etive
TECHNOLOGIES

Digital Identity Trust Scheme for the Home Buying and Selling Sector

MyIdentity

Version: 2.2

Date: August 2021

Authors: Ian Imeson & Stuart Young

About the Authors

Ian Imeson: Ian is an independent consultant and expert in the development and implementation of Digital Identity solutions. Ian completed a research whitepaper in 2020 into digital identity and the home buying and selling transaction.[1]

Ian was part of the Government Digital Service that developed Gov.uk/Verify and went on to design and develop the identity assurance solution that supported the Royal Mail and GBG offerings on Verify. Ian also has extensive experience of European digital identity schemes having consulted for an extended period as a Principal Identity architect for a European preeminent digital identity and signatures provider. Previous work includes the development of an internal digital identity trust framework for UK government as part of the National Cyber Security Centre.

Stuart Young: Stuart is MD of Etive Technologies, a digital identity and property data technology company who have been working in identity since 2014, with Gov.uk/Verify. Etive worked with the Government Digital Service, Tower Hamlets Council, Hackney Council, Birmingham City Council, Open Identity Exchange (OIX) and the DWP on identity verification for thin file customers, linked to the introduction of Universal Credits. This involved using the Etive product, a Digital Log Book™. These projects resulted in two project white papers; Etive Local Authority Verify (Alpha)[2] and Micro Sources of Data (Discovery)[3].

Etive are also the leading UK supplier of Property Log Book™ and Home Log Book™ for residential properties since 2007 for new home builders, local authorities and social landlords.

[1] A Digital Identity Trust Framework and Home Buying & Selling

[2] OIX - Site Content - Page - Projects (openidentityexchange.org)

[3] https://openidentityexchange.org/projects?action=view&Project=372

Contents

Summary of Key Changes

1. Glossary

Personal Data StorePersonal Data Store (PDS)

A Personal Data Store enables people to store, manage and share their information in a highly secure and structured way. A PDS is sometimes referred to as a Personal Data Store or digital log book. A PDS can provide a mechanism or process that securely allows an identity owner to store their identity data/certificate, which also provides mechanisms for the identity owner to be able to consent to sharing the data/certificate with third-parties.

Within the Scheme a PDS is owned by the consumer who is then able, with consent, to share their information and identity certificate with Service Providers held in their personal digital log book. Other data might be stored in their Personal Data Store that a Service Provider might need to see, such as a copy of a passport or driving licence.

Identity Service Provider (IDSP)

A provider of identity verification services. In the context of this Scheme, they well be certified to provide identity verification to specific levels of assurance specified by government standards. Sometimes referred to as an Identity Service Provider (IDSP).

Level of Confidence (LoC)

The Governments standard for verifying identities digitally defines four Levels of Confidence, Low, Medium, High and Very High. The LOC relates to how much trust can be placed in the identity proofing process. The higher the Level of Confidence the more trust can be placed in the identity. This scheme will define the Level of Confidence required to meet the Money Laundering Regulations for identity verification part of customer due diligence. LOC was previously referred to as Level of Assurance within GPG45, going forward the Scheme will align terminology with GPG45.

Property Log Book (PLB)

A property log book is a digital record of a property that once created stays with the property for life. A property log book "is a common repository for all relevant building data" (Definition of the Digital Building Logbook: European Commission: J Volt & Z Toth, July 2020)

Service Provider (SP)

The organisations providing services in the home buying and selling process:

Estate Agents

Solicitors

Lawyers

Conveyancers

Mortgage Brokers

Mortgage Lenders

Financial Advisors

Property Log Book providers

Other organisations that require identity verification as part of the process.

The SPs will trust IDSPs certified by the Scheme to provide information that may be regarded as obtained from a reliable source, which is independent of the person whose identity is being verified.

The UK Government Digital Identity & Attribute Trust Framework (DIATF) refers to this role as a Relying Party. We have chosen to rename this as the term relying party could be seen to reference reliance as defined within the money laundering regulations.

Trustmark

A trustmark is a means of identifying IDSPs for consumers, home buyers and sellers and Service Providers that are participants of this Scheme and have been certified for the provision of identities. The Scheme will align with the government DIATF Trustmark.

Consumer

A consumer, in the context of the Scheme, is the identity owner who chooses to share their proof of identity with Service Providers.

Pilot Phase

MyIdentity scheme will initially operate in a pilot mode. It is expected that the Pilot Phase will start in July 2021 and run until September 2022. Live transactions are expected to begin in October 2021.

2. SOURCE LEGISLATION, FRAMEWORKS AND STANDARDS

The Money Laundering and Terrorist Financing and Transfer of Funds (Information on the payer) Regulations 2017.

The relevant part of the regulation, Part 3 Customer Due Diligence, can be found here

The Money Laundering and Terrorist Financing (Amendment) Regulations 2019

The regulation can be found here. The significant change is **Amendment of Part 3: customer due diligence.**

The UK digital identity and attributes trust framework.

Identity proofing and verification of an individual This is also referred to as Good Practice Guide (GPG) 45.

Using authenticators to protect an online service. This is also referred to as Good Practice Guide (GPG) 44

ETSI TS 102 778-1 - PAdES Overview - a framework document for PAdES

3. CONTEXT TO THE PROJECT

This project will develop a digital identity trust scheme (DITS) for the home buying and selling sector, aligned to the eventual UK Digital Identity and Attributes Trust Framework that is being developed by the Department for Digital, Culture, Media and Sport (DCMS). The development of the Scheme, known as MyIdentity, will allow the digital identity of a home buyer/seller to be verified once and then be shared by the consumer used throughout the rest of the sales transaction, based on consent.

The DCMS Digital Identity and Attributes Trust Framework's objective is to ensure a standard for identity verification that can be applied across the whole UK economy. Working under this Framework, sectors across the economy are able to develop an appropriate Scheme that will meet its own sector specific needs if they wish to. This model will facilitate interoperability between schemes and ensure that minimum standards are met.

This Scheme is for the complete home buying and selling process/transaction and has active involvement from all key stakeholder groups including estate agents, conveyancers/lawyers, mortgage intermediaries, mortgage lenders, new home developers and identity providers serving the market.

The Scheme, by following GPG45 guidelines, is working to align with DCMS policy objectives and certifying identity providers (IDSP) adherence to the standard, allows IDSPs to support many methods of identity verification and provides certainty for all service providers, whilst ensuring inclusivity for consumers. The Scheme is working to ensure inclusivity, especially for digitally excluded people or those considered to be 'thin file' e.g. those who lack a digital footprint or credit file.

4. INTRODUCTION

The Home Buying & Selling Digital Identity Trust Scheme (MyIdentity) will allow participants in the Scheme to trust an identity proof provided by 3rd party Identity Providers (IDSPs), who are subject to audited certification and regulation.

Enabling trust of these certified 3rd parties will mean that consumers, buyers and sellers, are only required to prove their identity once throughout the buying and selling process. It will allow this certified identity verification to be shared with all the relevant Service Providers, following consent by the consumer.

The Scheme details how an identity can be digitally proven following the government's GPG45 standard, whilst meeting money laundering regulation (MLR) customer due diligence requirements.

To support a diverse ecosystem of participants in the Scheme, and integration with organisations that have only limited digital capability, the Scheme does not mandate technical integration between participants. To this end, the digital identity proof is a secure digital Identity Certificate that can be shared, simply and securely, with Service Providers.

The Scheme provides a technical integration specification for IDSPs to deliver the identity certificate to a person's 'Personal Data Store', referred to in this document as a digital log book (DLB). The Scheme will support and manage the provision of a DLB, but the Scheme does not mandate the use of the Scheme's DLB, as other appropriate Personal Data Stores can be used. The Scheme mandates that the identity certificate should be held in a Personal Data Store provided by an IDSP, MyIdentity or other Service Provider.

The DLB and the Identity Certificate can be linked to a property's property log book, using the technical specification for integration. This enables a property to have a high Level of Confidence of ownership and the linking of an identity to a property.

4.1 About this Document

This document defines what the Home Buying and Selling Digital Identity Trust Scheme is and what is required of the participants in the Scheme.

The contents of this document will form the basis of the contract between the Scheme, Service Providers and Identity Providers. A separate legally binding contract between the Scheme and Identity Providers will be instigated where there will be a binding handbook for Service Providers.

5. About the Home Buying & Selling Digital Identity Trust Framework

5.1 Purpose

The Scheme provides a framework to enable Service Providers (SPs) to use a proof of identity provided by certified Identity Providers (IDSPs) and meet their obligations under Customer Due Diligence (CDD). The objective being to identify individuals as detailed within The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, which sets out the amendments to the 2017 regulation.

This Scheme will not remove an organisation's responsibility to undertake a risk assessment for all transactions. The Scheme will require that all customer identities are verified to the GPG45 Level of Confidence (LOC) Medium. This LOC meets the requirements of The Money Laundering and Terrorist Financing and Transfer of Funds (Information on the payer) Regulations 2017. Where Enhanced Due Diligence (EDD) is required the necessary checks such as Source of Funds and Source of Wealth are outside the scope of the Scheme. The LOC, Medium, required by the Scheme is equivalent to the level of IDV required by HMLR Safe Harbour

5.2 Guiding Principles

The Scheme will be guided by a set of principles that were used to develop the Scheme and will inform its on-going development. The Scheme will be fully compliant with the eventual DCMS Trust Framework and will be part of the DCMS Alpha Test.

5.2.1 Trust

Service Providers will be able to trust in the identities verified by IDSPs, who are certified by the Scheme. SPs will be able to request evidence as required. Consumers, IDSPs or the Scheme will provide evidence on demand to Service Providers where they have not previously requested it as additional to the Identity Certificate. If the SP determines that there is a need for enhanced due diligence, requiring additional information such as Source of Funds / Source of Wealth, this will be the responsibility of the SP. The Scheme is not responsible for the quality or otherwise of any such additional information.

Regulators, who recognise the Scheme, accept that the use of participant IDSPs by their regulated entities for the purpose of identity verification as part of the CDD obligations can trust and use the proof of identity.

5.2.2 Data Privacy

The Scheme will align to the data privacy requirements of the UK DIATF.

There are additional Scheme specific principles. Consumer's data privacy must be maintained at all times, and data sharing will be for specific purposes, complying with data minimisation objectives. The Scheme will require that all parties adhere to the requirements of GDPR.

Sharing of proofs of identity will be controlled by the owner of that identity, the consumer.

Where there is a direct relationship between a SP and an IDSP, that is governed by the Scheme, IDSPs must ensure that consumer consent is gained and recorded for the sharing of the evidence as well as the identity certificate.

Identity evidence that has been stored to meet regulatory guidelines must be available to any regulatory authority for investigation on request.

5.2.3 Transparency

The processes used by IDSPs to prove an individual's identity must be transparent to the consumer and the Service Provider.

This process must be subject to proof of process during the certification process.

Where an IDSP fails to prove the identity of an individual they must not reveal to the consumer why the identity verification process has failed. This is an anti-fraud measure as a fraudster could use this information to be successful in future fraudulent attempts. The individual will be informed that their identity cannot be proven and referred back to the Scheme for information on how they should progress. A process has not yet been agreed on how to deal with these cases.

5.2.4 Value for Participants and Consumers

The scheme is designed to not restrict consumer or participant choice. The home buying and selling ecosystem is characterised by wide variety of estate agents (20,000+), solicitors, conveyancers and lawyers (3,900+), financial intermediaries (5,000+) and mortgage lenders (100+) and participation in the scheme should not cause this to change and will support a wide range of IDSPs. These are approximate figures and for guidelines only.

5.2.5 Consumer Protection

It is expected that the Scheme will enhance consumer protection as a direct result of a reduction in potential property and mortgage fraud. The implementation of a standards-based method of identity verification will directly reduce identity fraud, and this will be coupled with additional scheme wide anti-fraud measures.

5.2.6 Inclusivity

The Scheme is intended to be technology agnostic to ensure that no sections of society are excluded from participation.

The Scheme will also enable professionals and organisations with a low level of digital capability to adopt and utilise the Scheme and accept the Identity Certificate.

5.3 Scheme Management

The Scheme will be run during the Pilot Phase, with a Governance team made up of representatives from stake holder groups - Government, IDSPs, estate agency, legal and financial services. See **Section 10. Governance** for further information on the Governance structure.

The Scheme will be operated by Etive Technologies Ltd.

6. TRUST

6.1 Risk Assessment

The Scheme does not replace an organisations responsibility to carry out a risk assessment for every transaction. The organisation remains liable for undertaking their own due diligence. However, changes to the Money Laundering Regulation[4] (MLR) directly addresses the use of 3rd parties to undertake identity verification and allows their use with some constraints, see below.

The Scheme will provide identity verification at a GPG45 Level of Confidence that meets the requirements of the Service Providers and their regulatory obligations including AML. This is currently a **Medium Level of Confidence** (LOC). The Scheme will be responsible for ensuring that its requirements continue to meet regulatory requirements as and when these are updated.

If the risk assessment dictates that enhanced due diligence is required, then additional checks remain the responsibility of the SP. The additional requirements for enhanced due diligence do not require a heightened level of identity verification but additional separate checks such as Source of Funds / Source of Wealth and additional fraud checks.

6.2 Trusting an Identity Provider

MLR legislation supports the use of 3rd party identity providers for identity verification but specifically requires that the 3rd party meets certain conditions. The Scheme meets this requirement by requiring 3rd party providers to undertake identity verification following a Government identity standard and to be part of a Government or industry trust scheme that requires certification of IDSPs.

This Scheme implements both these requirements. The scheme has adopted the Government's identity verification standard, GPG45, as the basis of its identity verification requirements for IDSPs. The Government, through the Department for Digital, Culture, Media and Sport (DCMS), is developing a UK Digital Identity and Attributes Trust Framework. This Scheme will be compliant with the requirements of the DCMS Framework and therefore meet the requirement to be a Government recognised scheme. The scheme has the support of the Ministry of Housing, Communities and Local Government (MHCLG), Anti-Money Laundering Supervision (AMLS/HMRC), HM Treasury (HMT) and DCMS prior to the publication of the national framework. When the DCMS Trust Framework is fully implemented this Scheme will seek certification to the DCMS Framework.

6.3 Certification & Audit

IDSPs will be registered and required to undergo audited certification through a Government approved scheme. This ensures that trust in the IDSP is founded on the compliance of the IDSP with the rules of the scheme.

[4] The Money Laundering and Terrorist Financing (Amendment) Regulations 2019

The UK DIATF has not yet defined in detail how certification of IDSPs will be governed. Currently, only tScheme[5] is empowered through legislation to certify providers of trust services in the UK.

It is anticipated that during the pilot phase of the Scheme that the Scheme will define and moderate self-certification for the IDSPs taking part.

It is anticipated that once the DCMS has defined its certification framework that the Scheme will adopt this framework.

IDSPs will be certified following the DCMS Trust Framework Certification[6] . During the DCMS Framework Alpha pilot phase IDSPs will be required to undergo certification under the Alpha Certification process. In addition to this, the Scheme details additional requirements which the Scheme will require proof from the IDSP that they are meeting these additional requirements.

6.4 Scheme Trustmark

The DCMS UK DIATF will establish a Trustmark that shows the compliance to the scheme rules. IDSPs who are certified to the Scheme will be able to show the DCMS Trustmark. The Trustmark will enable Service Providers and consumers to readily identify compliant IDSPs and use their services with trust and reliance. The Scheme will also provide a website, www.myidentity.org, that enables consumers and SPs to check the ongoing compliance of IDSPs.

[5] tScheme is the self-regulatory body for electronic trust service approval in the UK | tScheme

[6] DCMS Trust Framework Certification

7. Roles, Responsibilities & Obligations

The following roles have been defined within the Scheme and detailed below:

- the Scheme Governing body
- Identity Provider
- Service Provider
- Attribute Provider
- Certification Body(s)
- Personal Data StorePersonal Data Store

7.1 The Scheme

7.1.1 Role

The Scheme is currently limited to transactions between individuals (natural persons) and new build sales to individuals. New build sales have been included here although they are sales between a company and individuals, as the transaction does not have the complications of ownership typical of company transactions. This also extends to individual customers who may be providing funds for house purchase on an individual basis.

The Scheme does not currently cover transactions involving sale by or to companies or trusts, except for new homes builders and developers.

It is anticipated that the Scheme will be extended to cover transactions between corporate and trust entities in a future phase, as and when Scheme members deem appropriate as well as providing scope for the private rented sector (PRS) and even possibly the public/social rented sector.

The Scheme manages the registration and update of certification status of IDSPs and all SPs using the scheme.

7.1.2 Scheme Operator

The Scheme will be operated by Etive Technologies Ltd, with an independent governance board, that will be responsible for the rules of the Scheme.

7.1.3 Responsibilities

The Scheme will ensure that only IDSPs who are registered and certified are using the DCMS trust mark. The register of certified IDSPs will be open to inspection by all members of the Scheme and consumers.

The Scheme will monitor developments in identity verification technologies and standards, developing threats and changes to legislation to ensure the Scheme rules are updated as required.

The Scheme will restrict access to archived identity evidence, only allowing access to regulatory and criminal authorities where an investigation has been initiated.

The Scheme will ensure there is a digital log book/Personal Data Store service available to all consumers, where IDSPs and SPs do not wish or are unable to provide this service. The Scheme may wish to charge IDSPs for this service.

The Scheme will provide an archive service, data vault, for the secure offline storage of all identity evidence where IDSPs do not commit to store identity evidence for the required period. This service is an escrow type service where access to evidence stored in the Scheme's data vault, or an IDSPs archive, is governed by the Scheme and will only be available where the transaction is subject to investigation.

Consumers will not be able to request the deletion of data from the data vault as result of the right to be forgotten. This information is being stored in line with a number of regulations, see **8.9 Audit & Data Retention**, as a result this data must be stored. When the final requirement for data storage has been exceeded the data will be deleted.

Complaint, Redress and Escalation Process

The Scheme will provide a complaint handling process for consumers and Scheme members, available through the Scheme website.

7.2 Identity Service Provider (IDSP)

7.2.1 Role

Identity providers will provide an identity verification service that meets the requirement of the Scheme. The DIATF recognises 3 types of IDSP. IDSPs operating within the rules of the Scheme will provide an identity verification services (which offers a point in time verification, and the user may or may not have an account). The Scheme does not preclude IDSPs from engaging with the consumer to change their role to either of the other definitions. The Scheme does not mandate the methods that an IDSP uses to verify identity and, in line with its principles, seeks diversity of providers to enable as many consumers as possible to be able to prove their identity, digitally. The methods used must conform to GPG45 LOC Medium.

IDSPs must output the results of the verification process in the format required by the Scheme and support the form of Personal Data Store (PDS) required by the Scheme. The Scheme encourages IDSPs to provide consumers with a PDS as part of their service. However, where an IDSP does not wish to provide this service the Scheme undertakes to provide a Digital Log Book (DLB) to store their identity information. The Scheme may choose to charge an IDSP for this service.

7.2.2 Responsibilities

1. IDSPs must verify identities following the rules of the Scheme which are detailed in **Section 8. Assuring Identities.**
2. IDSPs must be certified to the scheme rules to provide IdV checks.
3. IDSPs must be certified within the rules of the DCMS Framework and the additional requirements of this scheme.
4. During the pilot phase implementation of the Scheme IDSPs will be required to follow the DCMS Alpha certification process. The additional requirements of the Scheme are detailed in this document and IDSPs must provide evidence and documentation supporting their self- certification prior to commencement of the pilot. The Scheme will be responsible for assessing the documentation and approving IDSP inclusion in the Pilot. Only certified IDPs will be shown on the Scheme register and allowed to use

the DIATF Trustmark and use Scheme branding. The Scheme will ensure interoperability with other Schemes through the DIATF, which will enable ISPs to use the certification to provide identities to other sectors. IDSPs must ensure that the evidence used, and the data captured to verify the identity, is retained as defined in **8.8 Audit & Data Retention**. The Scheme will provide an archive facility to enable secure storage of evidence, where IDSPs are unable to commit to secure storage. The Scheme may charge IDSPs for this facility. This facility will only be provided during the Pilot Phase if there is sufficient demand from SPs and IDSPs.

5. IDSP's must be registered with the Information Commissioner's Office to store personal data.
6. IDSPs must allow consumers to choose an alternative Personal Data Store PDS if they choose to do so. This requirement will not be enforced during the Pilot Phase.
7. Where an IDSP commits to maintain its own evidence archive they are required to contractually commit to the transfer of that data to the Scheme in the event of the IDSP ceasing to trade.
8. IDSPs must have implemented full information security controls as detailed within the DIATF.

7.3 Attribute Service Provider (ASP)

ASPs must comply with the DIATF and be certified under the Scheme. Attribute service providers collect, create, check or share pieces of information that describe something about a user. Attribute service providers can share their attributes with relying parties and identity service providers, when they must have the user's agreement.

If an identity service provider is collecting, creating, checking or sharing attributes as part of their service, they will also be an attribute service provider. They will need to follow the rules for both roles.

Attribute service providers must be able to assess the quality of the attributes they keep.

In relation to the Scheme, ASPs may provide attributes such as PEPs, SoF/SoW, ID Fraud reports.

7.4 Service Provider (SP)

7.4.1 Role

SPs are consumers of the identity certificate. As members of the Scheme, SPs will have access to the proof of identity, identity certificate storage in the chosen store of the buyer or seller, the Scheme's digital log book or IDSPs service.

SP's can view the Identity Certificate or download a copy of the certificate. SPs may also request identity evidence.

7.4.2 Responsibilities

1. If a SP downloads a copy of the identity certificate, they must meet the Scheme rules for secure storage and access management of the certificate. This includes obtaining consent from the owner of the identity for the use of the certificate.

2. If a SP chooses to download an identity certificate, they must implement security controls in line with GDPR and use of personal identity data.
3. SPs must maintain fraud controls in line with legislation including suspicious activity reporting.
4. If an individual is acting as a "trusted person" or with delegated rights the identity of the individual must be verified as normal. It is the responsibility of the SP to determine that the individual has the right to act on somebody else's behalf.

7.5 Personal Data Store Provider (PDSP)

7.5.1 Role

A PDS provider delivers a service for consumers to store their identity certificate which they use to prove their identity to SPs.

An IDSP may also be a PDS provider, for example, as a mobile application.

The consumer has sole control of their PDS, and they determine who is able to access the Identity Certificate held in their PDS, irrespective of supplier.

The consumer can use their PDS provided to them from another Scheme, which includes their IdV.

The Scheme will provide for 3rd party PDSPs for consumers where the IDSP does not provide a PDS.

7.5.2 Responsibilities

1. The Provider must provide the consumer with secure access to their PDS, in line with requirements of GPG44 strong authentication.
2. The consumer must be able to manage consent to access their Personal Data Store. They must be able to give consent and remove consent.
3. The provider must provide secure access to authorised SPs to any Personal Data Store they have been given access to.
4. The provider must enable the move of an Identity Certificate to another provider if requested by the owner. This requirement will not be enforced during the Pilot Phase.
5. The provider must enable the owner to delete an identity certificate and close their Personal Data Store on request.
6. Personal Data Store providers must ensure that all data held in a customer's Personal Data Store is encrypted, and that the customer holds the keys.

7.6 Certification Body

7.6.1 Role

DIATF will determine the certification framework and the Scheme will align to this. DCMS have now published their certification guide[7]. The Scheme will align fully with the DCMS Trust Certification Guide.

7.6.2 Responsibilities

1. To be defined by DIATF.

7.7 Identity Owner (Consumer)

7.7.1 Role

The home buyer or seller, an individual or natural person, is the owner of the verified identity. Within the Scheme they are the owner of their Personal Data Store and the data held within it.

7.7.2 Responsibilities

1. The consumer is not responsible for any functional component of the Scheme.
2. The consumer is responsible for managing access to and consent to view their Identity Certificate and allowing identity evidence to be shared with SPs.
3. The consumer is responsible for safely keeping their security details used to access their Personal Data Store, such as a password or if an app on their mobile phone ensuring that their mobile phone is password protected.

[7] https://www.gov.uk/government/publications/uk-digital-identity-attributes-trust-framework-updated-version/trust-framework-certification

8. Assuring Identities

8.1 Money Laundering Statutory Requirements (MLR)

The Scheme addresses the obligation of SPs involved in home buying and selling transactions to identify individuals as part of their responsibilities for Customer Due Diligence (CDD) under MLR legislation.

CDD is a risk-based process and requires that a risk assessment is carried out for each transaction. This Scheme does not remove the obligation of SPs to undertake their own risk assessment for each transaction.

Under MLR, identity verification must meet an equivalent level to GPG LOC Medium or higher. The Scheme uses the UK Governments GPG45 guidance for identity verification. How the requirements of the MLR legislation are met by GPG45 is detailed below.

8.1.1 Trust Using 3rd Parties for Identity Verification

The 2019 amendment to the Money Laundering Regulation specifically recognises the role of 3rd parties in IDV and provided guidance on the conditions required to meet the SP's obligations.

An extract from The Money Laundering and Terrorist Financing (Amendment) Regulations 2019 is provided below:

> *"(19) For the purposes of this regulation, information may be regarded as obtained from a reliable source which is independent of the person whose identity is being verified where—*
>
> *(a) it is obtained by means of an electronic identification process, including by using electronic identification means or by using a trust service (within the meanings of those terms in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23rd July 2014 on electronic identification and trust services for electronic transactions in the internal market (11)); and*
>
> *(b) that process is secure from fraud and misuse and capable of providing an appropriate Level of Confidence that the person claiming a particular identity is in fact the person with that identity."*

The DCMS UK National Digital Identity and Attributes Framework is intended to meet the requirement in (a) above and this Scheme by being compliant with the DCMS Framework will meet this requirement.

In addition, the Scheme will meet the requirement in (b) above by:

- Specifying the specific GPG 45 level, LOC Medium or Higher, which meets the requirement of (b).
- The Scheme will require an initial PEP check and require IDSPs to undertake additional mitigation to ensure the person being checked is either the PEP or a different person (many PEP positives are false positives and require mitigation to proves the case). This ensures that individual risk will be addressed.

- GPG45 specifies profiles of what evidence is required to reach each level of proof. Some of these profiles do not require PEP or Fraud checks. This Scheme requires t PEP checks and mitigation in all situations.
- IDSPs will be audited and certified to the scheme meeting the requirements of (a) to be part of a trust scheme.

8.2 AML – GPG45 Equivalence

See Appendix 1. For a detailed comparison of MLR requirements, supervisor guidelines and GPG45.

8.3 Identity Verification Standard GPG45

The UK Government has defined how identities are assured in the GPG45 standard, which is now detailed in two documents:

1. *How to prove and verify someone's identity* [8]- details what methods, documents and data sources are available and how they score. Achieving a defined level of IdV is dependent on the identity evidence score. Identity profiles are then used to determine if a range of evidence meets the requirement for a specific level of proof and verification. The Scheme requires a LOC of Medium to meet the MLR requirement.
2. *Identity profiles*[9] – details how each assurance level may be met using the methods, documents and data sources detailed in *How to prove and verify someone's identity.*

Full details can be found in these documents and these form part of the rules of the Scheme for IDSPs. Appendix 2 is an extract of some of the information from these documents. GPG45 45 provides guidance on how to prove identities digitally and also how you can prove identities to the same standard manually. it also details how manual checks should be undertaken, where these are used.

In addition to the specific profile requirements of GPG45, there are additional Scheme specific requirements that must be completed. Each of these specific requirements can be a component of and count to the achievement of a GPG45 profile. However, if the profile being used does not include any of these specific requirements, they must be completed in addition to the profile checks.

1. For all checks a verified self-image will be required using anti-impersonation measures.
2. A basic PEP and sanction check must be completed for every individual. These are a key requirement for the risk assessment and may inform whether an enhanced check is required. These checks do not need to be independent of the IdV check and can contribute to completing the GPG45 profile.

[8] How to prove and verify someone's identity - GOV.UK (www.gov.uk)

[9] Identity profiles - GOV.UK (www.gov.uk)

Note: From an interoperability perspective, these requirements, if not included in the profile, can be considered as additional attributes needed for the home buying and selling transaction.

8.4 Additional Required Attributes

To meet AML requirements the Scheme requires the additional checks to be completed. Some GPG45 – LoC Medium profiles require these attributes. Where the profile does not require these, it is a Scheme requirement that these are provided.

Proof of Address

IDSPs must **confirm the address the consumer provides** using an authoritative source.

Politically Exposed Person

The name of the consumer must be checked against an authoritative list of Politically Exposed Persons. It is expected that the IDSP will seek to mitigate any potential matches. The IDSP should be able to rule out name matches where there is no other matching criteria e.g. address, date of birth.

ID Fraud

An ID Fraud check is required. Assurance

Assurance is provided to the Service Providers by the identity certificate. The identity certificate documents the Level of Confidence achieved, provides a matching data set of biographic information and details the checks undertaken and results obtained.

The MLR in respect of identity evidence is open to interpretation. The Scheme interprets the requirement such that SPs do not need to see the evidence to meet their obligation, however some MLR supervisors determine that SPs are still obligated to see evidence to meet their obligation. As such, the Scheme supports all SPs who require to see and store the identity evidence and enable them to meet their requirements and obligations.

8.5 Fraud Controls

The Scheme has worked with Cifas to enable IDSPs to become members of Cifas. IDSPs will be able to undertake ID Fraud checks against the Cifas data source. IDSPs are free to use other sources of ID Fraud data, the scheme will need evidence of the source used and the coverage that this service provides.

Fraud in the home buying and selling process can occur in many forms. The Scheme will only deal with fraud controls relating to identity fraud. Proof of ownership is a key requirement within the transaction.

The Scheme will be fully compliant with the fraud controls that are required by the DCMS Digital Identity Trust Framework.

Fraud controls must be implemented by Identity Providers and Service Providers. IDSPs are making the identity trust decision and therefore are mainly responsible for identity fraud control.

Identity providers must implement fraud management tools that will pick up any fraud indicators during the proofing process and allow for generation of reports of potential fraud allowing for human assessment of the fraud risk.

Service Providers will be required to continue with their risk assessment and fraud management, the provision of a Scheme approved identity does not relieve the SP of this responsibility.

8.6 Suspicious Activity Reporting (SAR)

The Scheme does not take any role in SAR. SPs will continue to meet SAR requirements as they currently do. IDSPs will not have a requirement as part of this Scheme to meet SAR requirements.

8.7 Additional Attributes

If additional information is required of a buyer or seller, that is not required for IdV but is required in order to complete the transaction, then provision of these additional attributes will not form part of the Scheme.

They are documented below for understanding of the relationship with the verified identity.

8.7.1 Proof of Ownership

For Sellers proof of ownership of the property for sale is required.

Address checks can form part of IdV and therefore this check is likely to be completed alongside the IdV check and form a part of the scoring for a profile. However, the IdV check links an individual to an address but only provides evidence that an individual lives at the address it does not prove they own the property.

Proof of ownership is a specific check that must be completed and therefore may be completed later than the IdV. The IdV check informs this check as it proves the individual is who they say they are and therefore can be correlated with HMLR and mortgage information.

8.7.2 Source of Funds / Wealth

For buyers, a Source of Funds check must be completed. This form of check is not directly used within the IdV checks but completing this check can provide scoring information for the IdV check.

A source of funds check should be carried out after the proof of identity has been completed. Proof of identity is key to determining the source of funds as it proves the individual is who they say they are and therefore tightly links them to the funds.

8.7.3 Sanctions Lists

A proof of identity is checked to undertake a check against sanctions lists. A sanctions check is an eligibility check.

8.8 Audit & Data Retention

An audit record of all identity proofing transactions must be maintained by an IDSP for **6 years**.

Under MLR, identity evidence gathered as part of the proofing process must also be available for 6 years.

If IDSPs are unable or unwilling to provide storage the Scheme will provide secure data storage, and charge for this facility.

The Scheme provides a “data vault” to act as a repository for captured evidence in escrow. This facility is available to IDSPs who are unable to store evidence for such an extended period. The Data Vault is also available for IDSPs who cease to trade but have been storing evidence to ensure there is a continuing ability to store data. IDSPs who choose to store evidence records will be required to contract to move this evidence to the Data Vault should they cease to trade. Access to the evidence will be controlled by the Scheme and access will only be granted if an investigation is under way. See below, for details of how evidence will be protected.

There are additional data requirements specific to each sector these are the responsibility of the SP to ensure they meet these requirements.

8.9 Scheme Responsibilities

The Scheme is responsible for ensuring that all members of the Scheme meet any requirements over and above the certification required by DCMS. The Scheme will operate a technical infrastructure to allow the Scheme to perform as described. The technical infrastructure and consequent responsibilities are described in the MyIdentity Solution Design.

9. Using Identity Proof

9.1 Process Flows

The technical implementation of the Scheme is detailed within the MyIdentity Solution Design. Any technical information provided here is for information only and the Solution Design document takes precedence.

The diagrams below are a representation of the process flow for the home buying and selling digital identity solution supported by this Scheme.

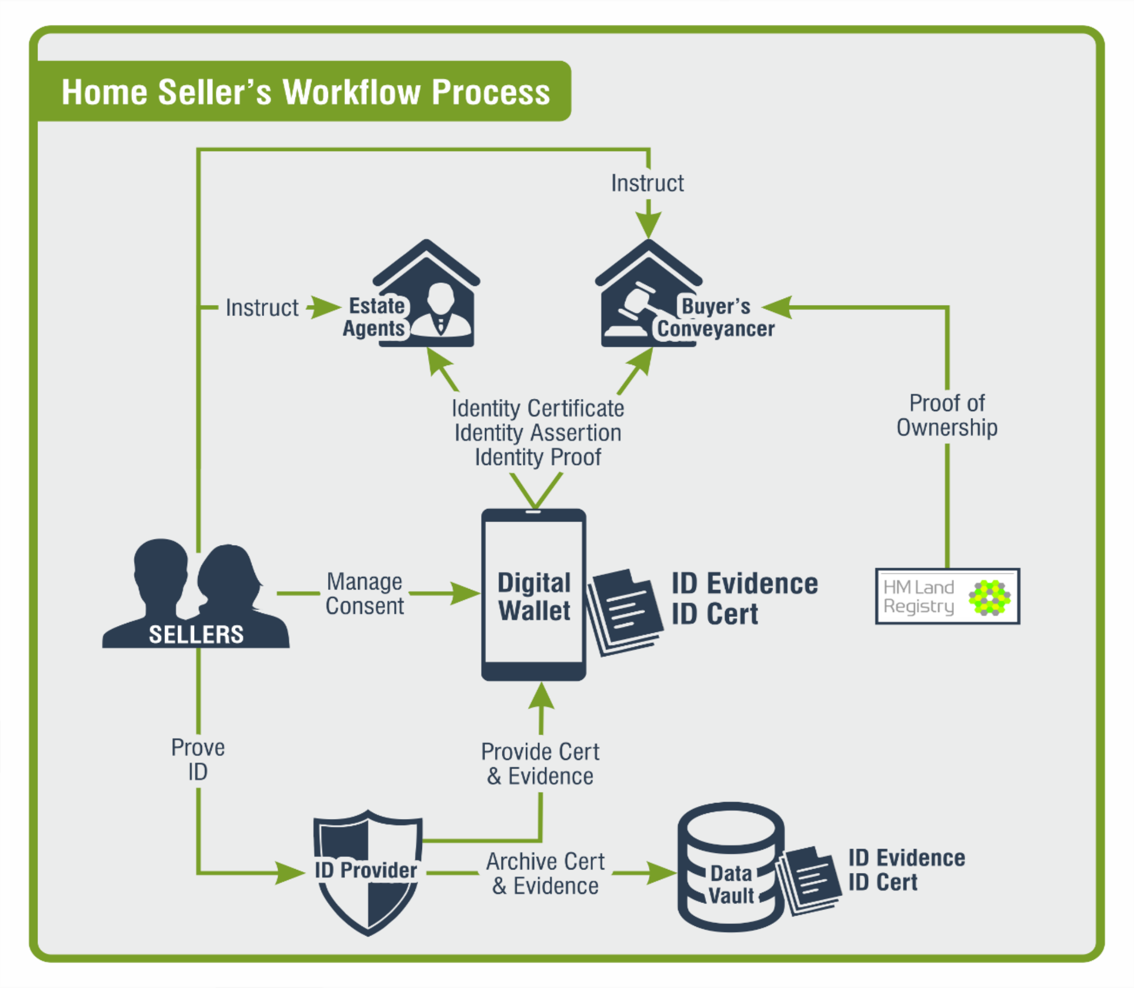


Image 1: Home Sellers Process Flow

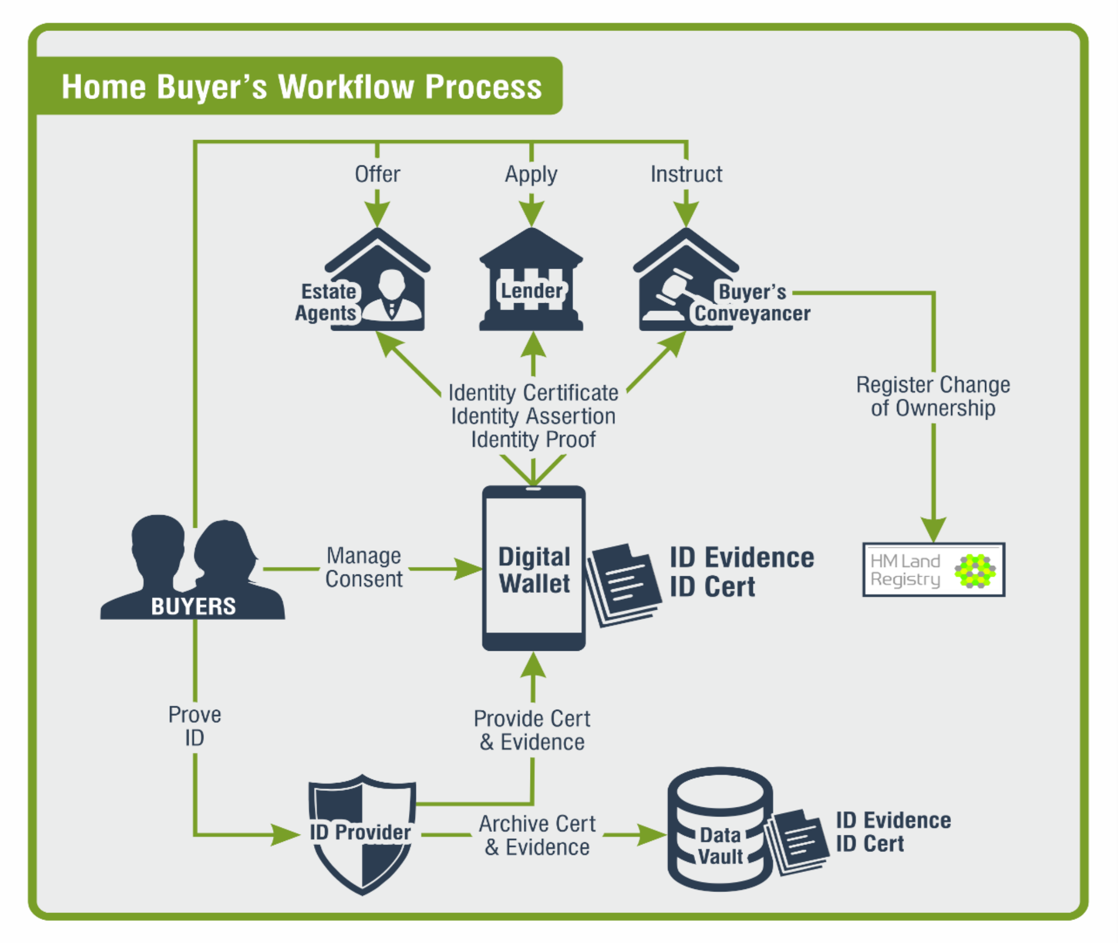


Image 2: Hone Buyers Process Flow

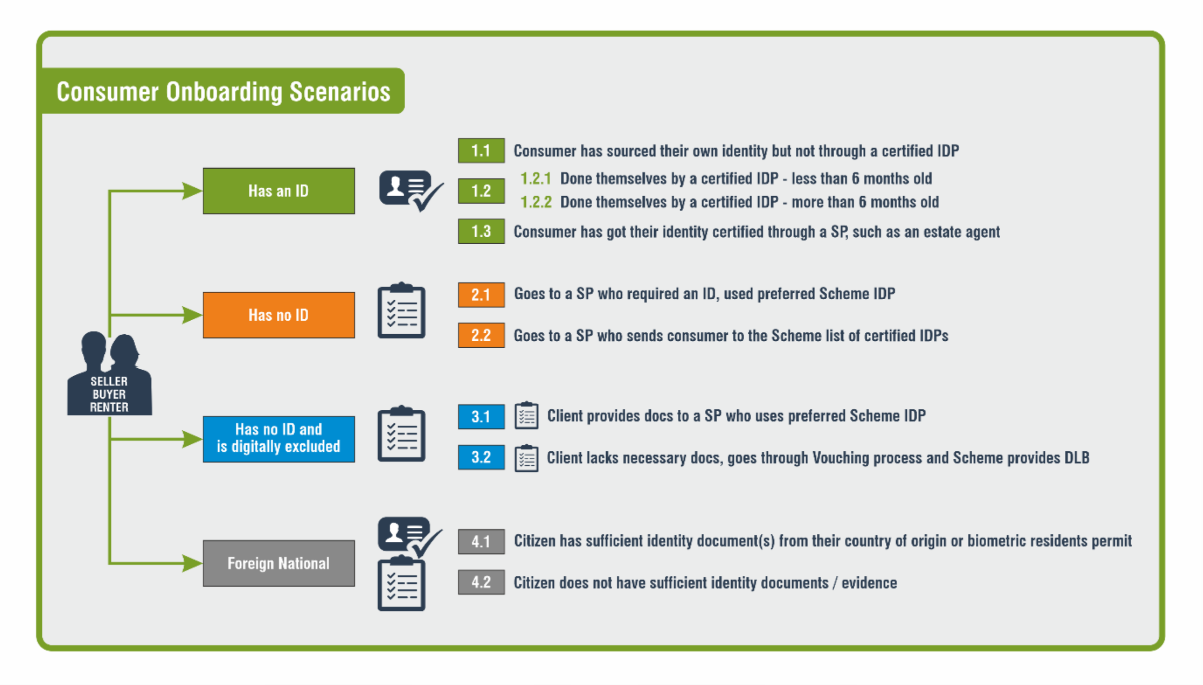
Process Steps

1. Each buyer or seller proves their identity through a certified IDSP.
2. IDSP creates Identity Certificate.
3. IDSP transfers Identity Certificate and evidence to the consumer's Personal Data Store.
4. Personal Data Store provider creates individual's personal data store and sends a link/access details to the consumer, enabling them to access and control their PDS..
5. Consumer accesses their Personal Data Store and enters details of the SP contact details and consents to sharing Identity Certificate and evidence, if required.
6. SP receives access details to the consumer's Personal Data Store and can access the ID Certificate and notes unique reference number and IDSP. If required, and allowed, the SP can download a copy of the ID Certificate and evidence.
7. Buyer's conveyancer registers change of ownership using ID certificate as proof of identity.

9.2 Consumer Onboarding

Note: How the consumer onboarding process works is still under discussion some probable routes are described below

The process flow shows the consumer using an IDSPs process directly. The consumer may be directed to the IDSP through different routes:


Consumer Onboarding Scenarios
SELLER
BUYER
RENTER
Has an ID
Has no ID
Has no ID and is digitally excluded
Foreign National

1.1 Consumer has sourced their own identity but not through a certified IDP

1.2
1.2.1 Done themselves by a certified IDP - less than 6 months old
1.2.2 Done themselves by a certified IDP - more than 6 months old

1.3 Consumer has got their identity certified through a SP, such as an estate agent

2.1 Goes to a SP who required an ID, used preferred Scheme IDP

2.2 Goes to a SP who sends consumer to the Scheme list of certified IDPs

3.1 Client provides docs to a SP who uses preferred Scheme IDP

3.2 Client lacks necessary docs, goes through Vouching process and Scheme provides DLB

4.1 Citizen has sufficient identity document(s) from their country of origin or biometric residents permit

4.2 Citizen does not have sufficient identity documents / evidence

Image 3. Possible Onboarding Journeys

9.3 Identity Certificate

The Identity Certificate is used to provide proof of how the identity was proven, it does not include the evidence that was used to prove the identity. The certificate is provided to the SP as proof that the identity was verified to the required level. In addition, the certificate provides some matching data as well as evidence of the process used.

The format of the certificate will be detailed in the Technical Specification. The Technical Specification will be developed during the pilot stage.

9.3.1 Unique Identifier

The ID Certificate will have a Scheme wide unique identifier, which is detailed in the Solution Design.

9.3.2 Validity

The DCMS Digital Identity Trust Framework supports the creation of digital identities that are not limited to transactions or duration. Once an identity is verified and the individual linked to the identity through strong authentication, the proof of identity remains valid. Periodically checks are made to see if the identity has been subject to potentially fraudulent activity which if shown requires additional checking to be undertaken.

Identities verified under the Scheme will not be limited to a single transaction or a duration. The Scheme will require anti-fraud checks at 6 monthly intervals. The IDSP will be required to undertake these checks and provide an updated certificate and evidence of the check. The IDSP may charge the consumer for these additional checks.

9.3.3 Matching Information

The certificate will contain information on the individual to ensure the identity certificate being viewed matches the individual presenting. This is not intended to support identification rather to ensure the certificate is matched with the right individual.

1. Photo – captured during the proving process
2. Names
3. Address
4. Date of Birth (DoB)
5. Telephone number
6. Email Address

9.3.4 Proofing Process Results

The certificate will identify the checks that have been undertaken and the result of those checks. This will include scoring, such as confidence scores in image matching and document scans where available and appropriate.

9.4 Identity Evidence

Identity Evidence will be stored in the Personal Data Store alongside the identity certificate. Identity Evidence will be provided to the SP when requested and consented to by the consumer.

The flow of data, identity certificate and evidence, supported by the Scheme is detailed in the Technical Solution.

During the audit process, an auditor may request visibility of evidence to support the certification process. This will be to specifically enable an IDSP to prove that for the process followed to verify an identity meets the requirements of the Scheme and that the identity certificate and identity evidence match. The terms and conditions of use of the data vault will specifically allow access for purposes of certification.

9.5 Personal Data Store (PDS)

A PDS is used to refer to the Scheme or IDSP provided Personal Data Store. The consumer must have the same control and rights to their PDS whether it is provided by an IDSP or the Scheme.

The PDS is a consent driven personal data store, owned by the person, enabling the person to store private information securely, ensuring no loss of information. Only the user can access and control their PDS but can share access to it and information from it. The PDS can store and manage any document or information the user wants. For the purposes of the Scheme the PDS will store the identity certificate and identity evidence.

The PDS can also be linked to a property log book enabling the Scheme to link a person, and their identity, to a home evidencing who they are and that they are the legal owner of the property. Their identity verifies their access to their property log book.

9.5.1 Consent

The PDS provides the functionality for the consumer to control who they share their identity certificate and identity evidence with. For the home buying and selling transaction to progress and complete SPs have a legal requirement to obtain proof of identity. This Scheme allows the consumer to control who they share this proof of identity with but once shared they do not have the ability to cause that information to be deleted. As this requirement to provide proof of identity is a legal requirement and once provided, the consumer is not in a position to consent or remove consent in GDPR terms.

9.6 Interoperability

The Scheme will conform to the requirements of the Government's UK National Digital Identity & Attributes Trust Framework. This will enable IDSPs, and the identities verified under the Scheme rules, to be used in other compliant schemes. This will ensure that those IDSPs who are certified through the Scheme will be able to provide identities into other sectors and through other Schemes without further certification.

10. Governance

Scheme Governance is still under discussion and will be subject to the requirements of the Government UK Digital Identity & Attribute Trust Framework.

10.1 Governing Team’s Responsibilities

- Maintenance of the Trust Scheme.
- Defining and maintaining Scheme standards, ensure Scheme keeps pace with technical developments and fraudster capabilities.
- Defining roles and responsibilities.
- Representation of all parties to the Scheme.
- Ensure that there is no preference given to any providers or specific technical solutions.
- Ensure the Scheme meets the requirements of all regulatory and representative bodies in the home buying and selling sector and that the Scheme is recognised in guidelines and obligations.
- Representation to Government bodies and the UK Digital Identity Trust Framework concerning digital identity and its use in the sector.
- Management of the certification process and investigation of breaches of the Scheme.
- Registration and awarding of a trustmark.
- Provision of Scheme digital log book.
- Provision of Scheme Data Vault.
- Define interoperability with other Schemes through compliance with UK National Digital Identity Framework.

10.2 Funding

- Funded from membership fees – who are members – Regulators, representative bodies, IDSPs, SP’s?
- IDSPs specifically charged for membership and supported through the provision of a trust mark, to differentiate the service.

10.3 Governance Team Members

- Chair (independent from outside industry) 1 year
- Representation from Government
- Representation from legal, financial and estate agency regulators
- Representation from legal, financial and estate agency membership bodies
- Representation from the IDSPs

10.4 Administration

- Remote working
- Light weight
- Membership administration
- Technical expertise
- Reporting every 6 months

10.5 Participation

- Open to all parties involved in the home buying and selling sector

APPENDIX 1. MONEY LAUNDERING GUIDELINES & SCHEME EQUIVALENCE

Legal Sector Affinity Group Anti-Money Laundering Guidance

Chapter 4 - Customer Due Diligence	The Scheme will provide a means to achieve obligations related to identity verification stated within Chapter 4
4.3.3 General Information - methods of verification. Verification should be completed on the basis of documents or information which come from a reliable source, independent of the customer. This means that there are a number of ways in which you can verify a client's identity including: • obtaining or viewing original documents • conducting electronic verification • obtaining information from other regulated persons • obtaining information from other reliable publicly available sources	The Scheme will set out the rules for identity verification following the government standard GPG45 ensures all requirements are met and the specific rules that will be applied by the scheme The scheme will as standard not share the evidence used to verify the identity, however a certificate will be issued which details what evidence was used to meet the Level of Confidence required.
Documents You should not ignore obvious forgeries, but you are not required to be an expert in forged documents. You may consider providing relevant employees with appropriate training and equipment to help identify forged documents	IDSPs certified under the scheme must use solutions which meet GPG45 in determining that documents are not counterfeit.

Electronic verification You should consider whether any electronic verification system you use properly establishes the customer’s identity, rather than just establishing that the identity exists. You should consider the risk implications in respect of the particular retainer and be on the alert for information which may suggest that your client is not the person they say they are. You may mitigate risk by corroborating electronic verification with some other CDD material. When choosing an electronic verification service provider, you should look for a provider who: • has proof of registration with the Information Commissioner's Office to store personal data • can link an applicant to both current and previous circumstances using a range of positive information sources • accesses negative information sources, such as databases on identity fraud and deceased persons • accesses a wide range of 'alert' data sources • has transparent processes enabling you to know what checks are carried out, the results of the checks, and how much certainty they give on the identity of the subject • allows you to capture and store the information used to verify an identity	The Scheme requires that all certified IDSPs must meet these requirements.

When using electronic verification, you are not required to obtain consent from your client, but they must be informed that this check will take place. While electronic verification can be a sufficient measure for compliance with money laundering requirements, there may be circumstances where it will not be appropriate	
4.8 Records	The Scheme will require IDSPs to maintain records to enable full reconstruction of the identity proofing and verification process, see 5.8. In addition, they will be required to store data for a minimum of 5 years or store data with the Scheme. The Scheme allows you to receive and store evidence yourself.
4.9 CDD on clients	In the first instance the Scheme will only support identity proofing and verification of natural persons. The rules of the scheme can be applied equally to UK and other nationals although it may prove more difficult to meet the scheme rules for overseas nationals particularly outside the EEA. The Scheme or GPG45 do not provide exhaustive lists of example documents that can be used, rather they provide the characteristics of documents and information sources. IDSPs will be required to provide evidence during acceptance and audit that their methods and accepted documents meet the rules of the Scheme.
4.12 Enhanced due diligence	The scheme will require PEP and Fraud marker checks to be carried out for all transactions to determine if there is a requirement mitigating activity by the IDSP. In addition, the Identity Certificate will disclose any fraud markers to enable full risk assessment. Where you determine that EDD is required you are responsible for ensuring these checks are undertaken. The Scheme does not provide for any EDD checks.

HMRC Guidelines and Scheme Equivalence

Estate agency business guidance for money laundering supervision	HBS Digital Identity Trust Scheme (DITS)
4.104 If using a service provider, you should make sure that it is reliable and accurate using extensive source data. You should consider the following criteria in your selection:	
it is registered with the Information Commissioner's Office to store personal data	The Scheme would require identity providers to register with the ICO and the scheme would specify acceptable security policy.
it is accredited to give identity verification services through a government, industry or trade association process that involves meeting minimum standards	The Scheme will comply with the Governments Digital Identity Trust Framework and will also be supported by the Trade Associations
the standards it works to, or certification, require its information to be kept up to date	The Scheme will document re-verification requirements
its compliance with the standards is assessed	The Scheme will require Identity Providers to be accredited to meet the documented standards
it uses a range of positive information sources, and links a person, through other sources, to both current and previous circumstances	The Scheme will adopt the Governments standard for identity assurance GPG45
it uses negative information sources, such as databases relating to identity fraud and deceased persons	The Scheme will require Identity Fraud checks
it uses a wide range of alert sources, such as up to date financial sanctions information	The Scheme will require PEPS and Sanctions checks to be undertaken

it has transparent processes that enable the firm to know what checks were carried out, what the results of these checks were	The Schemes rules will be fully available for all members of the scheme allowing all organisations using the scheme to understand how compliance is achieved
it can set the level of certainty as to the identity of the subject suitable for your risk assessment	The Scheme will link risk assessment to the level of identity being asserted. With levels being defined within GPG45
should be able to keep records of the information used to verify identity information or allow a download to be stored on your own server	The Scheme will require that Identity Providers complete audit trails of how an identity was assured enabling reliant parties to be able to prove a compliant process was undertaken.
if your customer due diligence records are kept on the outsourcing service provider’s server make sure that in the event of the service provider going out of business that you will continue to have access to the data for 5 years from the end of your business relationship with the customer	The Scheme will require that Identity Providers ensure full audit records are maintained for 5 years.

JMLSG Guidance and Scheme Equivalence

JMLSG Guidance on CDD	HBS Digital ID Trust Scheme
2.16 Outsourcing and non-UK processing Many firms outsource some of their systems and controls and/or processing to elsewhere within the UK and to other jurisdictions, and/or to other group companies. Involving other entities in the operation of a firm’s systems brings an additional dimension to the risks that the firm faces, and this risk must be actively managed. Firms must obtain assurance that outsourcing providers meet the standards or requirements set out in this Guidance.	Certification of providers will provide the assurance that Identity Verification undertaken by IDSPs as part of CDD will meet the standards or requirements set out. The Certification ensures that the GPG45 Level of Confidence gained meets the requirements for CDD.

2.17 Regulation 39(7)(8) Nothing in the ML Regulations prevents a firm applying CDD measures by means of an agent or an outsourcing service provider (but see paragraphs 5.3.51 to 5.3.53 in Part I, Chapter 5), provided that the arrangements between the firm and the agent or outsourcing service provider provide for the firm to remain liable for any failure to apply such measures.	The liability model adopted by the scheme supports this requirement. IDSP's have a liability to complete IdV by adhering to the rules of the scheme. This does not change the liability for the Relying Parties
5.3.52 Before using an organisation for digital identities, electronic or digital identity verification, or trust services, firms should be satisfied that information supplied by the provider is considered to be sufficiently extensive, reliable, accurate, independent of the customer, and capable of providing an appropriate Level of Confidence that the person claiming a particular identity is in fact that person. This judgment may be assisted by considering whether the provider meets the following criteria:	
it is a notified identity scheme under the eIDAS Regulation29; or it is provided by means of a trust service covered by the eIDAS Regulation30; or it provides a service as defined by eIDAS regulation or has a similar Level of Confidence as eIDAS notified schemes;	The Scheme would be the 3rd option. In addition, it would be compliant under the UK Government UK Identity Trust Framework
it is recognised, through registration with the Information Commissioner's Office (or national equivalent for EEA/EU registered organisations), to store personal data;	The Scheme would require identity providers to register with the iCO and the scheme would specify acceptable security policy.
it is accredited or certified to offer the identity verification service through a governmental or industry process that involves meeting minimum published standards;	The Scheme will require Identity Providers to be accredited to meet the documented standards

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; it accesses negative information sources, such as databases relating to identity fraud and deceased persons; it accesses a wide range of alert data sources;	The Schemes rules will align to the governments published standard GPG45.
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 reverification;	The Scheme will document re-verification requirements
arrangements exist whereby the identity provider's continuing compliance with the minimum published standards is assessed; and	The Scheme will require ongoing certification
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.	The Schemes rules will be fully available for all members of the scheme allowing all organisations using the scheme to understand how compliance is achieved
it keeps sufficient records of information used to provide its services.	The Scheme will require all participants to maintain full audit trails to allow full investigation of any particular transaction
5.3.53 In addition, an organisation should have processes that allow the enquirer to capture and store the information they used to verify an identity, and/or return a Level of Confidence that can be stored by the enquirer as evidence of the organisations' verification processes.	The Scheme will require that Identity Providers complete audit trails of how an identity was assured enabling reliant parties to be able to prove a compliant process was undertaken.

APPENDIX 2: APPLYING GPG45

Applying GPG45 is achieved using Profiles with evidence as required. The Scheme is using the Medium level of Confidence which is in line with MLR requirements for identity verification. This is extracted from The UK digital identity and attributes trust framework and this should always be directly referenced as this is under constant review and may be updated.

	Score					
Level of Confidence	Profile	Strength	Validity	Identity Fraud	Verification	Activity History
Medium	M1A	4	2	1	2	N/A
	M1B	3	2	1	2	1
*	M1C	3	3	N/A	3	N/A
	M1D	2	2	1	3	2
	M2A	2	2	2	2	3
		2	2			
	M2B	3	2	2	2	1
		2	2			
	M2C	3	2	1	3	N/A
		2	2			

	M3A	2	2	2	2	2
		2	2			2
		2				

* M1C is the profile adopted by HMLR Safe Harbour

The tables below detail the evidence that can be used and how that evidence is scored. Full detail on how to use the evidence can be found in GPG45 and this should always be referenced we are determining if an identity has been adequately checked.

Evidence Score	Strength	Validity	Fraud	Verification
2	Home Office travel document, birth certificate, education certificate, rental or purchase agreement, PASS, marriage certificate, gas or electric account	Check it is valid using an authoritative source or genuine using original documents either manually by trained personal or electronically	belongs to someone who's still alive is known by an organisation that should have a record of that person (for example an Electoral Registration Office in a local authority) is at a usual risk of being impersonated (for example a 'politically exposed person' like a politician or judge is at a higher than usual risk of being impersonated)	Make sure the person physically matches the photo on or associated with the strongest piece of genuine evidence you have of the claimed identity (you can do this in person or remotely) make sure the person's biometric information matches biometric information from the strongest piece of genuine evidence you have or an authoritative source ask the person to complete multiple 'dynamic' KBV challenges that only the claimed identity should be able to do

3	Passports, ID Cards, UK & EU Driving Licenses, Finance Account, PASS proof of age, high eIDAS ID, a bank account	Any evidence protected by cryptographic security features will have a score of 3. You must make sure these security features are genuine or confirm the evidence is valid or check the evidence has not been cancelled, lost or stolen or confirm any physical security features are genuine or check the evidence has not expired	You'll get a score of 3 if you use more than one authoritative source to do all the checks needed to get a score of 2. The sources must also be 'independent'	Either of the following in person or remotely: Make sure they physically match the photo on (or associated with) the strongest piece of genuine evidence you have of the claimed identity make sure their biometric information matches biometric information from the strongest piece of genuine evidence you have or an authoritative source of the claimed identity
4	Biometric passports, biometric ID cards, biometric residence permit	all of the following: confirm the visible security features are genuine confirm the UV or IR security features are genuine confirm the cryptographic security features on the evidence are genuine check the evidence has not been cancelled, lost or stolen check the evidence has not expired		The person will get a score of 4 if you make sure their biometric information matches biometric information from the strongest piece of genuine evidence you have or an authoritative source It must also be able to tell when someone is spoofing the system using a sophisticated artefact that's taken a lot of time, money, effort or criminal activity to create.

Activity History

	Interactions over the last 3 months	Interactions over the last 6 months	Interactions over the last year	Interactions over the last 2 years	Interactions over the last 3 years
Identity was not checked	N/A	N/A	Score 1	Score 2	Score 3
Identity was checked following a published policy	Score 1	Score 2	Score 3	Score 4	Score 4
Identity was checked following the Money Laundering Regulations	Score 2	Score 3	Score 4	Score 4	Score 4
Physical appearance or biometric information was checked against an official source	Score 3	Score 4	Score 4	Score 4	Score 4