SYNECTICS SOLUTIONS

DIGITAL IDENTITY IN 2024/25: A UK FINANCIAL SERVICES GUIDE

Developed by Synectics

DIGITAL IDENTITY IN 2024/25: A UK FINANCIAL SERVICES GUIDE

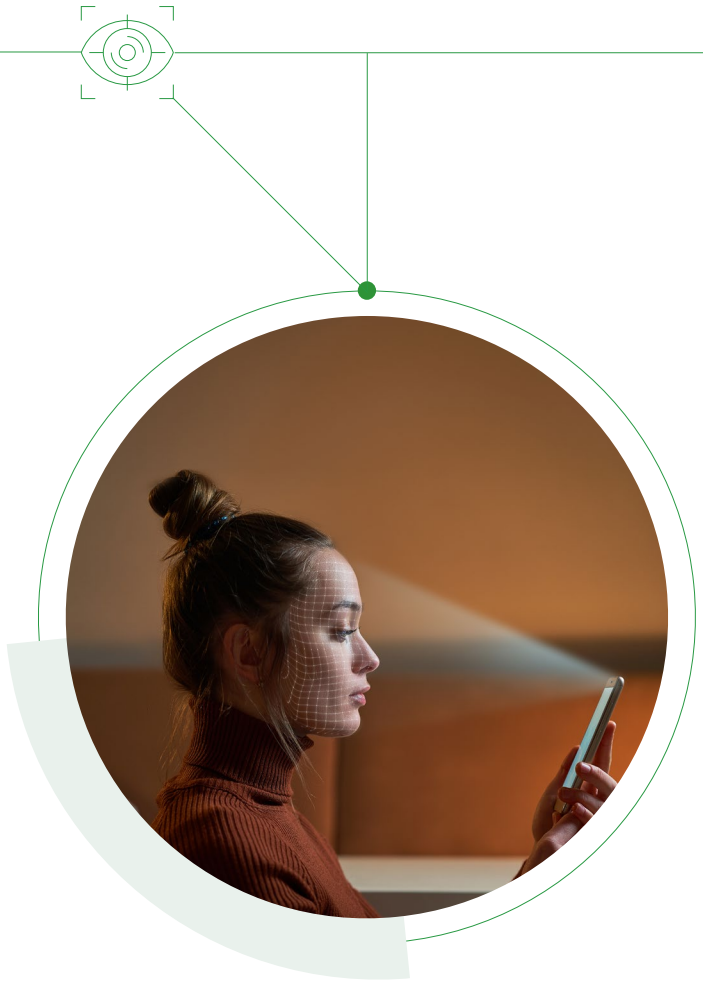
Developed by Synectics

SYNECTICS SOLUTIONS

The concept of 'digital identity' has gained significant traction. In fact, by the end of 2024 an estimated 70 billion[1] digital identity verification checks will have been carried out globally, enabling individuals to prove their right (and suitability) to work, rent, access financial products and services, and carry out a wide range of online transactions.

With the new UK government declaring its support, and intended legislative backing for digital IDs as a route for people and service providers to interact safely and efficiently in an increasingly digital world, continued growth in digital ID usage looks inevitable.

This guide has been developed to explain what this means for the UK financial service sector. It covers:



- A recap of **DIGITAL ID**
- A tour of relevant **GUIDANCE**
- **PROS AND CONS** of using digital identities
- The current **STATE OF PLAY** for digital ID in the UK
- **EXAMPLES OF** Digital IDs in practice

Identity has never been more important to society and our economy. Digital IDs will offer a friction-reducing route for people and service providers to interact safely, smoothly and with trust. Read on to get up-to-speed on digital ID and to see how it could benefit you.

If you are an Identity Service Provider (IDSP) a dedicated guide for you can be found here.

[1] Digital Identity Verification Checks to Pass the 70 Billion Mark in 2024 (juniperresearch.com)

SECTION 1

A Recap of Digital Identity

What is a 'Digital Identity'?

Essentially a digital ID is a collection of information about a person that exists online; information that enables them to prove they are who they say they are during interactions and transactions. They can easily be created and accessed via online platforms and apps, remove the need for physical documentation and in-person checks.

There are two types of digital ID.

Single Use

This refers to a digital ID being used for a single, dedicated purpose e.g., signing up for a mortgage. This is currently the most common type if usage but is limited in scope.

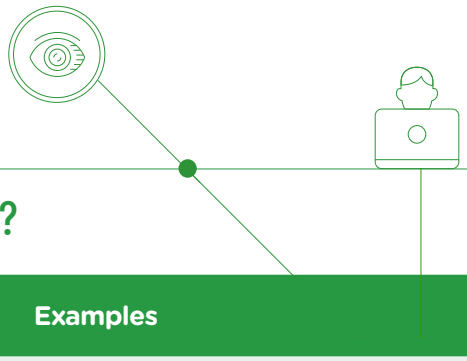
Reusable

As the name suggests, this refers to digital IDs that can be used multiple times by different organisations. This is the current direction of travel for digital identity, in the UK and globally.

It is important to remember that in both cases, the digital ID (and all the data it comprises) is owned by the individual. In this sense, it is a consumer tool that authorised financial organisations can leverage.

How are digital identities used?

Digital identities are used to prove a person's identity, and to verify that the identity is valid and has existing over time. As with traditional ID however, it is important that digital IDs are verified.



Who's involved in the digital identity verification ecosystem?

Party	Definition	Examples
Relying Party (RP)	The organisation requiring the identity to be verified	Banks, insurance companies, estate agents, finance providers, local authorities, employment vetting companies
Identity Provider (IDP) **or** Identity Service Provider (IDSP)	The organisation or person verifying the identity	Yoti, the Post Office, Mitek, IDverse, TransUnion, Equifax
Attribute Provider (AP) **or** Attribute Service Provider (ASP)	The organisation or person providing information to verify an identity	Synectics, DVLA, UK Passport Office, Credit Refence Agencies
Orchestration Service Provider	The organisation or person ensuring identity credentials are securely shared between parties	Mvine, Signicat, Avast
Scheme Owners	The organisation or person who created and runs a scheme for the use of digital identities and attributes	Home Office, MyIdentity, ConnectID, the Pensions Dashboard

Scheme/guidance specific facts & phrases for understanding the current UK digital ID landscape.

SECTION 1

A Recap of Digital Identity

What is the 'UK Digital Identity and Attributes Trust Framework'?

Developed by the DCMS, this is the UK government's approach to digital ID – a framework of rules, policies and standards that aim to support safe, efficient, and effective use of digital ID solutions in the UK.

You can learn more about the Framework here.

What is the 'Good Practice Guide 45 (GPG45)?

This is continually updated (technology agnostic) guidance from the UK government on how to check and verify an individual's identity.

Fundamental to the UK Digital Identity and Attributes Trust Framework (DIATF), GPG45 defines 5 types of "attribute" required to verify an identity. These attributes can be collected at the same time or incrementally. These attributes are:

Strength
Get evidence of the claimed identity.

Validity
Check the evidence is genuine or valid.

Activity History
Check the claimed identity has existed over time.

Identity Fraud
Check if the claimed identity is at high risk of identity fraud.

Verification
Check that the identity belongs to the person who's claiming it.

> "Millions of people are already using digital identity services to save them time. When people choose to use them, these services cut down admin and increase security making it much easier to open bank accounts, start jobs, rent flats and much more. Our legislation will make sure that people can fully trust these services."
>
> Science Secretary,
> Peter Kyle

The guidance supports using evidence to validate and score ID attributes from a wider pool of authoritative public, private, and syndicated fraud data sources. This may be carried out by IDSPs and ASPs.

Data sources such as:

Financial services*	**Telco***
Insurance*	**DDRI**
Utilities*	**Gig Economy***
NCA Amberhill	**Car rental***

**suspected/proven fraudulent and cleared IDs*

You can read more on GPG45 here.

What is an 'Identity Profile'?

Different combinations of attribute scores create identity profiles, which can carry a low, medium, high, or very high level of confidence (LOC) in an individual's identity. The level of confidence an organisation requires is dependent on the specific application, use case and associated risk.

Using identity profiles as a means to verify digital IDs therefore moves away from a binary rules-based approach (e.g. 2+2 verification), towards a more flexible methodology.

SECTION 2

The Pros and Cons of Using Digital Identification

For you and your customers

The Case for Digital Identities

The accurate verification and authentication of ID is fundamental to maintaining customer trust and guaranteeing the security of transactions. In a digital services era, the shift from hybrid identity verification systems to using purely digital identities offers value creation on several fronts:

Improved customer experience:

In the UK, around 25%[2] of all financial applications are abandoned due to difficulties in the registration process. Digital identities can help streamline authentication processes to avoid this outcome and help build trust. Customer retention rates will also benefit.

Greater financial inclusivity

Many individuals don't have access to traditional forms of ID needed for many basic financial services, or struggle to pass existing verification processes due to thin/poor credit files that don't necessarily reflect their true situation. Digital identity solutions can help break down these barriers by supporting validation through alternative ID attributes. For example, our own ID verification solutions, SynID, has helped users achieve a 50% increase in pass rates for customers with thin credit files.

With financial inclusivity such an important aspect of this technology, we have produced a separate guide to the topic which can be downloaded, here.

Business growth

Because digital ID verification is more inclusive, it is possible for FSPs to confidently say 'yes' to more good customers. As well as being better for those seeking access to financial services, there are clear 'increased revenue' implications for providers.

Reduced costs and increased GDP

Avoiding the need for repeated, time-consuming manual checks when onboarding customers - relying instead on a digital identity already validated by a trusted third-party - saves time and resources. On-going costs can also be reduced. For example, research suggests that around 30% of all support calls to call centres are password reset requests due to an individual forgetting their details. This can be avoided with reusable digital identities. At the same time, McKinsey estimates that digital IDs could increase a country's GDP by between 3 and 13 percent by 2030[3].

KYC accuracy and fraud prevention

Digital identities help eliminate the potential for human error, for example when comparing photographic ID to an individual, or in failing to spot counterfeit/doctored documents. Broader data captured (strictly in line with data protection legislation) and expanded on over time, can also deliver a more precise understanding of an individual's behaviour as a basis for determining potentially suspicious account activity and for supporting ongoing due diligence checks.

A spotlight on ID fraud

The benefit of using digital ID verification as a route to improve fraud defences cannot be underestimated. Our analysis of data from National SIRA, the UK's most authoritative risk intelligence syndicate, shows that ID fraud is already the no.1 fraud type reported by banks and other financial service providers, and could account for 50% of all reported fraud by the end of 2024.

[2] Private sector economic impacts from identification systems, World Bank, 2018

[3] https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

SECTION 2

The Pros and Cons of Using Digital Identification

For you and your customers

Single vs Reusable: Challenges and Answers

The above-mentioned benefits primarily apply to the adoption of Reusable digital IDs, as while Single Use digital IDs may be easier to implement there remains a high reliance on duplicative checks.

Also, customers still need to re-verify for each new product or service they wish to use. This also means that Single Use applications are also potentially more susceptible to fraud - particularly synthetic ID fraud.

But the widespread adoption of Reusable digital IDs is not without its concerns and challenges. For example:

Adoption

Widespread consumer adoption is needed which also relies on RP adoption and implementation. For both to happen simultaneously, thought is needed to ensure applications are of real use i.e., worth signing up for, and easy to navigate for all involved.

Integration

For reusable digital IDs to work, multiple Relying Parties (all potentially with very different internal processes) must be able to integrate successfully with the identity service platform developed. Problems on this front can cause delays in uptake which links back to concerns around adoption.

Liability

For such a heavily regulated sector, it's no surprise that liability is a strong concern for financial services. Indeed, within a digital identity ecosystem, liability for accurate customer checks and ID verification does sit with the Relying Party, meaning they need to have absolute confidence in the verification services they use.

Current developments in the UK not only demonstrate an awareness of these concerns, they also indicate a route forward which tackles them. Let's look at that in more detail.

SECTION 3

The current state of play for digital ID in the UK

Certification as a litmus test for appetite

Perhaps the biggest indication that digital IDs, and their accompanying verification processes, are the future for UK finance is the number of IDSPs that have already been certified against the DIATF – 51 as of August 2024.

This means that they have been independently assessed and shown to adhere to the identity verification procedures, data security measures, and interoperability requirements outlined in the framework.

Many of the certified organisations have also been certified for specific additional rules relating to specific Right to Work, Right to Rent and Disclosure and Barring Service digital ID schemes.

It's worth noting that while relying parties are not obliged to use IDSPs and ASPs certified to DIATF standards, the assurance level delivered (for Relying Parties and their customers) makes this path likely.

Legislative developments: the Digital Information & Smart Data Bill

Establishing a legal basis that would allow the DIATF to be developed is the next critical step to broader adoption. Ahead of the July 2024 UK election, this need was set to be fulfilled (at least in part) by the Data Protection and Digital Information (DPDI) bill. However, the bill failed to pass before parliament was dissolved.

Taking its place, and demonstrating the new government's commitment to digital ID usage in the UK, is the Digital Information and Smart Data (DISD) bill.

Exact details within the bill are to be confirmed but based on information shared in the King's Speech, the intent is that it will:

1. Provide a legal framework to support the use of digital ID products and services from certified providers – enabling businesses and consumers to use such tools with "confidence and peace of mind."

2. Reform data sharing and standards, which includes introducing 'Smart Data schemes' which will allow the secure sharing of customer data with authorised third parties, with customer permission.

More information about the Bill is available here.

Industry alignment

It isn't just government guidance and policies that support digital identity use in the UK. Industry support for digital ID verification services came very early in the process.

For example, In June 2020, the Joint Money Laundering Steering Group (JMLSG) issued updated guidance for regulated financial services organisation in relation to the prevention of money laundering and terrorist financing. The revised guidance embraced the important role that digital identity can play in ensuring organisations meet their regulatory obligation in this area.

The JMLSG is closely monitoring development with the DIATF and GP45 to ensure that any details set to become enshrined in UK legislation will align with regulatory demands for the sector in terms of AML/KYC ID checks.

SECTION 3

The current state of play for digital ID in the UK

Watch and learn – Examples in action

There are also several digital ID schemes and pilots already in operation that will serve as important learning opportunities, support ongoing development of policies, and help build trust in the approach.

Three notable examples are:

Right to Work, Right to Rent and DBS checks

Since 6 April 2022, employers have been able to use certified IDSPs to digitally verify the identity of British and Irish citizens as opposed to carrying out manual right to work checks. All identity checks for Right to Work purposes must achieve a minimum Medium Level of Confidence (LOC).

Digital ID Connect

Yoti ID, Post Office EasyID and Lloyds Bank Smart ID are three separate digital ID apps, all supported by Yoti technology. Together, they also form Digital ID Connect – a network of reusable digital ID apps that are interoperable, meaning any business that accepts one as proof of ID will also accept the others. Users can demonstrate they are who they say they are, and for example guarantee proof of age, without having to show specific individual ID documents or share personal data beyond what the business in question requires.

Yoti verification technology leverages Synectics' SynID – a tool which utilises private and public sector digital consortium data to determine the assurance level of an identity based on strength, validity, identity fraud and activity history attributes.

MyIdentity (Etive)

MyIdentity is an identity trust scheme that allows the buyer or seller to be verified once so they can then use this verified ID across the home buying ecosystem e.g. with estate agents, conveyancers, mortgage lenders, and any other party involved in the transaction. The scheme has also now been expanded to include other use cases such as savings, loans, account opening and cards.

> "Synectics offer a single integration for multiple data points that help with GPG45, so they are well-placed to assist the industry in this fast-moving sector."
>
> John Abbott,
> Chief Commercial Officer at Yoti

Why this all matters to you

With so many pieces of the puzzle starting to come together, the UK Financial Services sector has a real opportunity to leverage digital identity schemes to:

- Enhance customer experience
- Expand customer base
- Reduce risk of fraud and financial crime
- Reduce onboarding and ongoing operational costs

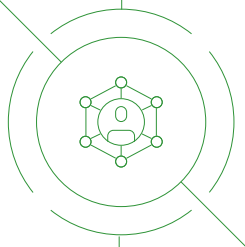
If you have not already started to, it is worth considering how digital identity processes might align with, and integrate to, your existing customer on-boarding journeys and KYC processes. It's also worth looking for suitable pilots that you may be able to take part in.

Get in touch

Finally, talk to us. As an Attribute Service Provider, already working with leading IDSPs and directly with financial services companies, we are happy to help explore opportunities that will help you be part of the rapidly evolving digital identity landscape.

Thomas Whitaker
Account Development Director

thomas.whitaker@synectics-solutions.com



SYNECTICS SOLUTIONS

Synectics Solutions Ltd,
Hamil Road, Stoke-on-Trent, ST6 1AJ

+44 (0) 1782 664000
info@synectics-solutions.com
www.synectics-solutions.com