ADVP Simple Guide to Digital Identity

Background

The ADVP is a trade association representing companies that provide electronic validation of identity documents in the UK. Its members deploy a wide range of technology solutions that are used across the public and private sectors to check millions of identity documents every year for a multitude of purposes including remote onboarding of customers or employees.

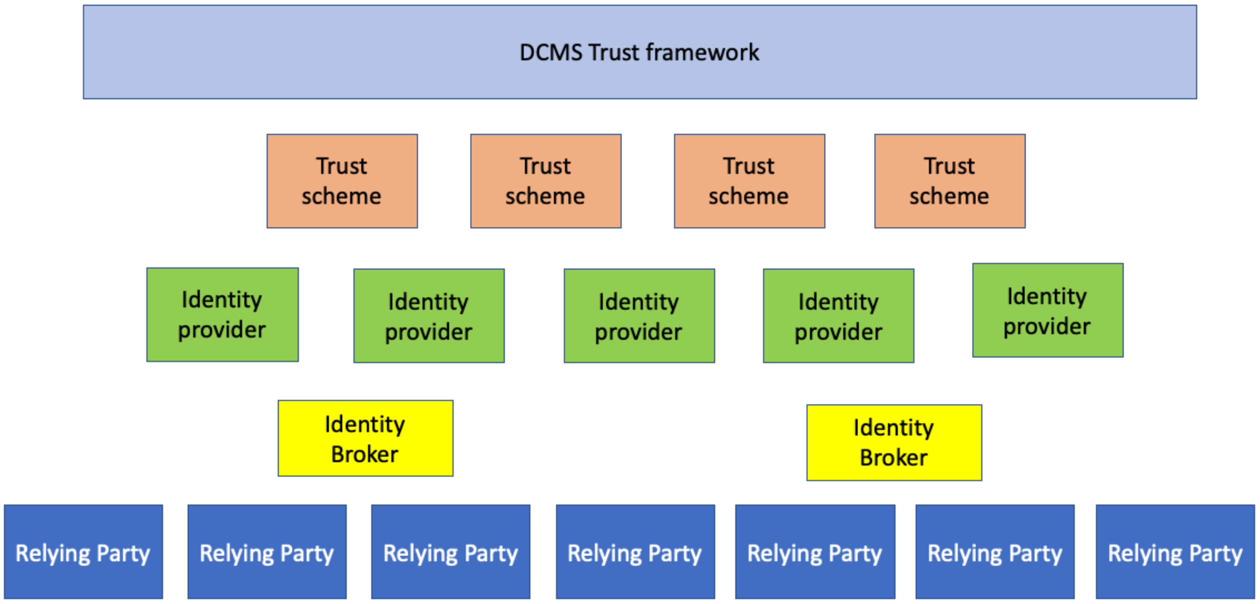
The ADVP has been engaged in much of the work around the development of a UK digital identity ecosystem – particularly through OIX and direct contact with DCMS and GDS. Whilst there are a significant number of workstreams regarding the construct of a safe and trusted digital identity ecosystem, the ADVP interest/input is focused on the electronic validation of identity documents where needed as part the creation of a digital identity.

This guide is designed to assist ADVP member companies that are not operating digital identity solutions to better understand the evolving digital ecosystem.

UK market

The release of the DCMS UK digital identity and attributes trust framework (alpha) in February 2021 has demonstrated UK government commitment to digital identity. This in turn has generated more market activity in this space. Whilst there is still a significant amount of detail to come in terms how the trust framework and the digital identity schemes accredited to it will work, it is becoming clearer what the future UK digital identity market will look like.

UK digital identity ecosystem



Definitions (OIX Glossary) – the framework

- **Trust Framework** – a set of specifications, rules and agreements often referred to as various names such as "operating regulations" or "scheme rules". The framework is likely to include a certification process by which other roles in the eco-system can be shown to be compliant with the trust framework. Each trust framework is likely to need some form of governance or oversight authority to maintain and oversee compliance with the framework.
- **Trust Scheme** – Defines an implementation of the framework for identity within the overarching rules defined by the trust framework. Implementations could be sector specific, territory specific or global-multinational. These sector specific schemes will often contain the actual implementation of local or global regulation specific to that sector. For example, a Trust Scheme might define the ID Proofing requirements set by the Trust Framework. Where the line between Trust Framework and Trust Scheme is drawn needs careful consideration.

Definitions (OIX Glossary) – authentication

- **Authentication** – a process that enables the electronic identification of a natural or legal person.
- **Validation** – validating that the user exists. Validation uses evidence that the user can provide to prove who they say they are such as passport, driving licence or bank account. The strength of the evidence should be taken into

account (passport stronger than utility bill). The evidence must be validated to ensure it is genuine. Validation is typically done by an evidence verifier. Validation may also include checking for evidence of user activity at the address they provide or via the use of some other form of evidence they provide, such as social media.

- **Verification** – verifying that the user is the person they are claiming to be. This might be by checking possession of evidence presented by the user either through a face-to-face check, via video, via an electronic token or via biometric cross match (e.g. selfie to passport photo). The user might also be verified as genuine by the collection of separate verification specific evidence such as the ability to answer knowledge-based questions. The verification of a user as the genuine holder of a piece of evidence might be done by the same evidence verifier who validated that evidence or be done by a separate evidence verifier. The identity provider may also play the role of evidence verifier in this respect, linking pieces of evidence together to create a single piece, or collection of, more robust evidence.
- **Identity Evidence** – evidence that proves who the user is. This could be electronic issuance or verification of ID documents (e.g. passport), proof of social/societal activity, ID fraud risk assessments.
- **Identity Assurance** – a combination of the Identity Verification and Proofing process and the trust imparted by the means of authentication as measured against a set of criteria and levels as adopted by the Trust Framework.
- **Level of Assurance** - a set of outcome-based requirements and processes that must be met in order for the trust implied by an assertion of identity to be easily recognised as part of an authentication process. Some already exist such as ISO/IEC 29115, NIST 800.63.3, EIDAS Regs, GPG 45.

Definitions (OIX Glossary) – key roles

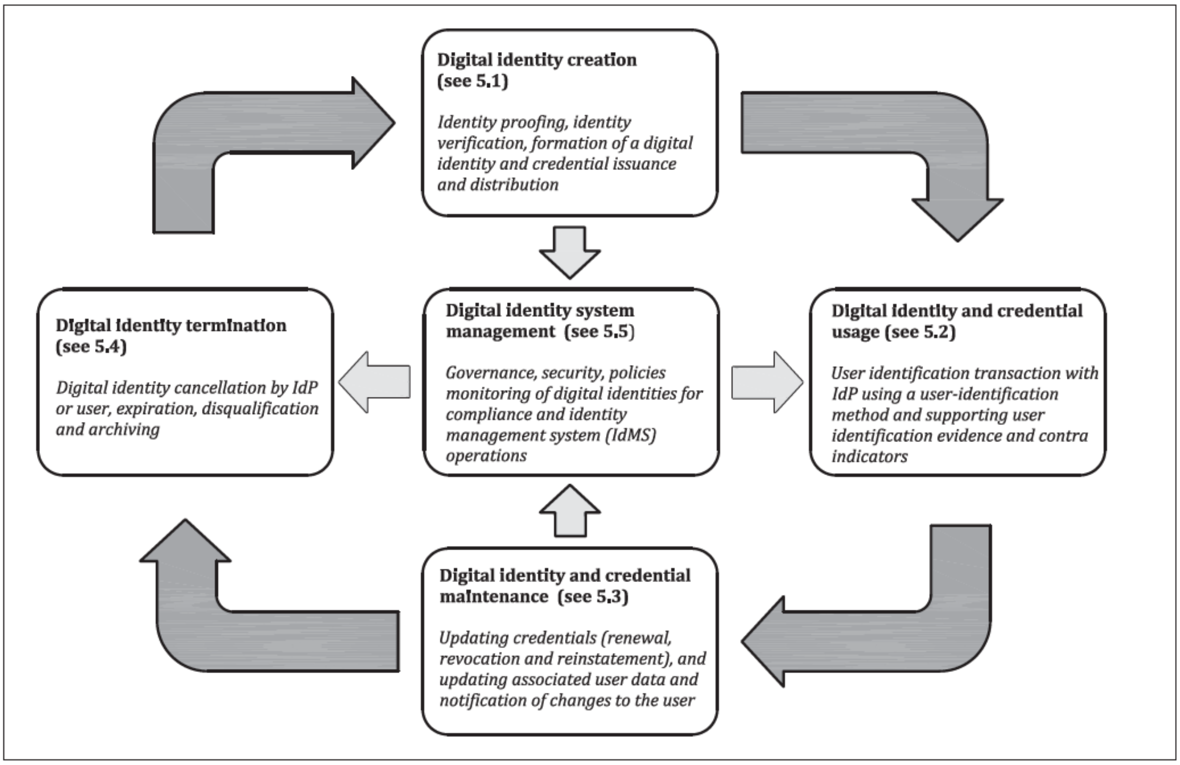
ADVP members involved in the electronic validation of documents will fit within the categories of 'Identity Technology Provider' or 'Evidence Verifier'.

- **Identity Provider** – creates and maintains a Digital Identity for users that they can present to Relying Parties to prove who they are. Trust is established by evidence issuers. The Trusted Digital Identity must comply with the overall rules of the trust framework and of the sector specific trust schemes. In the self-sovereign model, the provider of an app to hold verifiable credentials, provide the user with bound authenticators, and present credentials to relying parties could be a proxy for the identity provider.
- **Identity Technology Provider** - a technical or service component used as part of the establishment and provision of trust in the identity. Types include: ID Proofing and verification, ID authenticators, Fraud controls, Identity Access Management, Aggregators.
- **Evidence Verifier** – validates some form of evidence that proves who the user is and/or what they are eligible to do and then verifies that the evidence belongs to the User. This role uses the rules for identity proofing and records the process of such as verified evidence and claims.

- **Broker** – allows relying parties to enter into a single contract and single technical integration to access a critical mass of IDs and entitlement information from different Identity Providers or Evidence Issuers. Or an intermediary that would typically be defined by the specific Trust Framework.

Digital identity life cycle (BS8626)

ADVP members involved in the electronic validation of documents will fit in the box titled ‘Digital identity creation’ in the following table.



Digital identity creation (see 5.1)

Identity proofing, identity verification, formation of a digital identity and credential issuance and distribution

Digital identity termination (see 5.4)

Digital identity cancellation by IdP or user, expiration, disqualification and archiving

Digital identity system management (see 5.5)

Governance, security, policies monitoring of digital identities for compliance and identity management system (IdMS) operations

Digital identity and credential usage (see 5.2)

User identification transaction with IdP using a user-identification method and supporting user identification evidence and contra indicators

Digital identity and credential maintenance (see 5.3)

Updating credentials (renewal, revocation and reinstatement), and updating associated user data and notification of changes to the user

UK digital identity ecosystem – challenges

- **Standards and governance** – who sets the standards and how are they regulated/supervised across every aspect of the ecosystem – identity verification, data management, security etc?
- **Interoperability** – how does a digital identity created by one organisation get used in another?
- **Trust** – how can relying parties and consumers trust all participants in the ecosystem?
- **Liability** – who pays when it goes wrong?
- **Inclusion** – how to ensure that no one is excluded from using digital identity.
- **Ecosystem architecture** – how does it all work safely and securely across multiple digital identity providers and users?
- **Counter fraud and security** – how to protect the ecosystem from criminals and imposters?

UK digital identity ecosystem – publications to refer to

- **The UK digital identity and attributes trust framework** - alpha version (beta version due summer 2021) https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework

- **BS8626** – Design and operation of online user identification systems – Code of Practice https://shop.bsigroup.com/ProductDetail/?pid=000000000030379130

- **JMLSG** Prevention of money laundering combating terrorist financing - Guidance for the UK Financial Sector

  https://jmlsg.org.uk/guidance/current-guidance/

- **PAS 499:2019** Code of practice for digital identification and strong customer authentication (written and published by BSI and is a requirement of the Second Payment Services Directive "PSD2" and recommendations will be incorporated into BS8626 in due course)

  https://shop.bsigroup.com/ProductDetail?pid=000000000030342524

- **ISO/IEC 29115** – Information technology – Security techniques – Entity authentication assurance framework

- **NIST 800.63.3 (US)** – Digital Identity Guidelines

- **UK EIDAS regulations** - The UK eIDAS Regulations set out rules for UK trust services and establishes a legal framework for the provision and effect of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication (regulated by ICO)

  https://ico.org.uk/for-organisations/guide-to-eidas/

- **GPG 45** – How to prove and verify someone's identity

  https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual

- **GPG 44** – Using authenticators to protect an online service

  https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services

- **Land Registry** - Practice guide 81: encouraging the use of digital technology in identity verification

  https://www.gov.uk/government/publications/encouraging-the-use-of-digital-technology-in-identity-verification-pg81/practice-guide-81-encouraging-the-use-of-digital-technology-in-identity-verification

- **OIX** publications including ‘OIX Guide to Identity Proofing and authentication’

  https://openidentityexchange.org

UK digital identity ecosystem – timelines

- **The UK digital identity and attributes trust framework** alpha released in February 2021 with beta version due summer 2021 – any required legislation unlikely before 2022.
- **Government Document Checking Service** trial enabling participants to check if a passport number exists (only seven private sector companies signed up). The results of the trial will help determine what happens next with making government data available to the private sector.
- **DBS** currently planning a fully digital process to be available later in 2021 as an alternative to existing process. A further iteration will support a DBS digital identity scheme.
- **Private sector** activity includes TISA financial services digital identity scheme POC and Etive home buying digital identity scheme project.
- **Digital identity** is unlikely to become mandatory and will likely co-exist with existing identity verification practices over the coming years.