Aligning GPG45 and JMLSG Guidance for Customer Due Diligence

to underpin the adoption of digital identity schemes

OIX Members Meeting

Thursday 9th May 2019

Intended Impact of the Project

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

We recognise that other industries take into consideration Guidance Notes from the JMLSG.

OIX Project Team

Barclays

HSBC

Lloyds Banking Group

Post Office

Government Digital Service

Experian

LexisNexis Risk Solutions

Innovate Identity

Peer Review Group Invited Participants

Dept for Digital, Culture, Media and Sport (DCMS)

HM Treasury (HMT)

Financial Conduct Authority (FCA)

Association of British Insurers (ABI)

Building Societies Association (BSA)

Finance and Leasing Association (FLA)

Tax Incentivised Savings Association (TISA)

UK Finance (UKF)

Joint Money Laundering Steering Group (JMLSG)

FinTech Delivery Panel (FDP)

Open Banking Implementation Entity (OBIE)

Gambling Commission (GC)

Remote Gambling Association (RGA)

tScheme

ICO

Experian

Innovate Identity (InID)

Open Identity Exchange (OIX)

Good Practice Guide 45 v 4.1

1. Improved language, easier for non-technical readership
2. Included examples to help readers better understand the requirements
3. You can reuse identity checks done by another organisation, for example, a relying party, if they do some or all parts of the identity checking process as set out in the guidance
4. Identity Levels 1-4 are now Low, Medium, High, Very High Identity Levels of Confidence
5. More Identity Profiles (scored combinations of identity checking processes) offering more flexibility. For example, there are 4 possible Identity Profiles that can result in a Low Confidence Identity Level
6. More guidance around biometrics

Good Practice Guide 45 v 4.1

Scope for

1. Using Identity Evidence scores to create additional profiles and/or Identity Levels of Confidence. For example, the online gambling sector could create an Identity Profile and/or Level of Confidence for account opening – Identity Profile G1A
2. Organisations with customer bases could apply score and create Identity Profiles and/or Levels of Confidence (note, more Identity Profiles to cater for users that are well known to an organisation but have limited identity evidence)
3. Sharing of underlying scoring within Identity Profile with relying party (scheme rules)

Good Practice Guide 45 v 4.1

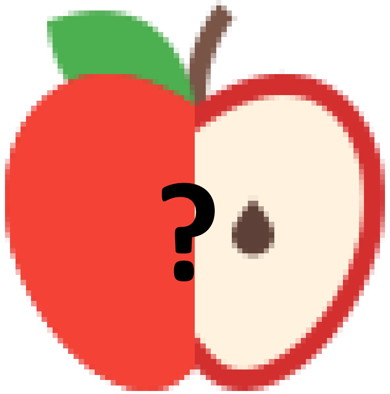
However

There may be GDPR considerations on what can be shared, that need to be worked through. For example, if a user has a higher Identity Level of Confidence than is needed for the service they wish to use.

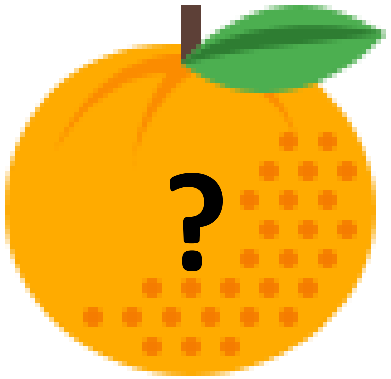
Alternative Identity Levels of Confidence need to be considered in context of interoperability across sectors. For example, Identity Profile G1A (Gambling) would need to be stepped-up for a government service requiring an Identity Level of Confidence MEDIUM, but not for a service that requires LOW

Aligning between GPG45 and JMLSG Guidance

Standards vs Risk-based approach



STANDARDS VS RISK-BASED



Standards-based vs risk-based – **Identity Level of Confidence** to **Identity Risk Level** equivalency will vary based on the organisation, the customer, the product and the context.

- This is reflected in:
    - the range of data required by firms
    - the type of evidence relied upon, and
    - the strength of the checks undertaken

Gap Analysis
a) Language and Definitions

EXAMPLES OF LANGUAGE AND DEFINITIONS VARIANCE:

1. Verification

2. Authentication

3. Face-to-face vs in-person (digital link; physical presence)

4. References to ‘Documents’ and ‘original documents’ in JMLSG

Gap Analysis

b) Granular Analysis - Evidence of Identity

There is broad (90%+) commonality of the evidence used across GPG45 LOC MEDIUM and above, and the expectations set out in JMLSG Guidance regarding CDD and customer identification.

- A LOW level of confidence identity provides insufficient identity evidence to be considered equivalent to any standard CDD requirement under JMLSG
- A HIGH level of confidence identity meets or exceeds the standard identity evidence requirements set out in JMLSG
- A MEDIUM level of confidence identity may or may not meet the identity evidence set out in JMLSG, depending on the Identity Profile of the user
- The hierarchy (strength) of identity evidence in JMLSG differs in some areas to the strength of evidence in GPG45

Recommendations

1. Government/industry to establish GPG45 scoring framework as a basis for private sector digital identity interoperability
2. Government to enable digital identity schemes used in the private sector to utilise the Document Checking Service
3. Government (HMT) to implement 5MLD in line with the EU text and consider the impact of the UK's interpretation of liability rules (EU – Responsibility)
4. Relevant national authorities (regulators, supervisors) to establish the means to recognise suitable schemes in line with 5MLD
5. For industry groups to research sectoral CDD needs and the case for additional identity levels to be recognised (eg online gambling)

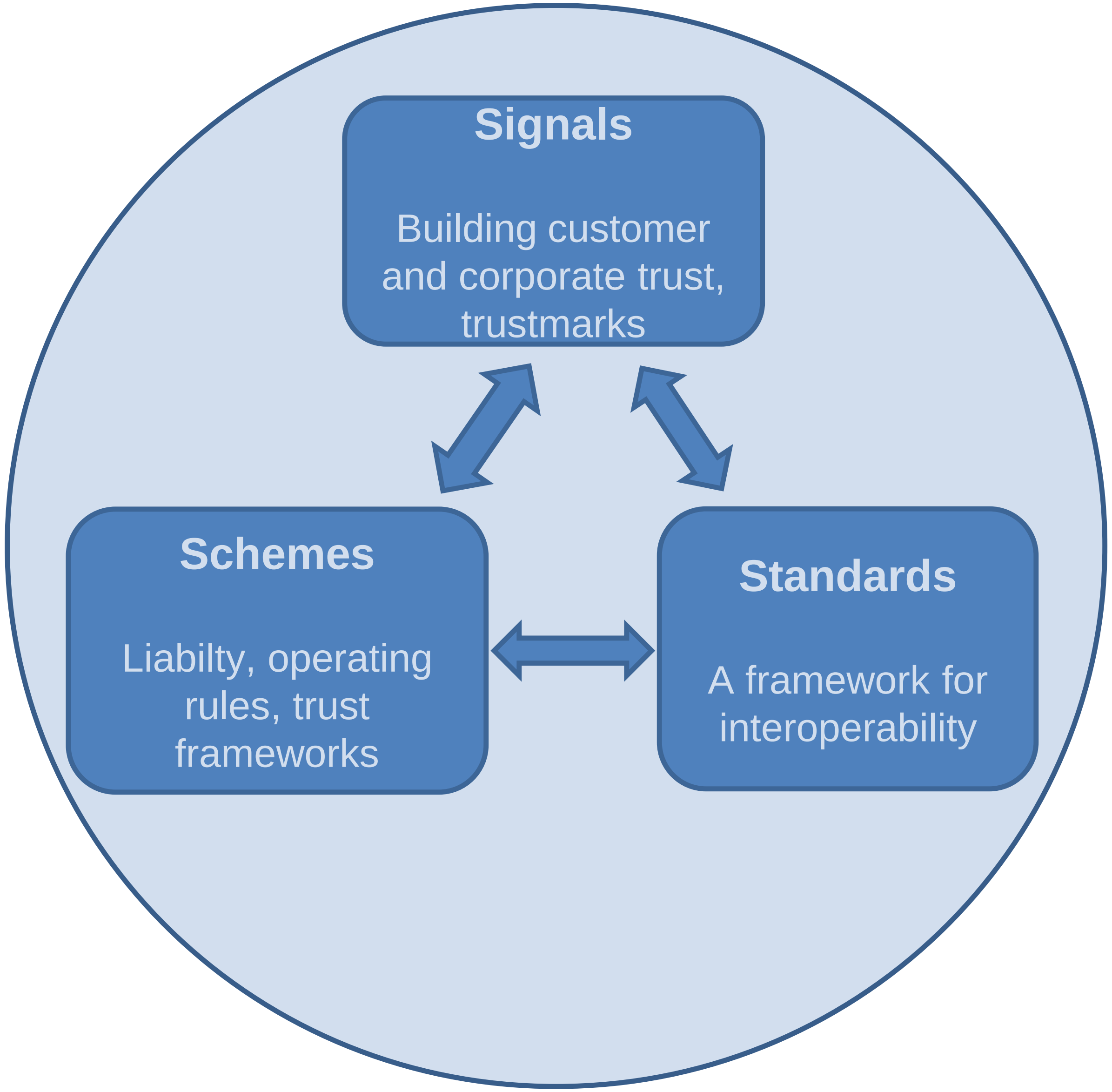
Recommendations

6. For JMLSG to align language and definitions used
7. For JMLSG to consider cross-referencing to, or adopting, the more detailed evidence weighting and criteria, and the scoring framework presented in GPG45
8. For industry and regulators to consider future application and suitability of knowledge-based checking

What Happens Next?

1. Publication of white paper and separate executive summary paper
2. Economics of Identity Event
3. Closer collaboration with techUK
4. OIX working with industry sectors
5. New project – Establishing an Interoperable Digital Identity Ecosystem in the UK. Is there a need for signals, certification and an independent authority?

Circle of Trust



Signals

Building customer and corporate trust, trustmarks

Schemes

Liabilty, operating rules, trust frameworks

Standards

A framework for interoperability

Establishing an Interoperable Digital Identity Ecosystem in the UK.

Is there a need for signals, certification and an independent authority?

Hypothesis:

In an emerging market of interoperable digital identity schemes, relying parties, IdPs and citizens/consumers/users will need assurances that any one scheme conforms to a known level of trust.

That level of trust can only be assured through appropriate signals and certification, encapsulating such matters as legal and regulatory compliance, consumer protection, dispute resolution, recompense, approved standards, and certification processes.

The acts of determining signals and issuing certification is best governed by an independent authority.

Establishing an Interoperable Digital Identity Ecosystem in the UK.

Is there a need for signals, certification and an independent authority?

Peer Review Group

- Government departments
- Regulators and industry supervisors
- Trade associations and relying parties
- Certification authorities

Project Team

- Providers – identity, hubs, security, etc

Establishing an Interoperable Digital Identity Ecosystem in the UK.

Is there a need for signals, certification and an independent authority?

High-Level Objectives:

1. To understand the guiding principles that underpin risk mitigation and build trust
2. To determine the key elements of the ecosystem and where these principles need to be applied
3. To review the mechanisms available to 'signal' trust (ie conformance)
4. To consider and make recommendations on how such a 'signal' could be implemented in the UK
5. Publish the findings in a white paper - September

Aligning GPG45 and JMLSG Guidance for Customer Due Diligence

to underpin the adoption of digital identity schemes

THANK YOU