR SUCCESSFUL 5MLD IMPLEMENTATION

Changes introduced by the revised Pre-ambble, Article 13.1(a) and Article 40 Paragraph 1 would provide a great deal of clarity and greater certainty for potential relying parties, concerning the status of digital identity as part of a CDD process, if implemented in line with the agreed EU text for 5MLD.

- Transposing these changes in line with the EU's agreed text for 5MLD would provide regulatory clarity concerning digital identity use for CDD by regulated firms, when undertaken in line with recognised processes.
- 5MLD provides specific clarity on the use of eIDAS-notified schemes, relevant eIDAS trust services, or alternatives recognised by the competent national authority to undertake CDD.
- 5MLD implementation would provide an opportunity to consider the impact of the transposition of 4MLD into Article 39 of the UK ML Regs, and to consider how this impacts on liability within schemes, and the development of the digital identity market.
- The transposition of 5MLD to the UK Statute Book would also trigger a review and update of the relevant sections of the existing JMLSG Guidance, providing an opportunity to consider acting on a number of the recommendations contained in this report.

5MLD implementation is not critical for an interoperable digital identity market to emerge in the UK – the building blocks would be provided by interoperability between GPG45 and JMLSG Guidance, and possible under existing regulation.

However, 5MLD implementation is one means to provide additional regulatory clarity for participants and facilitate an interoperable digital identity market being established in practice.

## PART 1

# Interoperability Analysis: GPG45 and JMLSG Guidance

Part 1 explores the findings of the Gap Analysis, assessing the alignment of language and definitions, and of the potential for interoperability between GPG45 v4.0 and JMLSG Guidance Notes.

### 3 DIFFERENCES IN TERMINOLOGY AND DEFINITIONS

Common definitions and terminology across guidance documents, standards and legislation is vital, particularly when seeking interoperability; for legal and operational clarity, common communication, and generating trust and common understanding, potentially across a range of organisations from different sectors.

At present, GPG45 and JMLSG Guidance each speak two subtly different languages, at least in a number of places: hardly surprising given the different development routes the two sets of guidance have taken, their intended purposes and audiences. However, while linguistic and process differences exist, their ultimate aims are not so far apart.

#### **THE CONVERGENCE OF TWO VERY DIFFERENT REGIMES, WITH A COMMON PURPOSE**

There are many commonalities between JMLSG Guidance and GPG45, even given that they have emerged along very different paths.

JMLSG guidance has been developed by the representative bodies of the financial services sector, and other sectors that the regulations cover, to interpret regulation to prevent money laundering. It reflects the language used in AML circles, much of which originates from the Money Laundering Regulations and international guidance.

GPG45 on the other hand was originally developed to create a digital identity framework for the public sector, and reflects the language and definitions used by public sector relying parties, and particularly the language of the digital identity 'ecosystem'.

As such they differ in approach, language, and the underlying processes they describe.

But ultimately both frameworks provide guidance to enable the successful identification of an individual, using robust processes, to reach a sufficiently strong level of confidence in the individual's identity.

This commonality of purpose provides a foundation for interoperability between the two regimes.

**AREAS OF DIVERGENCE: TERMINOLOGY AND DEFINITIONS**

Despite broadly shared aims, the terminology and definition used in the two sets of guidance is not aligned and diverges significantly in some important areas. Some examples are provided below.

TERMS AND DEFINITIONS	JMLSG GUIDANCE	GPG45
<b>AUTHORITATIVE vs RELIABLE AND INDEPENDENT</b>	JMLSG Guidance Notes and the broader international framework of AML guidance and regulation (FATF, 4/5MLD, UK ML Regs and JMLSG Guidance) all emphasise the need for identity evidence relied upon for CDD, and the sources against which they are checked, to be <i>'Reliable and Independent'</i> . <sup>xxvi</sup>	GPG45 instead sets out criteria for <i>'Authoritative'</i> sources (GPG45 3.1).  This may proxy for JMLSG Guidance use of the word <i>'reliable'</i> , but it is not a given that a source is <i>'independent'</i> , excepting identity fraud scores of 3 or greater (GPG45 7.3.2)
<b>IDENTIFICATION</b>	Identification: <i>"Ascertaining the name of, and other relevant information about, a customer or beneficial owner."</i> (JMLSG Guidance Notes Part 1 Glossary)	Identification is not specifically defined; Identity is.  <i>"An Identity is a combination of characteristics that identifies a person."</i> (GPG45 2.0.1)
<b>VERIFICATION</b>	<i>"Verifying the identity of a customer, by reference to documents or information obtained from a reliable source which is independent of the customer, or of a beneficial owner through carrying out reasonable measures so that the firm is satisfied that it knows who the beneficial owner is."</i> (JMLSG Guidance Notes Part 1 Glossary)	To <i>"check that the identity belongs to the person who's claiming it"</i> (GPG45 8.0)
<b>VALIDATION</b>	JMLSG Guidance does not specifically define validation as a process.  Some reference to the subject is made in Part I Guidance 5.3.78 as well as in Part II Annex:  <i>"As with all retail customers, firms should take reasonable care to check that documents offered are genuine (not obviously forged), and where these incorporate photographs, that these correspond to the presenter."</i>	A process to <i>"check the evidence is genuine or valid"</i> (GPG45 5.0)

<b>FACE-TO-FACE</b>	<p>At the last review of the JMLSG Guidance in 2017, a number of references to ‘in-person’ were changed to ‘face-to-face’.</p> <p>This has potential to allow live video interactions, and similar approaches, as having at least some equivalence to an ‘in person’ interaction. A similar approach has been taken by German regulators since 2014 to enable remote and electronic onboarding by regulated firms in line with 4MLD.<sup>xxvii</sup></p> <p>However, in JMLSG Guidance the term is not directly defined.</p>	<p>References to face-to-face in GPG45 follows the interpretation of it being an ‘in-person’ process (i.e. physically present). (e.g. GPG45 1.0.2)</p> <p>The terms are not specifically defined, however the use of both ‘in person’ and ‘face-to-face’ are used somewhat interchangeably to refer to a person being ‘present’ (e.g. GPG45 8.2.1), while other methods are described as being ‘remote’. (e.g. GPG45 8.2.2)</p>
<b>‘DOCUMENTS’ AND ‘ORIGINAL DOCUMENTS’</b>	<p>Although JMLSG Guidance acknowledges the option to undertake CDD electronically, there are many references to ‘documents’ and ‘original documents’, as compared to more specific references to ‘evidence’, ‘credentials’, and ‘documents’ in GPG45.</p>	<p>GPG45 is more consistent and specific in its language concerning credentials and sources of identity evidence, and whether this is digital data, physical documentation or both.</p>

In addition to the direct comparisons above, there remains a wide range of terminology for which there is either a lack of an equivalent term or definition. For example:

- Authentication is an important element in the eventual use of a digital identity, and is key process for carrying out financial transactions online, and yet authentication is not covered in JMLSG Guidance, and is defined in another Good Practice Guide (44).
- Other terms such as ‘credentials’, ‘identity evidence’ and ‘proofing’ may also benefit from some further definition and linkage across the two separate sets of guidance.
- *NB: This research did not consider the issue of credential binding – i.e. how certain a relying party is that it is the owner of the identity that is using the credential. JMLSG does not currently include this issue in its guidance, however given its criticality when relying on third party identity data it may be an issue worthy of JMLSG’s further consideration.*

## THE IMPORTANCE OF ALIGNING TERMS AND DEFINITIONS

The current divergence of language between JMLSG Guidance and GPG45 simply makes interoperability more complex; mis-alignment of the terminology and definitions used creates uncertainty for the end users of both sets of guidance, and uncertainty in a highly regulated space becomes a challenge.

Divergence of language does not directly prevent interoperability; however, it makes alignment or equivalency of processes less certain, and thereby may increase risk.

## 4 GAP ANALYSIS

### OVERVIEW: GPG45 (v4.1)

This research has utilised the latest v4.1 when analysing interoperability between GPG45 and JMLSG Guidance.

GPG45 demonstrates how to check a 'claimed identity' sufficient to reach a given level of confidence in the person's identity – expressed for the purposes of this report as 'Identity Levels'. GPG45 sets out a number of different elements to the overall process:

- **SCORING FRAMEWORK:** a detailed scoring framework provides a score to each identity evidence type based on its features and relative strength, and to each part of the identity checking process.
- **IDENTITY CHECKING PROCESS:** The various checks that are undertaken to build up confidence in an identity are set out in 5 different elements, and each scored individually:
  - Strength – evidence of the claimed identity.
  - Validity – checking the evidence is genuine or valid.
  - Activity – checking that the claimed identity has existed over time
  - Identity Fraud – checking if the claimed identity is at a high risk of identity fraud.
  - Verification – checking that the identity belongs to the person who is claiming it.
- **IDENTITY PROFILES:** The particular combination of scores across the 5 elements.
- **IDENTITY LEVEL:** GPG45 sets out 4 different levels of confidence, or Identity Levels, each of which can be reached by a number of different Identity Profiles, each with a different mix of evidence and checks to reach a pre-determined level of confidence. The four pre-determined Identity Levels in GPG45 are:
  - Low
  - Medium
  - High
  - Very High

It is important to note that GPG45 v4.1 (2019) has introduced a number of changes:

- Simpler, more understandable language, and using a wider range of examples
- Identity evidence is scored based on common criteria, rather than providing an exhaustive list of evidence types.
- The five parts of the Identity Checking process have been re-ordered and renamed from the previous Elements A-E.
- Greater detail is now provided regarding some of the technical processes used during the checking process, particularly with regard to checks carried out in-person.
- While some different combinations of proofs and validations were used to reach different Identity Levels in previous GPG45 v3.0 (e.g. route 3:2 vs route 2:2:2), the v4.1 Identity Profiles are far greater in number and in the breadth of combinations that can be used to reach the four identity levels.

## **COMMON LEVELS OF CONFIDENCE: IDENTITY LEVELS**

GPG45 is risk-based but outputs to four common Identity Levels. A number of different Identity Profiles, each comprised of a range of different types of evidences, checks and processes can be used to derive these four Identity Levels.

The four distinct Identity Level each expresses a consistent degree of overall confidence, and therefore mitigation of risk, for the relying party. Within each Identity Level, the range of scores used to create the identity are balanced – stronger evidence or processes in one part may be used to balance lower strength evidence or processes in other parts.

## **OVERVIEW: JMLSG GUIDANCE NOTES (Dec 2017)**

The ML Regs 2017 require banks (and other financial and regulated industries) to apply risk-based customer due diligence measures, and to take steps to prevent services from being used for money laundering and terrorist financing.

Similarly to GPG45, although in a less detailed or granular manner, JMLSG Guidance sets out categories of evidence, based on the features of the identity evidence (whether providing photo, name, address or date of birth), cross-referenced by the type of organisation that issued the credential (whether by government, a regulated entity, or other types of organisations).

It sets out ‘standard’ identification credentials, giving particular weight to documents issued by Government, and when they include photographic evidence. The list of evidence that can be considered by the regulated entity is open-ended, at the discretion and risk-assessment of the onboarding organisation.

## **RISK-BASED CDD**

JMLSG Guidance follows the requirement for a dynamic, case-by-case risk-based assessment that has long been enshrined in AML regulation and guidance, both in the UK and internationally.

This is a flexible system that requires the onboarding or relying organisation to firstly assess the risk associated with a transaction or a business relationship on a case-by-case basis. There are a very wide range of risk factors, including (but not limited to):

- The organisation’s own risk appetite.
- The status of the customer (e.g. are they considered to be a Politically Exposed Person).
- The geographic location of the customer, and whether they are physically present in undertaking the transaction.
- The nature of the product or service, and the intrinsic money laundering or financial crime risks (and identity risks) associated with it.

JMLSG Guidance requires that the identity evidence, proofing and verification checks that the regulated firm carries out a) are from 'independent and reliable sources', and b) that they collectively enable the onboarding or relying party to be 'reasonably satisfied' that the Claimed Identity is real and associated to the individual in question.

The level of confidence (and therefore identity risk mitigation) that the relying party must establish in an identity, is directly proportionate to the level of assessed risk.

JMLSG Guidance does not set out pre-determined Identity Levels in the same way as GPG45.

JMLSG Guidance provides a less detailed or specific form of scoring framework than GPG45 for identity credentials, proofing and verification.

The onboarding organisation retains its own analysis for assessing levels of risk and therefore the risk mitigation required and achieved by the Applicant. The equivalent to Identity Profiles currently used by onboarding firms under JMLSG Guidance are aligned to the level of risk, and particular to the relying party, not determined by a third party CDD provider (as would be the case under GPG45).

## **GRANULAR VS HOLISTIC ANALYSIS**

The analysis concerning interoperability between the evidence and process requirements GPG45 and JMLSG Guidance was carried out in two steps, reflecting the dynamic relying party-led analysis of risk mitigation and how this is achieved under JMLSG Guidance, with the pre-determined levels of risk mitigation presented under GPG45's balanced risk approach.

The initial analysis was carried out clause-by-clause, providing a granular but mechanistic view of the alignment and potential interoperability between the GPG45 standards and JMLSG Guidance, more in line with CDD requirements and how they are set out in JMLSG Guidance. This is focused on the mix of individual scores that make up the levels of confidence.

The findings of the granular comparative analysis are included in Section A, below.

The second layer of the gap analysis was to examine more holistically the potential for interoperability between what relying parties are required to undertake under JMLSG Guidance, with the holistic 'balanced risk assessment' set out in GPG45, expressed in the varying Identity Profiles, and ultimately in the four Identity Levels.

How the GPG45 framework with standardised outcome-focused levels of confidence interoperates with JMLSG Guidance's more granular CDD is explored in detail in Section B.

The research did not consider wider environmental aspects that would provide a backdrop to an interoperable market – whether future identity schemes can successfully mitigate residual identity risks such as impersonation, for example. These are issues that may be considered in further research on the shape of an interoperable digital identity market.



## 4 A: GRANULAR ANALYSIS

### STRENGTH - evidence of the claimed identity

- The evidence of a person's identity used to establish a digital identity under GPG45 *can* interoperate with JMLSG' Guidance's requirements to establish an individual's identity as part of the CDD process, *if* the evidence is sufficiently strong, or of the right type.
- There is misalignment in the scoring / relative weighting given to different types of evidence across GPG45 and JMLSG Guidance – specifically comparing public vs private sources:
  - JMLSG Guidance down-grades identity evidence derived from a customer's banking relationships relative to the weighting given to them by GPG45, and up-grades evidence that has been provided by Government.
  - GPG45 down-grades identity evidence provided by Government sources relative to the weighting set out in JMLSG Guidance, and more highly scores evidence that has been derived from a customer's banking relationships.
- The scoring of identity evidence in GPG45 is based on objective criteria, rather than being provided as an exhaustive list (as previously in v3.0). This establishes a more open-ended pool of evidence for identity providers and consumers to choose from, that is widely interoperable with the range of evidence that can be used under JMLSG Guidance.
  - Open criteria could assist inclusion by potentially allowing use of some non-standard evidence such as letters from officials/organisations (facilitated also by the better description of in-person identity evidence and validation).
  - Widening the evidence base, if it provides better access to digital identities, could ensure that the market addressable by digital identity is maximised.

#### Interoperability assessment:

- There is broad similarity of the evidence that can be used across GPG45 identities.
- Evidence with a score of 1 is likely to provide insufficiently strong identity evidence to be considered interoperable with CDD requirements in JMLSG, unless this element is able to be augmented by the relying party.
- Identity evidence with scores of 3 or 4 meet or exceed the standard identity evidence requirements set out in JMLSG.
- Identity evidence with a score of 2 is broadly equivalent to non-photo, non-governmental identity evidence set out in JMLSG.
- Some questions remain regarding the direct interoperability between some Identity Profiles that can be used to establish a digital identity with a Medium level of confidence, and the specific, granular requirements set out in JMLSG:
  - Some score 2 evidence is weighted more highly in GPG45 than by JMLSG.
  - The use of 'over-weighted' evidence (particularly as one component of a 2-evidence based profiles) may not be acceptable to some relying parties, based on their risk appetite.
  - Clarity to the relying party regarding the specific Identity Profile used and/or details of the evidential mix may therefore be needed.

## **VALIDITY** - checking the evidence is genuine or valid

- There is no hierarchy of validation means provided in the JMLSG Guidance equivalent to that in GPG45 – under JMLSG Guidance validation of evidence is at the risk-based discretion of the onboarding firm undertaking CDD.
- Validation of evidence by banks is undertaken by a mixture of physical checks by trained staff, checking of certain physical or cryptographic security features included in some identity documents such as e-passports, and via electronic data-based validation against records and registries held by third parties, such as credit reference agencies and accessible central and local government databases (e.g. electoral roll).

### **Interoperability assessment:**

- Validation processes with a score of 1, and Identity Profiles that include score 1 validation are unlikely to be considered interoperable with JMLSG Guidance for CDD.
- Validation processes with a score of 2 are assessed to be interoperable with JMLSG Guidance.
  - Some validation checks outlined under GPG45 5.2.1.1. are an option not currently available to banks, i.e. to validate some types of evidence by checking with the document issuer (e.g. with Passport Office, or DVLA).
  - Other score 2 options appear in line with physical document checks carried out by trained staff in-person, or by checking vs authoritative (reliable and independent) sources.
- Validation processes with a score greater than 2 meet or exceed the requirements of JMLSG Guidance and are therefore interoperable.
- Outside of direct interoperability, whether validation is carried out in an automated or manual method may have implications for whether the process is considered to be material outsourcing under current regulation.

### **ACCESS TO TRUSTED SOURCES – Document Checking Service**

The Government's Document Checking Service (DCS), used to validate documents in the creation of digital identities for public sector use, is not currently available for private sector applications.

This is not a function of GPG45, rather the rules relating to accessing the Document Checking Service itself.

**Access to the DCS for private sector digital identities would provide a significant additional validation option for regulated firms that goes beyond what is currently possible (or specifically covered by JMLSG Guidance).**

## **ACTIVITY HISTORY** - checking that the claimed identity has existed over time

- JMLSG Guidance does not directly specify any activity history checks that firms must undertake. However, with regard to the criteria the guidance sets out under which an electronic identity verification can be utilised, it does include the following (broad) specification:
  - *“It (the provider) uses a range of multiple, positive information sources, including other activity history where appropriate, that can be called upon to link an applicant to both current and previous circumstances;”<sup>xxviii</sup>*
- In practice firms utilise credit bureau data, trusted registries and increasingly Open Banking data to provide an activity history, such as for applications involving credit.
- GPG45 also includes a potentially wide variety of acceptable sources for activity history to be established.
- GPG45 grades the levels of Activity History based on the number of calendar days of history that has been established.

### **Interoperability assessment:**

- Score 1 activity history may not provide sufficient confidence regarding a claimed identity’s activity history and may not be suitable for higher risk transactions.
  - However, JMLSG Guidance does not stipulate specific expectations regarding activity history, and recent innovations such as Open Banking may provide alternative means to establish this digitally in many cases, perhaps combined with standard forms of account checking.
- Score 2 activity history or higher (3 months+), while not strictly required by JMLSG Guidance, is assessed as interoperable with processes utilised by financial services (when derived from an active, non-automated account).

## **IDENTITY FRAUD** - to check if the claimed identity is at a high risk of identity fraud

- GPG45 requires the identity provider to use reliable and authoritative sources to undertake a number of counter-fraud measures, the mix of which are dependent on the Identity Profile used. This ranges widely – from zero checks to strong counter fraud measures, and higher levels of confidence not always correlating to higher strength counter-fraud measures (e.g. High level identity, Profile H1B (9.3.1.2)).
- JMLSG Guidance frequently references the need for counter-fraud measures, and the important link between AML and Counter Terrorist Funding regimes and fraud and financial crime prevention, including identity-based crime.
- However, JMLSG Guidance does not itself set out the detail of what these measures should be, nor how they are applied by firms; this information is elsewhere.
- Detailed guidance concerning counter fraud checks and their application is not openly available outside of regulated firms and industries, except in high-level or redacted forms. This limits the degree to which a detailed gap analysis is possible to undertake or publish in detail.

**Interoperability assessment:**

- It is unclear at this stage the extent to which a JMLSG Guidance-compliant digital identity-based CDD process would require fraud checks to be built in – for example banks have alternative anti-fraud processes which exist under other Guidance and legal obligations, and whether the counter-fraud processes outlined in GPG45 would satisfy those requirements.
  - How this aligns with additional processes that the identity provider might undertake may be considered, such as additional screening and fraud checks.
- Processes to counter identity fraud that reach a Score of 2 under GPG45 involving additional checks (Electoral Roll entry for example) may not automatically pass an ‘independent and reliable’ check (independence of source is not guaranteed with Score 2 Fraud checks – see 7.3.2.). Detailed consideration of the specific GPG45 evidence-types and whether they each fulfil the test of ‘documents, data or information obtained from a reliable and independent source’ may be needed.
- Score 3 ensures a second authoritative source is used, and the two sources must be independent.

**VERIFICATION** - check that the identity belongs to the person who is claiming it

- There is broad equivalence of verification methods used across GPG45 and set out in JMLSG Guidance.
- GPG45 includes Knowledge-Based Verification (KBV) as an acceptable means of verification across a number of the identity levels and this is also referenced in JMLSG Guidance.
  - There have been some recent questions raised as to whether KBV and Knowledge-Based Authentication (KBA) is fit for purpose in the Financial Services sector, particularly when it is the sole factor.
  - The direction of travel for banks appears to be away from using KBV, although JMLSG Guidance currently references this as an acceptable method, and it plays an important role in verifying customers without photo evidence.










**Interoperability assessment:**

- Verification processes that receive a score of 1 include options where verification can be undertaken against information from another ML Regs 2017 compliant firm, which would require JMLSG Guidance compliance.
- However, score 1 verification could include a single high-quality KBV, which alone is unlikely to interoperate with JMLSG requirements in the majority of cases.
- Score 2 verification in GPG45 includes checks involving facial matching, biometric matching more widely via digital methods, or a series of dynamic KBV challenges.
  - The first two methods could meet the the JMLSG’s requirements, however;
  - Recent NCSC Guidance<sup>xxix</sup> concerning the potential weakness of KBV as the sole method of verifying or authenticating an individual would have to be taken into account by a relying party considering use of a Score 2 verification based solely on KBV;
  - To address this issue, KBV processes should be dynamic, and high quality.

**CAN GPG45-BASED SOLUTIONS MEET THE JMLSG CRITERIA FOR AN IDENTITY PROVIDER?**

JMLSG Guidance sets out an overarching list of criteria that digital identity providers would be required to meet, based on the requirements of the Money Laundering Regulations.

**GPG45 vs JMLSG GUIDANCE CRITERIA CHECKLIST**

JMLSG GUIDANCE NOTES CRITERIA		GPG45
1	It is recognised, through registration with the Information Commissioner's Office, to store personal data.	 Dependent on the IDP
2	Unless it is on the Information Commissioner's list of credit reference agencies (see <a href="https://ico.org.uk/for-the-public/credit/">https://ico.org.uk/for-the-public/credit/</a> ), it is accredited, or certified, to offer the identity verification service through a governmental, industry or trade association process that involves meeting minimum published standards.	 Scheme-level issue
3	It uses a range of multiple, positive information sources, including other activity history where appropriate, that can be called upon to link an applicant to both current and previous circumstances.	
4	It accesses negative information sources, such as databases relating to identity fraud and deceased persons.	
5	It accesses a wide range of alert data sources.	
6	Its published standards, or those of the scheme under which it is accredited or certified, require its verified data or information to be kept up to date, or maintained within defined periods of re-verification.	
7	Arrangements exist whereby the identity provider's continuing compliance with the minimum published standards is assessed.	
8	It has transparent processes that enable the firm to know what checks were carried out, what the results of these checks were, and what they mean in terms of how much certainty they give as to the identity of the subject.	 GPG45 does not preclude
9	A commercial organisation should have processes that allow the enquirer to capture and store the information they used to verify an identity.	 GPG45 does not preclude

## 4 B: HOLISTIC ANALYSIS

Perhaps the most fundamental difference between JMLSG Guidance Notes and GPG45 is the approach to managing risk – whereas GPG45 features standardised outputs (Identity Levels) and is prescriptive of the mix of credentials and processes that can be used (Identity Profiles), the JMLSG Guidance model is based on a risk-based assessment of what is deemed necessary to mitigate risk by the organisation undertaking the CDD, on a case-by-case basis.

JMLSG Guidance prompts organisations undertaking CDD to be proportionate to the level of risk, and this is reflected in a wider range and mix of evidence and checks used to satisfy a relying party-led CDD process. CDD processes can be used by the relying party in a more flexible way than is provided by the four Identity Levels established by GPG45.

The exact strength of the evidence and checking processes needed in order for the organisation to be ‘reasonably satisfied’ of the individual’s identity, is within the gift of the organisation to decide, and varies between organisations and sectors.

This does present challenges when assessing interoperability between GPG45 standardised outputs and risk-based guidance and raises some fundamental questions.

### **GPG45 IDENTITY PROFILES**

An Identity Profile is defined in GPG45 as a particular combination of identity checking processes.<sup>xxx</sup>

Under JMLSG Guidance relying parties create the equivalent of an Identity Profile for each individual for which they undertake CDD – they will have identified the level of risk in line with the risk factors set out in the JMLSG’s guidance, and applied their own risk appetite. They will have required a set of evidence, of a given strength, and checked to a given level of confidence as a result.

The output from that process is *in effect* an Identity Profile, just one that has been established to mitigate identity risk in a particular circumstance, rather than to a predetermined level, such as Low, Medium, High or Very High.

## ASSESSING IDENTITY PROFILES AGAINST JMLSG GUIDANCE

Looking at GPG45 through the lens provided by the JMLSG Guidance, how do the various Identity Profiles compare to the specific requirements of JMLSG?

### LOW Level Profiles

	Pieces of Evidence	1	1	1	3
	Profile	L1A	L1B	L1C	L3A
<b>Evidence 1</b>	Strength	2	3	3	1
	Validity	2	2	3	1
<b>Evidence 2</b>	Strength				1
	Validity				1
<b>Evidence 3</b>	Strength				1
	Validity				1
<b>Activity</b>					3
<b>Identity Fraud</b>		2		1	2
<b>Verification</b>		1	3	2	2

xxxii

#### Identity Level LOW: potential Identity Profile issues

1. Three Identity Profiles use only one piece of identity evidence – while a single piece of evidence is accepted in principle, this must be government-issued photo evidence with a name and address or name and DOB, and single evidence applications are not universally accepted in practice.
2. The Identity Profile with three pieces of evidence utilises only strength one evidence, which does not meet requirements of JMLSG Guidance Notes.
3. Several Identity Profiles have zero or score 1 for Activity and / or Identity Fraud. While in principle still interoperable with JMLSG Guidance (there are no specific JMLSG requirements to judge against), in practice this may require additional checks by the relying party.
4. Identity Profiles with a verification score of 2 may be utilising KBV as a sole method of verification, which is contrary to NCSC industry guidance. It should be noted that GPG45 v4.0 introduces more stringent criteria for knowledge-based checks, and this is considered as part of a balanced approach to mitigating risk.

## MEDIUM Level Profiles

Pieces of Evidence		1	1	2	2	2	2	3
Profile		M1A	M1B	M2A	M2B	M2C	M2D	M3A
<b>Evidence 1</b>	Strength	4	3	2	3	3	4	2
	Validity	3	3	2	3	3	3	2
<b>Evidence 2</b>	Strength			2	2	2	2	2
	Validity			2	2	2	2	2
<b>Evidence 3</b>	Strength							2
	Validity							2
<b>Activity</b>			2	3	2	2		2
<b>Identity Fraud</b>		1	1	1	2	1	2	2
<b>Verification</b>		3	3	3	2	3	2	2

### Identity Level MEDIUM: potential Identity Profile issues

1. Two Identity Profiles use only one piece of identity evidence – while a single government issued photo evidence is accepted in principle under JMLSG Guidance, single evidence applications are not universally accepted in practice.
2. Identity Profiles that utilise strength 2 evidence could be utilising evidence that is not considered sufficient for CDD purposes under JMLSG Guidance Notes (e.g. mobile phone contract)
3. Several Identity Profiles have score 1 for Activity and / or Identity Fraud. While in principle still interoperable with JMLSG Guidance (due to the lack of specific requirements to judge against), in practice this may require additional checks by the relying party.
4. Identity Profiles with a verification score of 2 may be utilising KBV as a sole method of verification.



## HIGH Level Profiles

Pieces of Evidence		1	1	2	2	2	3
Profile		H1A	H1B	H2A	H2B	H2C	H3A
Evidence 1	Strength	4	4	3	4	4	3
	Validity	3	4	3	3	3	3
Evidence 2	Strength			3	3	2	2
	Validity			3	3	2	2
Evidence 3	Strength						2
	Validity						2
Activity				3		2	3
Identity Fraud		3		2	2	2	3
Verification		3	3	2	3	3	3

### Identity Level HIGH: potential Identity Profile issues

1. Two Identity Profiles use only one piece of identity evidence – while a single strong photo evidence is accepted in principle, this may not be acceptable in practice.
2. Several Identity Profiles have zero Activity and / or Identity Fraud score. While in principle still interoperable with JMLSG Guidance (there are no specific requirements to judge against), in practice this may require additional checks by the relying party.
3. Identity Profiles with a verification score of 2 may be utilising KBV as a sole method of verification.

## VERY HIGH Level Profiles

Pieces of Evidence		1	2	2	3
Profile		V1A	V2A	V2B	V3A
Evidence 1	Strength	4	4	4	4
	Validity	4	4	4	4
Evidence 2	Strength		4	3	3
	Validity		4	3	3
Evidence 3	Strength				3
	Validity				3
Activity		4		2	1
Identity Fraud		3	2	3	3
Verification		4	4	4	4

### Identity Level VERY HIGH: potential Identity Profile issues

1. Two Identity Profiles use one piece of identity evidence; while a single piece of photo evidence is acceptable in principle, this may not be acceptable in practice.
2. Two Identity Profiles have zero Activity or Identity Fraud score. In practice this may require additional checks by the relying party to meet obligations.

## THE BENEFITS OF GPG45'S SCORING FRAMEWORK FOR INTEROPERABILITY

GPG45 provides a detailed framework for the scoring of evidence and checking processes across the 5 elements. It sets out objective criteria to enable scores to be assessed, and collectively these are used to create Identity Profiles (potentially not just those set out in GPG45) that can then be clearly recorded and shared in a consistent way.

In so doing, it provides a framework that can interoperate directly with JMLSG Guidance, albeit at present with the limitations and challenges identified on the following pages.

Despite that, the benefits of the scoring framework are numerous:

- Enabling an identity provider to record with some precision, the balance of evidence and processes used to create an identity.
- If shared, this information could be understood by the relying party, and would enable them to assess this against their risk assessment and their CDD requirements.
- Even if not shared, the framework set out in GPG45 enables a relying party to understand the range of Identity Profiles that could have been used to create a digital identity, and to consider that against their CDD requirements.
- Provides a framework within which specific additional or higher strength identity evidence or checks could be identified to inform a 'step-up' in an Identity Profile and its level of confidence.

### Digital Identity 'Step-Ups'

The concept of a step-up for a digital identity involves being able to add additional pieces of evidence, or more robust checks, to increase the overall level of confidence in a digital identity. For example, this could be to give details of your passport, when previously the evidence you had provided was based on something considered to be weaker – such as a council tax letter.

Or the identity provider or relying party could carry out some further checks – to give them greater confidence that you are who you claim to be, and that the evidence you've given is real, and belongs to you.

By doing this, the digital identity can move up to a higher level of confidence – e.g. moving from Low to Medium. This would have a number of benefits for the customer – perhaps lower costs because they become a lower risk customer, or access to a wider range of services.

Within a federated digital identity scheme, the additional information and identity data is retained, and can be re-used by the customer in future.

One key factor to enable 'step-ups' may be to enable sharing of Identity Profiles that are currently insufficient to meet the relying party's needs to be shared, and additional evidence or checks undertaken by the relying party to reach the desired level of confidence and enhance the customer's Identity Profile, and for that data to be retained for re-use.

## THE IMPACT OF GDPR ON THE LEVEL OF IDENTITY USED

The issue of identity level ‘step-up’ is explored on the previous page, but there may be other issues arising under GDPR when an individual has a digital identity level with a higher level of confidence than required to access the service. Much conversation has centred on the benefits that using a higher identity level would bring in terms of additional certainty and reduced risk, but GDPR may prevent disclosure of additional data not expressly required for the task in hand.

GDPR Article 25 concerns data protection by design and default.<sup>xxxiii</sup> It requires organisations to implement appropriate measures that are designed to implement data protection principles, and the need for data minimisation is specifically highlighted.

Article 5 1. c) is also relevant, and sets out the purpose limitation principle, requiring organisations to only process the personal data needed for the purpose.<sup>xxxiv</sup>

Therefore, if a customer has a ‘High’ level digital identity, but seeks to access a service requiring only a ‘Medium’ level of confidence, the relying party may be prevented from processing the additional identity evidence and checks that have elevated the confidence level associated with their digital identity from Medium to High. Whether this includes the profile score or just the underlying data and evidence remains unclear, and is a matter worthy of further consideration.

## THE IMPACT OF 5MLD ON THE NEED FOR DATA

If 5MLD is implemented in line with the text, relying parties would be enabled to accept digital identities from eIDAS-notified schemes to undertake CDD, or digital identities from other standards or schemes subsequently recognised by the relevant national authority (likely FCA or the UK Government).

If a given level of confidence or specific scheme were to be confirmed as meeting requirements for CDD via the implementation of 5MLD, then the need for the RP to have greater clarity on the exact evidence and processes underpinning a specific digital identity would diminish. This would greatly assist with ensuring data minimisation (vis-à-vis GDPR).

JMLSG Guidance would be amended to reflect the new Regulations and provide the regulatory clarity relying parties currently lack.

## POTENTIAL CHALLENGES

In addition to the issues already explored, there are a number of further challenges that could arise from interoperability between the profiles and levels of confidence set out in GPG45 and JMLSG Guidance:

**Financial Inclusion Issues:** If the lowest identity level that is interoperable with JMLSG Guidance is a Medium Level of Identity, this may create access and inclusion challenges.

In the example of thin-filed customers, perhaps applying for a lower-risk product, a Medium Level Identity may be very challenging to obtain, particularly in inclusion cases where non-standard identity credentials are often used by banks to identify these customers at present under JMLSG Guidance.

While the evidence range has increased with GPG45 v4, the types of non-standard identity credentials (some letters of introduction) do not appear to be permissible as evidence under GPG45, and those customers are unlikely to be able to gain an identity of sufficient assurance to satisfy the relying party's CDD needs, despite them being able to satisfy a risk-based onboarding for a basic product using more traditional channels.

**Limiting the Addressable Market:** If, as above, there are significant number of customers unable to obtain a sufficiently high identity level to satisfy relying parties, the addressable market size, and therefore addressable value via that channel, is reduced.

While there are other channels available to customers, remote and digital options are increasingly important for many sectors, many of which are reducing their physical presence on the high street.<sup>xxxv</sup>

**Additional Risk Mitigation:** Certain risk factors may require (at the firm's discretion) additional or stronger identity evidence to be supplied by the customer, or for additional checks (such as an additional verification method) to be used to mitigate the risk of identity impersonation, potentially part of a wider Enhanced Due Diligence (EDD) process.

How this would work in an interoperable digital identity environment based around GPG45, where the step-up between a Medium and High Level Identity Profile may be significantly more than the additional check required (and therefore more onerous for the customer to obtain) is another challenge that would require further consideration.

It is likely in such cases that the relying party would need to undertake additional, but more specific checks, to step up the level of confidence provided by the digital identity.

**Disproportionate risk mitigation:** While it is positive in principle to apply additional levels of risk mitigation, much AML Guidance, such as that produced by FATF, references the need for regulated firms to apply *proportionate* approaches to risk management.<sup>xxxvi</sup>

The three challenges above are a consequence of the identity level of confidence, from the 4 Identity Levels, or levels of confidence available, being disproportionate to the identity risk assessed by the relying party. Where this has no impact on the customer's experience, moving to a higher level of confidence is a very positive step – issues only emerge if unintended customer detriments occur, such as exclusion, or additional customer friction.

Customer detriments are likely to be experienced more acutely the greater the differential between required risk mitigation and the Identity Levels available to the relying party.

## 5 CONCLUSIONS AND RECOMMENDATIONS

### CONCLUSIONS

#### LIMITED INTEROPERABILITY MAY BE POSSIBLE NOW

- The in-depth scoring framework included in GPG45 v4 provides a firm foundation for future interoperability between schemes, and between JMLSG Guidance and GPG45.
- The scoring and profile frameworks provide a consistent, if potentially complex way to describe and share data about the strength of the evidence and checks used to create a digital identity.
- The retention of four common Identity Levels maintains a clear hierarchy of pre-determined levels of confidence to match against a relying party's assessment of risk for any given transaction.
- The framework would provide clarity for Identity Level step-ups to be effected, either between the four established levels of confidence in GPG45, or to increase the strength of specific elements of a person's Identity Profile.
- Despite the holistic and balanced approach in GPG45, relying parties may need to follow the more granular approach of JMLSG Guidance, making the misalignment of evidence categorisation across the two Guidances, the potential challenges around knowledge-based processes, and some profiles utilising single pieces of identity evidence a pertinent consideration for relying parties.
- In practice this could prevent some specific Identity Profiles from being used without further checks being made by the relying party – and to do this would require details of the Identity Profile data to be shared with the relying party.
- One possible solution to the point above would be to use 5MLD to recognise schemes or specific Identity Levels or Profiles using the GPG45 scoring framework.
- An alternative may be to provide relying parties clear sight of the individual Identity Profile used to create an identity, to enable additional targeted checks to be made by relying parties, or for identities to 'step up' to a higher level of confidence.
- A further alternative would be to transmit to the relying party the much more detailed underlying data concerning the identity and the specific evidence and checks used in its creation, although questions exist regarding the compatibility of this approach with GDPR's data minimisation requirements.

## **5MLD IMPLEMENTATION WOULD BE A BIG BOOST FOR INTEROPERABILITY**

- While not critical to the development of an interoperable digital identity market, the provision in 5MLD of a clear regulatory standing for eIDAS digital identity schemes for undertaking CDD would increase certainty and reduce regulatory risk for relying parties and could provide regulatory support for the use of existing eIDAS identities by regulated firms in the private sector.
- It would also provide an opportunity for relevant national authorities to recognise other schemes, which would also then gain regulatory clarity and thereby lower risks for relying parties – this is explored in more depth in Part 2.
- 5MLD should therefore be implemented in line with the text and intention of Article 13.1 of the agreed text, at least concerning the specific recognition of eIDAS-notified digital identity schemes and other schemes recognised by the relevant national authority will have a clear status in the CDD regime.

## **LANGUAGE SHOULD BE ALIGNED**

- GPG45 and JMLSG Guidance’s terminology and definitions are not aligned in a number of areas.
- The language used to describe processes relating to digital identity in JMLSG Guidance should be reviewed and the potential for them to be aligned with GPG45 be considered.
- The language used in GPG45 to describe processes and principles central to CDD and set out in JMLSG (e.g. Reliable and Independent) should be reviewed and the potential for them to be aligned or cross-referenced with JMLSG should be considered.

## **CROSS-REFER TO THE GPG45 SCORING FRAMEWORK IN JMLSG**

- JMLSG’s criteria for evidence-weighting is not as granular as that provided in GPG45, nor does it provide a consistent or detailed framework to allow information concerning CDD evidence and process to be shared amongst parties in a reliance relationship.
- JMLSG should consider whether the more detailed scoring framework set out in GPG45, for both evidence and checks, and the underlying criteria should be referenced in JMLSG, or even incorporated.

## **REVIEW RELIANCE ON KNOWLEDGE-BASED PROCESSES**

- GPG45 v4.1 presents a more sophisticated range of KBV and associated processes than previously, with more stringent criteria for their use, and this is considered as part of a balanced score within Identity Profiles.

- However, given the wider move away from KBV, particularly when used as a sole factor, the prominence and weighting given to KBV in industry guidance should be kept under review.
- To address potential weaknesses relating to KBV, any KBV processes should be of high quality and involve dynamic checks.

#### **FURTHER CHALLENGES WOULD STILL EXIST**

- There are wider challenges to consider outside of GPG545 and JMLSG Guidance interoperability – such as the issue of FCA rules concerning systems and controls and the issue of material outsourcing. These lie outside of the scope of this research, and merit further consideration.
- The research has predominantly focused on CDD by financial services. However, requirements for identity risk mitigation are not consistent even across this one sector. This variance is greater still when other sectors are considered.
- The Identity Profiles or Identity Levels required by a relying party in practice could vary significantly, and a Medium level identity would set a disproportionately high bar for uses with lower levels of identity risk. This was considered particularly true by the participants in the project's Peer Review Group.\*

*\* The Peer Review Group included representatives from a range of regulated sectors – see page 1 for a list of participants, and Part 2 for further details.*

- Identities reaching only a Low Identity Level (a low level of confidence) remain too low for the vast majority of JMLSG Guidance's CDD purposes.
- Financial exclusion, limited access to digital identities and to services via digital identity, and market size could all be negatively impacted if the difference is too great between the assessed level of risk, and the Identity Level available to be used.

A number of these challenges are amongst the future-facing issues explored in Part 2.

## RECOMMENDATIONS

Based on the conclusions above, the following actions are recommended:

- 1. Establish GPG45 as a basis for private sector digital identity standards.**  
While GPG45's status is considered to be guidance, it provides a framework that could be used as the basis for recognised standards within schemes in the UK.
- 2. Extend the use of the Government's Document Checking Service to private sector digital identity schemes.** This would enhance the range of trusted validation processes available to the private sector.
- 3. Implement 5MLD in full, and in line with the EU text.** This also provides an opportunity to review the intended interpretation of 'Liability' vs 'Responsibility' (Article 39 ML Regs 2017).
- 4. For the relevant national authority/s to recognise standards or schemes in-line with Article 13.1 of 5MLD.** This could be the identity Profiles set out in GPG45, or include additional Identity Levels, based on the outcome of Recommendation 5 below.
- 5. To research sectoral needs and the case for additional Identity Profiles or Identity Levels to be considered by industry representative bodies.**  
This analysis would inform Recommendation 4 above.
- 6. Align language and definitions for common issues and concepts – this will require close working between GDS and the JMLSG secretariat.**  
Where JMLSG Guidance refers to issues central to digital identity, to adopt or cross-refer to GPG45 definitions (e.g. verification, identity evidence, credentials, proofing, authentication), and for GPG45 to adopt or cross-refer to JMLSG Guidance's definitions for established AML-related terminology (e.g. refer to 'independent and reliable' sources).
- 7. For JMLSG to consider cross-referring to, or adopting, the more detailed evidence weighting and criteria, and the scoring framework presented in GPG45.** This would greatly improve interoperability and remove ambiguity for relying parties.
- 8. Consider the future application and suitability of knowledge-based checking, and knowledge-based processes much be high quality and dynamic.** This may be particularly important when it is used as a single-factor, even within a balanced score approach.



## PART 2

# Developing an Interoperable Digital Identity Market

Part 2 considers potential interoperable market scenarios, and what this means for GPG45 and JMLSG Guidance.

## 6 TOWARDS AN INTEROPERABLE DIGITAL IDENTITY MARKET

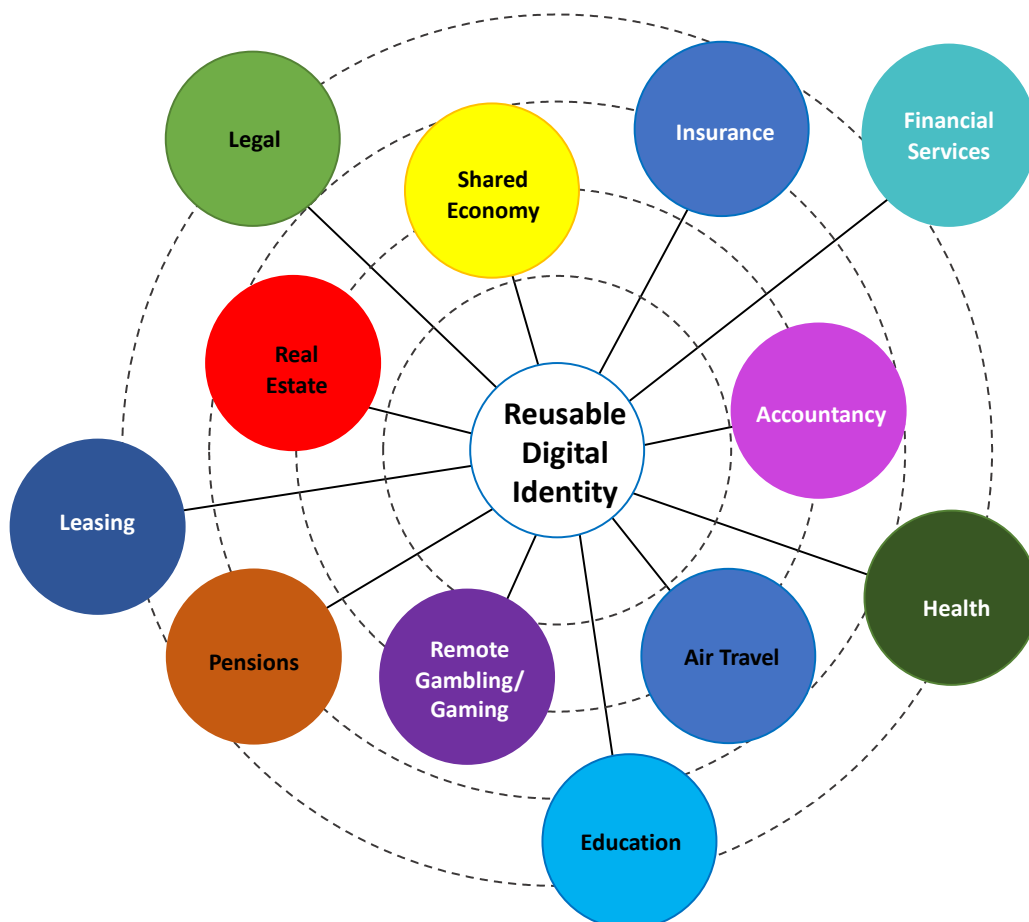
The project's core aims are met in Part 1 of this report. However, the project participants and the wider Peer Review Group also considered what an interoperable market with GPG45 and JMLSG Guidance as part of it could look like, within the wider aspects of Objective 5 of the project:

*5. Identify where factors such as guidance, standards, procedures and design may need to be modified or adapted to enable convergence of the industry guidance and potential use of GPG45 in such a way that allows a customer to use a digital identity in an onboarding journey.*

The considerations and future options explored are included in Part 2, alongside a balanced view of their potential benefits and challenges, demonstrated with a number of interoperable market scenarios.

### POTENTIAL RELYING PARTY ECOSYSTEM

JMLSG Guidance and CDD obligations impact on a wide range of activities, supervisory bodies and trade associations in addition to those in the financial services sector.



Stakeholders' reflections on what a good interoperable market would look like:

## FEATURES OF A 'GOOD' DIGITAL IDENTITY MARKET

- **Widely interoperable** – interoperability across sectors/uses enabled by recognised standards was a consistent feature in the discussions.
- **Identities that are re-usable** - that digital identities can be re-used, and the associated benefits were considered fundamental to a good digital identity market.
- **Cross-border** – existing links to eIDAS and other international identity frameworks should be retained, and extending international interoperability would be beneficial.
- **Mobility and choice** – Customers to be able to:
  - choose / move between identity providers
  - move between different ID profiles and 'step-up' their identity when possible
  - have multiple digital identities
- **Competition** – positive competition between identity providers **and** schemes.
- **Further differentiation** – different relying parties and sectors should be able to determine Identity Profiles that closely meet their risk-assessed requirements.
- **Avoid fragmentation** – the potential for market fragmentation was also discussed, and a fragmented / confusing market was identified as a negative outcome.
- **Coalescence** – a mature market was thought likely to see coalescence around a limited number of widely applicable digital identities or schemes.
- **Granular** – exact components of identity profiles and the level of identity confidence required should be driven by market need.
- **Data access** – the evidence and checks that were used to create the identity should be accessible to relying parties:
  - A mature market may require access to data only upon demand, established identity profiles become trusted.
  - The early market was discussed as possibly requiring the underlying data to be shared for every digital identity relied upon, to allow firms to apply a risk-based assessment should they wish, identify potential step-ups if required, and to build confidence in the suitability of the identity profile used.
  - For some financial institutions having access to the data that underpins the identity was considered to be vital.
  - An audit trail to the original source of evidence when required (for instance for law enforcement) was also considered essential by some relying parties.
- **Inclusive** – reliance on digital identities should not present unnecessary barriers for customers to access services.
  - Digital Identity was seen by many relying parties to be more than 'another channel' – inclusivity was an important factor for relying parties.
  - It was also considered in terms of increasing the value of the market addressable by digital identity.
- **Certification** – Some form of market-facing certification of schemes.
- **Formal Recognition** - recognition of the status of specific identity profiles / schemes, ideally by government, regulator or supervisor.
- **Strong governance** – effective governance and oversight of schemes is vital for trust to be established.

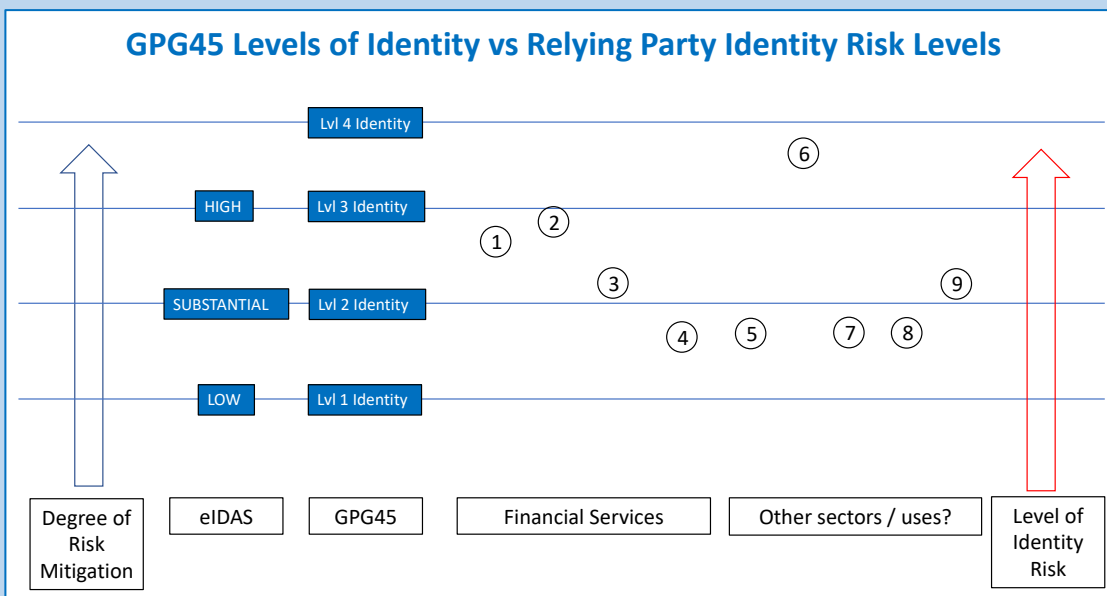
To develop an interoperable market, stakeholders will need to consider how the further challenges identified in the Part 1 analysis could also be addressed, and ways to enhance interoperability and the functioning of the market.

In particular:

- To retain the ability of relying parties to apply a proportionate risk-based approach
- To seek to address financial exclusion, and market access issues
- To ensure the relying party is confident in using digital identity for CDD

**THE REQUIRED LEVEL OF IDENTITY VARIES ACROSS USES AND SECTORS**

Relying parties that apply risk-based CDD have a variety of needs, proportionate to the assessed level of identity risk, and therefore vary in the strength of the risk mitigation they require, and the evidence profile and relative strength of a digital identity that could satisfy their need. This variance is true even for individual relying parties, across their different relationships or transactions.



1-9 are illustrations of the varying level of CDD risk across different activities and sectors.

## EXPLORING POTENTIAL FUTURE SCENARIOS

There may be a number of ways to develop a digital identity framework that can enable a wide range sectors and uses, and that can provide firms with the ability to apply a proportionate approach to mitigating identity risk.

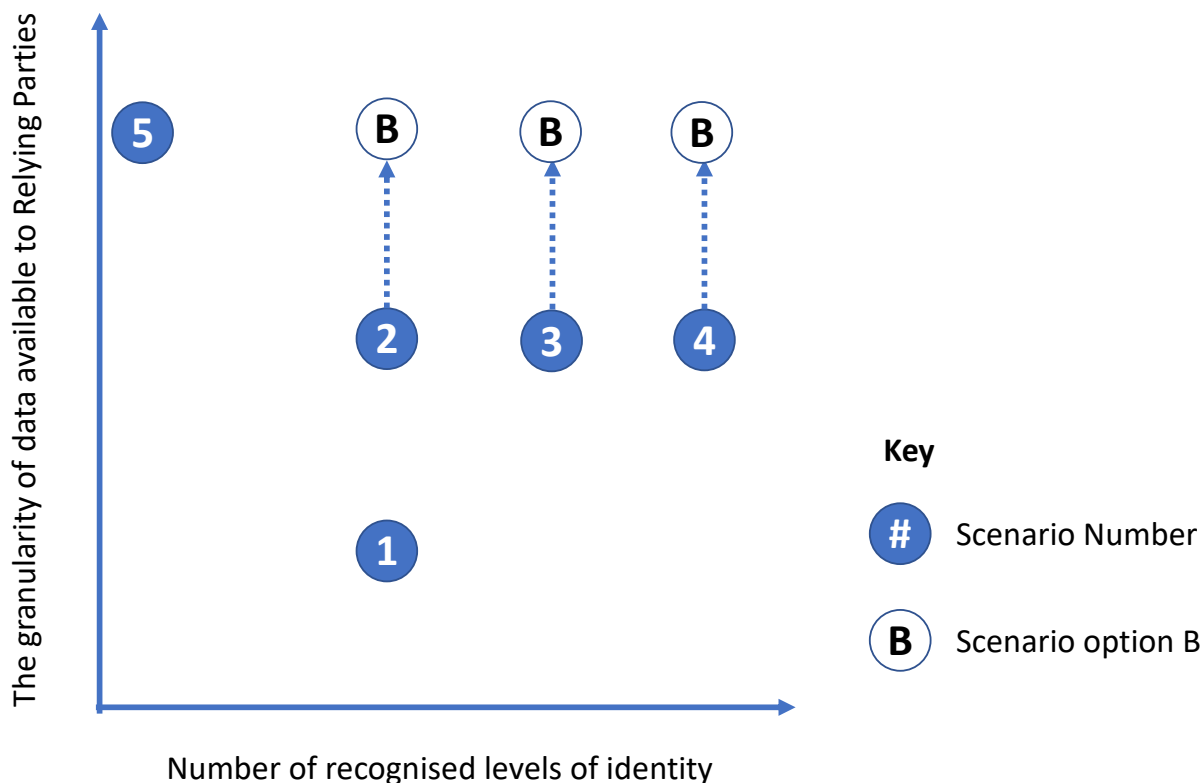
Two key variables that will be considered in the scenarios will be:

- The number of recognised Identity Levels (levels of confidence)
- The granularity of the data made available to the relying party concerning the specific evidence and checks used to establish an identity

Five scenarios are expressed below, to illustrate some of the range of options to create a digital identity market based on the two variables above.

SCENARIO FEATURES (KEY VARIABLES IN BOLD)	
SCENARIO 1	<ul style="list-style-type: none"> <li>- <b>GPG45 provides digital identity standards for the private sector.</b></li> <li>- <b>No Identity Profile data shared with relying parties.</b></li> <li>- <b>Granular data is available to relying parties only on request.</b></li> <li>- <b>GPG45 Identity Levels Low to Very High are recognised by the relevant authority.</b></li> <li>- <b>No other Identity Levels are recognised.</b></li> </ul>
SCENARIO 2	<ul style="list-style-type: none"> <li>- GPG45 implemented (as above).</li> <li>- <b>Identity Profile information is provided to relying parties as standard.</b></li> <li>- <b>Version B (of this scenario): granular data concerning evidence and checks undertaken is provided to relying parties.</b></li> <li>- GPG45 Identity Levels Low to Very High are recognised (as above).</li> <li>- No other Identity Levels are recognised (as above).</li> </ul>
SCENARIO 3	<ul style="list-style-type: none"> <li>- GPG45 implemented (as above).</li> <li>- Access to data – as Scenario 2/2B above.</li> <li>- <b>An additional 1 or 2 Identity Levels or alternative Identity Profiles are established, reflecting additional relying party/consumer needs.</b></li> <li>- <b>Both GPG45 Identity Levels and 1 or 2 additional Identity Levels are recognised by the relevant authority/s.</b></li> </ul>
SCENARIO 4	<ul style="list-style-type: none"> <li>- GPG45 implemented (as above).</li> <li>- Access to data – as Scenario 2/2B above.</li> <li>- <b>A number of additional Identity Levels are established on a sector-by-sector basis and recognised by relevant authority/s.</b></li> </ul>
SCENARIO 5	<ul style="list-style-type: none"> <li>- GPG45 implemented (as above).</li> <li>- Access to data – as Scenario 2B above.</li> <li>- <b>No specific Identity Levels are recognised by the relevant authority/s.</b></li> <li>- <b>Each digital identity is considered on the strength of the evidence and checks used to create it – the customer’s Identity Profile.</b></li> <li>- <b>Relying parties use digital identities as a means to undertake risk based CDD as now, but via a digital identity channel.</b></li> </ul>

### SCENARIOS ANALYSIS



### SCENARIO 1

POSITIVES	NEGATIVES
<ul style="list-style-type: none"> <li>• Benefits of having established Identity Levels recognised for use in CDD.</li> <li>• Recognition of GPG45-based schemes, and alignment with international frameworks possible post-5MLD.</li> <li>• Ecosystem of existing identity providers already working under GPG45.</li> <li>• Growing population of GPG45 digital identities already in existence.</li> <li>• Relying parties can still access identity source data upon request (e.g. if required by the regulator) to retain legal compliance.</li> </ul>	<ul style="list-style-type: none"> <li>• The four Identity Levels available may be disproportionate for some identity risks assessed by relying parties.</li> <li>• Access and inclusion issues.</li> <li>• Limits the value of the addressable market</li> <li>• Limitations to undertake limited additional checks via a digital identity solution.</li> <li>• Relying parties would not be able to identify what credentials or routes were used to create an identity- this may unduly limit their ability to satisfy themselves under JMLSG Guidance.</li> </ul>

## SCENARIO 2

POSITIVES	NEGATIVES
<ul style="list-style-type: none"> <li>• Benefits of having established Identity Levels recognised for use in CDD.</li> <li>• Recognition of GPG45-based schemes, and alignment with international frameworks possible post-5MLD.</li> <li>• Ecosystem of existing identity providers already working under GPG45.</li> <li>• Growing population of GPG45 digital identities already in existence.</li> <li>• Relying parties can access Identity Profile scores, or source data (scenario vB) for each identity. This enables an accurate and detailed risk-based assessment by the relying party.</li> <li>• Very specific step-ups for individual customers could be identified, or specific additional checks undertaken.</li> <li>• Regulatory recognition under 5MLD could remove concerns regarding differences between Identity Profiles.</li> </ul>	<ul style="list-style-type: none"> <li>• In some cases, Identity Levels may still be disproportionate for some identity risks assessed by relying parties.</li> <li>• Access and inclusion issues.</li> <li>• Limits the value of the addressable market.</li> <li>• Limitations to undertake limited additional checks via a digital identity solution.</li> <li>• Additional costs or security risks involved in transmitting detailed data have not been assessed in this report.</li> </ul>

## SCENARIO 3

POSITIVES	NEGATIVES
<ul style="list-style-type: none"> <li>• The Identity Levels available could provide a level of confidence in a digital identity that is more proportionate to the risks associated.</li> <li>• Reduced barrier to access a digital identity could mean it is more inclusive.</li> <li>• The size of the market addressable by digital identity is increased.</li> <li>• Potential for enhanced market competition and added differentiation and choice for consumers.</li> </ul>	<ul style="list-style-type: none"> <li>• Moving away from the established four Identity Levels may create confusion amongst relying parties and consumers.</li> <li>• Will confidence in additional Identity Levels take time to be developed?</li> <li>• Do we have the data required to identify the additional Identity Levels that may be required?</li> <li>• Further Identity Levels will require more complex step ups, and potential additional friction and costs.</li> </ul>

## SCENARIO 4

POSITIVES	NEGATIVES
<ul style="list-style-type: none"> <li>• The Identity Levels available could provide a level of confidence in a digital identity that is more proportionate to the risks associated.</li> <li>• Reduced barrier to access a digital identity could mean it is more inclusive</li> <li>• The size of the market addressable by digital identity is increased</li> <li>• Potential for enhanced market competition and added differentiation and choice for consumers.</li> </ul>	<ul style="list-style-type: none"> <li>• Moving away from the established 4 Identity Levels of Confidence may create confusion amongst relying parties and consumers.</li> <li>• Will confidence in additional levels take time to be increased?</li> <li>• Do we have the data required to identify any common levels required?</li> <li>• Further levels will require more complex step ups, and potential additional friction and costs.</li> </ul>

## SCENARIO 5

POSITIVES	NEGATIVES
<ul style="list-style-type: none"> <li>• Ensures that the level of confidence required of a digital identity can be highly calibrated to the use case.</li> <li>• More accurately reflects the relying party’s risk-based CDD needs – it is in effect today’s system; an additional electronic channel for identity data to those already in existence.</li> <li>• Provides maximum control for relying parties.</li> <li>• Potential for self-sovereign identity solutions to emerge.</li> </ul>	<ul style="list-style-type: none"> <li>• No regulatory certainty if common Identity Levels are not recognised.</li> <li>• Complexity and friction for customers may increase.</li> <li>• Trust is not enhanced.</li> <li>• New product and service development could be stifled by a less federated market.</li> </ul>

## FUTURE MARKET TRAJECTORIES

These scenarios are not the only potential outcomes; however they do serve to provide illustrations of some key future options and their potential merits.

- Scenarios 1 and 2 are based on existing guidance, although they will require formal recognition of GPG45 by the relevant national authority/s.
- Scenarios 3 and 4 feature additional Identity Levels being established and formally recognised – this may take time, and may not prove to be required.
- Scenario 5 is a ‘wildcard’ option – it may be more likely if 5MLD is not implemented.



## 7 FURTHER ISSUES TO CONSIDER

It is clear from the analysis that relatively little needs to happen in order for GPG45 to be interoperable, at least in principle, with JMLSG Guidance. However, without further thought and potentially some changes to how elements of GPG45 are intended to be used, and how data is shared, implementation will not be optimal and barriers will continue to exist for relying parties.

The action recommended to ensure that interoperability is possible, and the soft barriers such as differences in language and definitions are addressed, are set out at the end of Part 1 of this report.

Looking to the future and developing a truly interoperable digital identity market, informed by the deliberations of the project participants, the Peer Review Group, and by the scenario analysis above, a number of issues meriting further consideration have emerged:

### **CONSIDER RECOGNISING ADDITIONAL DIGITAL IDENTITY PROFILES OR IDENTITY LEVELS IN ADDITION TO THOSE SET OUT IN GPG45**

There are likely to be many use cases where the existing GPG45 Identity Levels (Low to Very High) are perfectly able to meet the needs of private sector relying parties in their current form, if issues such as the equivalency of evidence types and the ongoing standing of processes such as KBV can be addressed.

Alternative Identity Levels or Identity Profiles could also be developed, specific to a given use case or sector, or even for uses across sectors. These alternatives could be then be recognised by the relevant authority, in line with 5MLD, providing regulatory certainty.

There are some significant positives that would derive from this, although it would by no means be a general panacea, and risks adding to market complexity, additional costs and potential confusion to customers. However, the strong preference expressed by other sector representatives in the Peer Review Group discussions make this an option that should be considered.

### **CONSIDER STANDALONE USE OF THE GPG45 SCORING FRAMEWORK**

The element of GPG45 that is ultimately vital to underpin interoperability, and that would be needed for an interoperable market to emerge, is the categorisation and scoring components of GPG45.

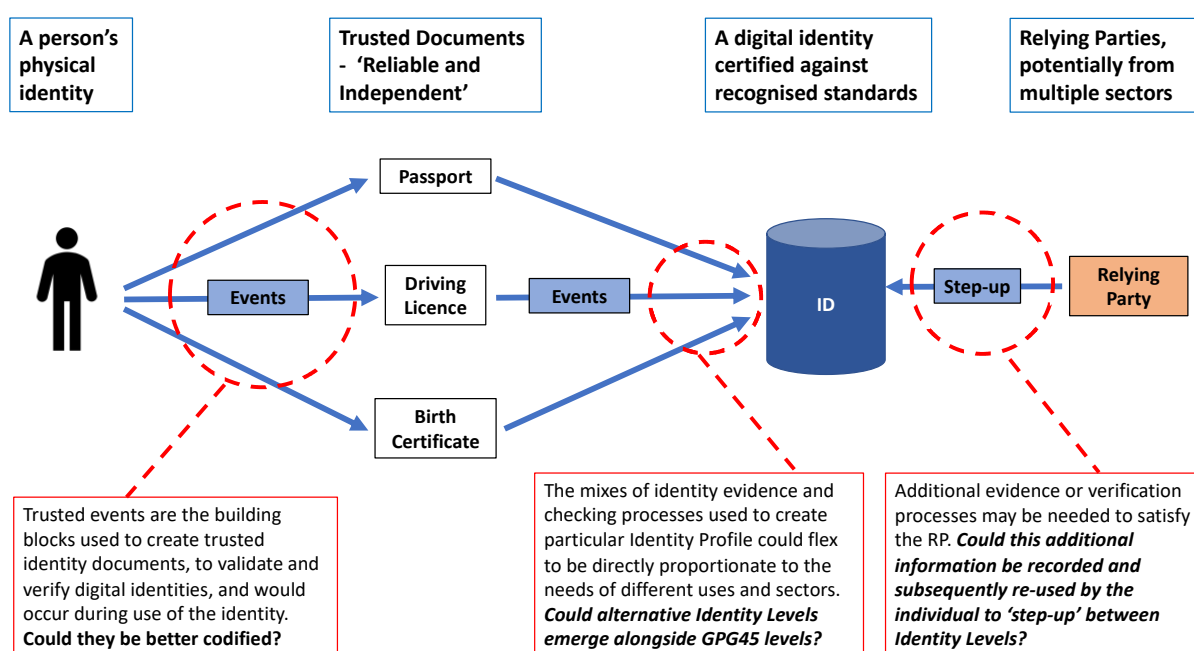
- The common scoring framework provide a means for an identity provider to assess, record, and share the specific components of an Identity and how it was created in a consistent and comparable manner, whatever the Identity Profile that results.
- It provides an opportunity to provide clear step-ups (below)
- It provides a means for an identity provider or relying party to understand the Profile of a 'partial identity', or a failed attempt to reach an established Identity Level, and still augment or utilise the identity data.

## CONSIDER HOW TO ENSURE MOBILITY BETWEEN IDENTITY LEVELS: STEP-UPS

It should be recognised that step-ups already exist between established Identity Levels that enable a customer to increase the level of confidence established by their identity by providing additional credentials and enabling additional or different verifications to take place.

If additional Identity Profiles or Identity Levels are developed, additional step-ups will need to be established to ensure customer mobility in the market, and to underpin market competition. This would be enabled by the common scoring framework above and enhanced by the greater standardisation of events (see below).

### STEP-UPS, STANDARDISED EVENTS AND ADDITIONAL IDENTITY PROFILES



### CONSIDER STANDARDISING TRUSTED EVENTS

The provision of standardised data concerning trusted events associated with an identity (such as additional verifications, or new evidence being provided by the individual) could give relying parties or identity providers even greater insight into the upstream methods by which a digital identity or its Identity Profile has been established, to assist them in making risk-based business decisions.

It would provide a much stronger audit trail to an identity and its creation, use and changes over time – a vital factor for use by financial service firms in particular, and beneficial to building trust in an identity over time. Standardised trusted event data could also be a significant enabler for self-sovereign identities, should this approach develop in future.

GPG45 itself does not capture a lot of event data, and nor does it aim to. Despite this, the fact remains that we do not currently have a sufficiently detailed framework to categorise

and share trusted events in a consistent and objective manner, and this could be a valuable next step for digital identities, and one that GPG45 should consider for future iterations.

Potential examples of categories for trusted events:

- Face to face verifications
- New identity evidence being issued
- Machine-read electronic evidence being verified
- Biometric credentials being added and verified
- Successful further verifications or authorisations
- A successful 'step-up' between Identity Levels

The subject certainly deserves further thought.

### **CONSIDER THE BENEFITS OF MAKING DETAILED UNDERLYING IDENTITY DATA READILY AVAILABLE TO RELYING PARTIES**

The underlying data concerning the credentials and processes used to create a specific digital identity could be shared with relying parties for every new CDD process, rather than upon request.

In the first instance this would enable firms to distinguish the various credentials, proofing and verification used to create a digital identity, and consider it in line with their own risk assessment.

This may in time build confidence amongst participants in a scheme regarding what they receive, and result in a more trusted environment, general acceptance of the data provided under established Identity Levels, and diminish the need for data provision longer-term.

### **CONCLUSIONS**

The in-depth analysis presented in Part 1 gave rise to a number of recommendations that can make the interoperability between GPG45 and JMLSG Guidance more complete, and remove residual points of friction or uncertainty. 5MLD will be a big help if implemented, but is not critical – GPG45 and JMLSG Guidance are already fundamentally interoperable, but with limitations. Part 2 raises a number of issues that merit further consideration by the various stakeholders in the emerging digital identity market – issues that can shape the future market, and in-turn begin to drive further innovation.

Ultimately, there is nothing that currently provides an absolute barrier to interoperability. Further action, and some amendments to both GPG45 and JMLSG Guidance could provide further momentum to the emerging market, and provide more complete interoperability framework. They can help to ensure the future digital identity market brings significant benefits to all parties – to identity providers, to relying parties, also to regulators and the Government, but most of all to consumers.

## REFERENCES

- <sup>i</sup> <https://www.gov.uk/performance/govuk-verify>
- <sup>ii</sup> FATF Guidance for a Risk Based Approach (2014)  
<http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf>
- <sup>iii</sup> JMLSG Part 2, 1.14  
<http://www.jmlsg.org.uk>
- <sup>iv</sup> FATF Guidance for a Risk Based Approach (2014) page 14, para 44 (link as above)
- <sup>v</sup> GPG45 v4.1 (2019)  
[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/795611/identity\\_proofing\\_and\\_verification\\_of\\_an\\_individual\\_v4.1.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795611/identity_proofing_and_verification_of_an_individual_v4.1.pdf)
- <sup>vi</sup> JMLSG Part 1, Para 5.3.81  
<http://www.jmlsg.org.uk>
- <sup>vii</sup> GPG45 v4.1 (2019) para 3.1, page 7  
[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/795611/identity\\_proofing\\_and\\_verification\\_of\\_an\\_individual\\_v4.1.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795611/identity_proofing_and_verification_of_an_individual_v4.1.pdf)
- <sup>viii</sup> NIST IR 8149 'Developing Trust Frameworks to Support Identity Federations' (2018)  
<https://nvlpubs.nist.gov/nistpubs/ir/2018/nist.ir.8149.pdf>
- <sup>ix</sup> ML Regulations (2017) Regulation 28(2)(a), and JMLSG Guidance Part 1 (2017), para 5.3.2  
<http://www.jmlsg.org.uk>
- <sup>x</sup> Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017  
<http://www.legislation.gov.uk/ukxi/2017/692/made>
- <sup>xi</sup> 4<sup>th</sup> Money Laundering Directive (2015), Article 25  
[https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ%3AJOL\\_2015\\_141\\_R\\_0003](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ%3AJOL_2015_141_R_0003)
- <sup>xii</sup> 4MLD Article 27 (link as above)
- <sup>xiii</sup> NCSC Guidance on Multi-Factor Authentication for Online Services  
<https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services>
- <sup>xiv</sup> Money Laundering: EU Law: Written question - HL9580 (17 July 2018)  
<https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Lords/2018-07-17/HL9580>
- <sup>xv</sup> JMLSG Part 1, 5.3.89 (link as above)
- <sup>xvi</sup> Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (2014)  
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN>
- <sup>xvii</sup> 5<sup>th</sup> Money Laundering Directive (2018), preamble (22)  
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN>
- <sup>xviii</sup> 4MLD Article 13.1 (link as above)
- <sup>xix</sup> 5MLD Article 13.1 (link as above)
- <sup>xx</sup> 5MLD, Annex III (link as above)
- <sup>xxi</sup> 5MLD Article 40 (1) (link as above)
- <sup>xxii</sup> 5MLD Article 27 (2) (link as above)
- <sup>xxiii</sup> ML Regs (2017) Article 39 (link as above)
- <sup>xxiv</sup> 4MLD Article 25 (link as above)
- <sup>xxv</sup> BankID Contract example, para 14, p.4  
<https://www.dnb.no/portalfront/dnb/nedlast/privat/avtaler/bankid-agreement.pdf>
- <sup>xxvi</sup> ML Regs (2017) Article 28 (18)(a) (link as above)
- <sup>xxvii</sup> BaFin Federal Financial Supervisory Authority Germany, Circular (2017)  
[https://www.bafin.de/EN/PublikationenDaten/Jahresbericht/Jahresbericht2017/Kapitel2/Kapitel2\\_5/Kapitel2\\_5\\_2/kapitel2\\_5\\_2\\_node\\_en.html](https://www.bafin.de/EN/PublikationenDaten/Jahresbericht/Jahresbericht2017/Kapitel2/Kapitel2_5/Kapitel2_5_2/kapitel2_5_2_node_en.html)
- <sup>xxviii</sup> JMLSG Part 1, 5.3.52 (link as above)
- <sup>xxix</sup> National Cyber Security Centre Guidance for Multi-Factor Authentication for Online Services (2018)  
<https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services>
- <sup>xxx</sup> GPG45 v4.1 (2019) 3.0.6 (link as above)
- <sup>xxxi</sup> Bullet 4: NCSC Guidance on Authentication (link as above)
- <sup>xxxii</sup> Bullet 4: NCSC Guidance on Authentication (link as above)
- <sup>xxxiii</sup> GDPR Article 25 <https://gdpr-info.eu/art-25-gdpr/>

<sup>xxxiv</sup> GDPR Article 5 <https://gdpr-info.eu/art-5-gdpr/>

<sup>xxxv</sup> Parliamentary Debate Report: Impact of ATM closures on towns and communities (2018)  
<https://researchbriefings.parliament.uk/ResearchBriefing/Summary/CDP-2018-0269>

<sup>xxxvi</sup> FATF Guidance for a Risk Based Approach (2014) (link as above)