Digital Identity Technology Explainer

Briefing Note August 2026

Lib**STEMM** is the party body (AO) for Science,Tech, Engineering, Medicine and Maths – either for those qualified in those fields or with an interest.

July 2026 – The UK Government has recently announced the cancellation of their planned mandatory state-run digital identity card system, but voluntary digital identity schemes still exist e.g. NHS App and the technology is advancing rapidly. Additionally, the EU Digital Identity (EUDI) scheme is progressing, with each member state mandated to make at least one EUDI Wallet available to their citizens for voluntary use.

Understandably, in such a fast changing environment there is much room for confusion. This briefing note provides a status update on some of the key terminology being used, the state of the technology, and the issues at the public policy and political interface – specifically aimed at a Liberal Democrat audience.

Overview of Digital Identity:

A Digital Identity is an electronically stored set of records and/or credentials and attributes of a person which can be used to **Authenticate** (prove who they are) and then **Authorise** them (grant permission) to access information or use services at the point of need without the requirement for physical documentation or other lengthy processes.

A person often has multiple records or credentials which have been issued by different departments or institutions. These could include Government Documents like a Driving Licence, other eligibilities e.g. eVisas, Right to Work/Rent Status or other official information like certificates, qualifications, memberships etc.

Attributes or individual pieces of information which describe the person, could include date of birth, name, address, fingerprint, iris scan etc.

Each of these attributes and credentials could be digitised and used as part of a digital identity.

e.g. Passport control at the UK border: A digital facial image is stored in an embedded chip in your passport, along with your full name, date of birth and passport number. This can be used to automatically confirm your identity (Authenticate) at an e-gate and then allow you into the UK (Authorise) if you are a UK citizen or hold a valid Electronic Travel Authorisation linked to your biometric passport.

HM Passport Office (HMPO):

- issues 6 – 7 million passports per year

UK passport coverage of UK population ~ 87%

- provides ID checking service to multiple government departments
- could play a key role in any future Digital ID scheme
- recently migrated into the “Cloud” with a high security architecture

3 Architectures for Digital Identity Provision

There are 3 main architectures for providing and managing Digital Identities[Shaun Cheon, 2026][Gravity, 2023]

1) Centralised

In this type of architecture, a single authority manages and stores all relevant data in a single, centralised repository or database. Users would then register with that authority to query the data. Examples include the Netherlands DigID scheme which is being rolled out, and India’s Aadhaar programme. Both of these use biometrics to register and authenticate. Aadhaar is an UID (Unique IDentifier), a unique 12 digit number issued to each citizen which is linked to the person’s photograph, ten fingerprints and two iris scans, all of which are stored in a central database. The associated ID card for that UID then allows access to government services, with the ability to authenticate a person’s biometrics against the central database in real time.

DigID enables the use of existing government documents e.g. driving licence or existing ID card, or smartphone apps. The

Printed, Published and promoted by Chris Lomax on behalf of LibSTEMM, 66 Buckingham Gate, London, SW1E 2AU.

app allows an ID check to take place using a passport biometric check, and then use the phone's facial recognition or fingerprint scanner for authentication and authorisation to access information and relevant services.

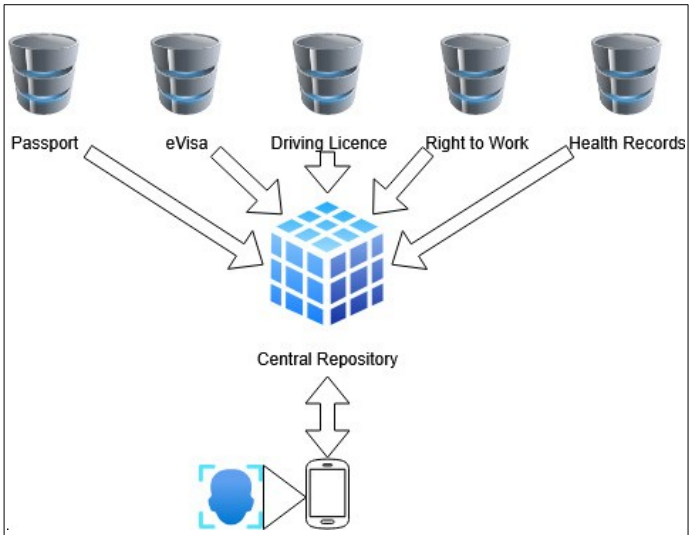

Figure 1: Centralised Digital ID Architecture

2) Federated

A federated system may look like a centralised system to the end user, with a single point of access, and the requirement to use a mandated single method of access and authentication e.g. a secure card with chip and pin, or a phone app with biometrics. However, behind the scenes, the data is not centralised but remains within the departments, organisations and systems it was originally created in. Instead, a portal is provided, and a trust relationship is set up between all the systems so that user authentication information captured by the portal is shared with the federation of systems who are part of that trust relationship, enabling a single user logon to then access relevant information and services across a number of back end systems.

A good example is Estonia's digital identity system which provides a federated data exchange platform (X-Road) connecting several government databases. Initially, citizens used a card reader, with chip and pin, to authenticate and access services but this is now largely carried out using a mobile phone app.

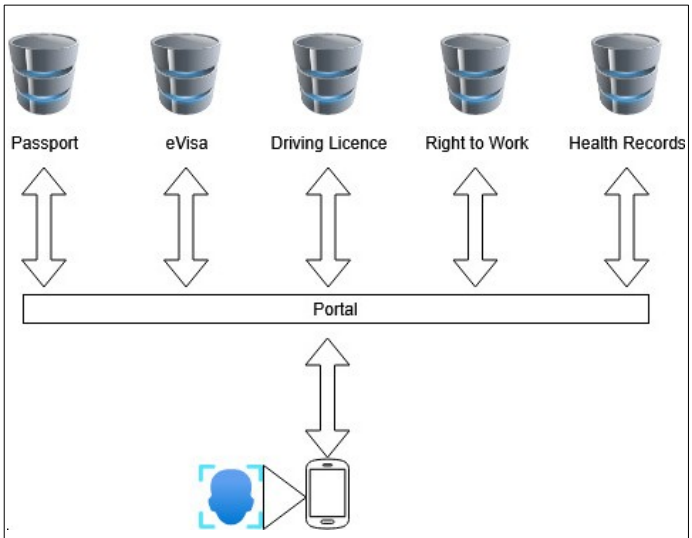

Figure 2: Federated Digital ID Architecture

3) Decentralised

A fully decentralised digital identity system would enable credentials to be issued by multiple authoritative sources and then stored locally by each individual. In this architecture, the individual has control over their information and can selectively share specific attributes which may be required for authentication and authorisation across multiple systems.

The key elements of this architecture are

- **Digital Wallet** (an end user application which can securely store the credential)
- **Distributed Ledger Technology** (enables secure recording and synchronising of data across multiple nodes, with no central control e.g. blockchain)
- **Credential source** which can securely issue credentials using the distributed ledger and support viewing or query of the credential's transaction history to prove authenticity

The current example of this architecture is the Mobile Driving Licence which supports the storage of secure digital versions of a physical driving licence in a compliant smartphone app. This uses the ISO/IEC 18013-5 standard for secure identity verification and is already available in some jurisdictions to store in an Apple Wallet on an iPhone or Apple Watch. Google's Wallet also provides support for this and the UK's GOV.UK One Login app and the European Digital Identity Wallet Framework are also planning to support this.

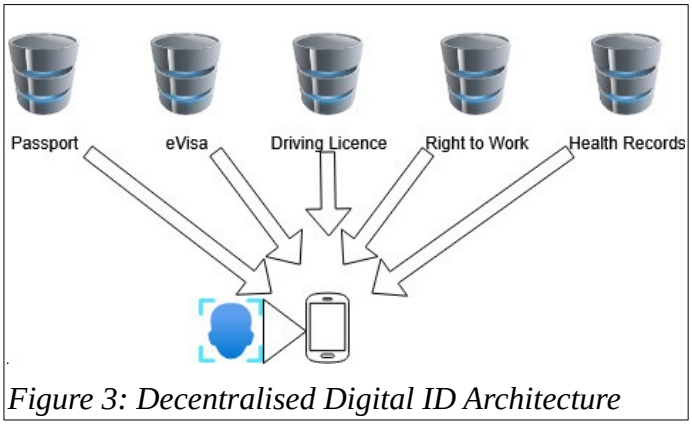

Figure 3: Decentralised Digital ID Architecture

The next step - Hybrid Federated and Decentralised Systems

The most likely architecture for the next Digital ID System to be implemented is a hybrid of the Federated and Decentralised systems. Most governments and institutions will already have a

significant amount of data which can be used for authentication and authorisation to provide access to data and services. In many cases this data will be spread across multiple departments, databases and systems. Given the cost of consolidating this data, and the cyber security risk of maintaining all the data in a single repository, creating a federated access layer to these systems would seem the most likely strategy, enabling systems to be included one by one, when ready. The UK's Gov Gateway was an example of such federation, and the GOV.UK One Login is the next step.
Where the hybrid architecture comes in is with the use of mobile apps to store personal data locally. Initially this would be basic identity and biometric data, with perhaps a Mobile Driving Licence once all those elements are in place, but the majority of the credentials would still reside in the federated government systems, with access to that data authenticated by the locally held personal data in the phone app.

Proposed UK Digital ID Scheme

The government had proposed to consolidate access to all government services from a single place – GOV.UK One Login, which would eventually replace all other access, including Gov Gateway[Gov UK 1].
This has now been cancelled, at least from being mandatory, however some elements of this may still progress under a voluntary basis to take advantage of new standards and technology.
This would have been accessible in 3 main ways[Gov UK 2]:

1. GOV.UK One Login smartphone application for Android 10 or higher and iPhone 8 running iOS 16.7, or higher
2. Online by answering security questions
3. Physically, at a Post Office

Each of these access methods requires existing government photo ID to have already been issued e.g. driving licence, passport, residence permit/card or work permit.
This initial Federated Architecture would have become a hybrid architecture with the addition of a GOV.UK Wallet which would enable some Decentralised storage of credentials. It was not stated whether this GOV.UK Wallet would have been a new application or an enhancement of the GOV.UK One Login smartphone application. However the statement that it is possible to save a digital version of an HM Armed Forces Veteran Card with the One Login application suggests that it might have been the plan to enhance the app for additional use[Gov UK 3].
The wider implementation of GOV.UK One Login would have introduced the UK Digital Verification Services Trust Framework[Gov UK 4], which enables organisations to be certified against the trust framework requirements and then be certified to provide Identification Services. There are various roles as part of the full implementation, which include:

1. Identity Service Providers: Checks Identities
2. Attribute Service Providers: Collects, Creates or Checks Attributes
3. Holder Service Providers: Holds Identities and/or Attributes
4. Orchestration Service Providers: Orchestrates data sharing between participants
5. Component Service Providers: Provides a specific component of the identity checking or authentication processes

There are currently 45 organisations certified to provide Digital Identity and Attribute Services on the Register[Gov UK 5].

How this could work:

Your identity credentials or attributes would be issued by the **Attribute Service Provider**, a trusted source e.g. GOV.UK One Login, cryptographically signed, and would then be stored using something provided by a **Holder Service** e.g. in a Digital Wallet application on a smartphone.
To prove your identity, or eligibility for something, a Relying Party e.g. Employer, might present your credential to an **Identity Service Provider**, who would then securely share that information using an **Orchestration Service Provider** check the authenticity of the **Attribute Service Provider**, that the credential had not been tampered with, the currency of the credential, and then validate the information in the credential against the check being performed.

Wider Considerations

The EU is rolling out a Digital Identity standard and framework[EU ID] (eIDAS 2.0) which requires all member states to provide a digital identity wallet to all citizens, residents and businesses. These wallets would be cross border compatible, to enable seamless digital identification across all member states.
The GOV.UK One Login system is intended to be implemented in alignment with internation standards e.g. ISO 17065:2012 and ISO 18013-5[Gov UK 6], and should therefore enable interoperability with the EU Digital ID scheme if required.

Bibliography

Shaun Cheon, 2026: Shaun Cheon, Digital ID Systems: A Global Comparison and the Path to Resilient Identity Solutions, 2026, https://andopen.co.kr/digital-id-systems-a-global-comparison-and-the-path-to-resilient-identity-solutions/
Gravity, 2023: , A Journey Through Identity Models: Centralized, Federated, and Decentralized, , https://www.linkedin.com/pulse/journey-through-identity-models-centralized-federated-decentralized
Gov UK 1: , Guidance Enabling the use of digital identities in the UK, 2026, https://www.gov.uk/guidance/digital-identity
Gov UK 2: , Using your GOV.UK One Login, 2026, https://www.gov.uk/using-your-gov-uk-one-login/proving-your-identity
Gov UK 3: , GOV.UK Wallet, 2026, https://www.gov.uk/wallet
Gov UK 4: , UK digital verification services trust framework, 2026, https://www.gov.uk/government/collections/uk-digital-verification-services-trust-framework
Gov UK 5: , Register of digital identity and attribute services, 2026, https://www.digital-identity-services-register.service.gov.uk/register/all-providers
EU ID: , European Digital Identity, 2026, https://commission.europa.eu/topics/digital-economy-and-society/european-digital-identity_en
Gov UK 6: , International use of digital identities and credentials: stakeholder survey responses, 2026, https://www.gov.uk/government/publications/international-use-of-digital-identities-and-credentials-stakeholder-survey-responses/international-use-of-digital-identities-and-credentials-stakeholder-survey-responses