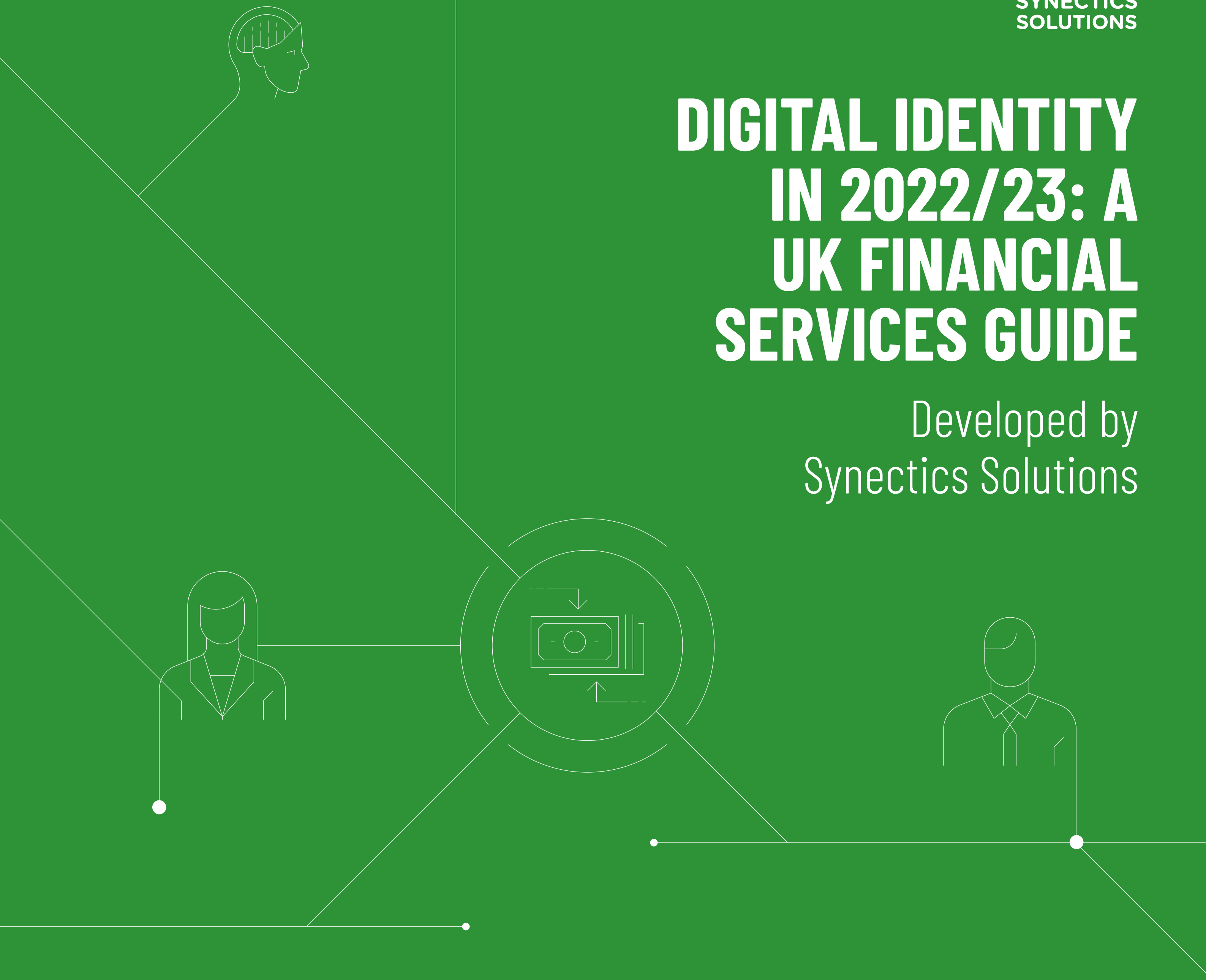
DIGITAL IDENTITY IN 2022/23: A UK FINANCIAL SERVICES GUIDE

Developed by
Synectics Solutions



“Digital ID has evolved significantly over the years, and reading this guide is a great way to bring yourself up-to-speed. Advancements in technology have resulted in fully automated models that are wholly compliant with evolving government regulations and contain advanced techniques to deter fraudsters which are unnoticeable to genuine customers.”

Russ Cohn,
GM at OCR Labs Global

“The clear benefits of Digital ID are finally starting to be realised, as several sectors start to adopt the technology. This excellent guide provides a clear and concise overview of what you need to know, so that you too can benefit from the improved UX, reduced cost and better fraud prevention offered by Digital ID.”

Steve Pannifer,
Managing Director at Consult Hyperion

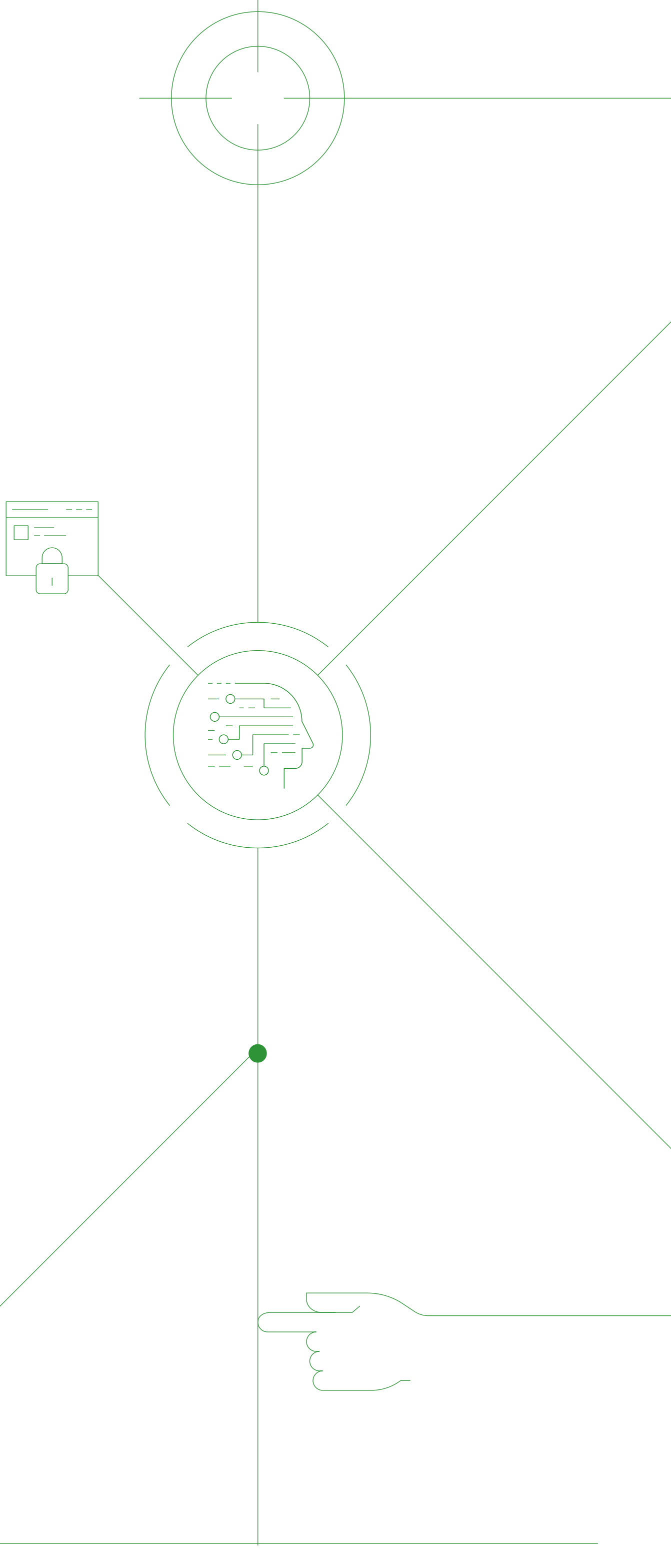
DIGITAL IDENTITY IN 2022/23: A UK FINANCIAL SERVICES GUIDE

Developed by Synectics Solutions

SYNECTICS SOLUTIONS

The concept of 'Digital ID' is nothing new to the UK financial services sector. What is new is the step up in pace we are currently witnessing around this topic. Important developments mean Digital ID is moving from concept to reality, fast. This guide has been developed to explain why and what this means. It covers:

- Some key **FACTS** and terminology
- A tour of relevant **GUIDANCE**
- Recent **CHANGES** and why it matters
- **PROS AND CONS** of using digital identities



Identity has never been more important to society and our economy. Digital ID potentially offers 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.

SECTION 1

Digital Identity: Key Facts and Phrases

General facts & phrases for understanding digital identity.

What is a 'Digital Identity'?

This is a digital representation of an individual that enables them to prove they are who they say they are during interactions and transactions. There are two types of digital ID.

- **Single Use:** when this digital representation is used for a single purpose e.g., signing up for a mortgage. This is currently the most common type of usage but is limited in scope.

- **Multiple Use:** when this digital representation 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.

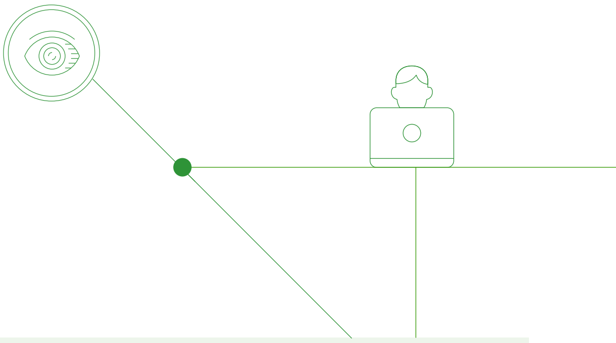
How are digital identities used?

Digital identities can be used for the following purposes.

- **Identification:** determining a consumer's identity for a product or service

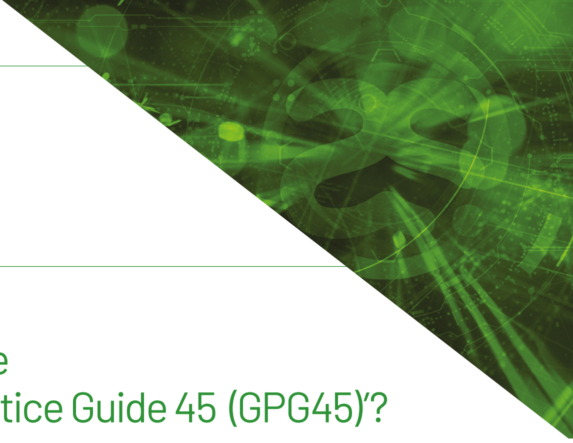
- **Authentication:** logging into a service or providing step up authentication

- **Authorisation:** determining a user or service's level of access to a system or process



Who's involved in the digital identity eco-system?

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, Hooyu, OCR Labs, TransUnion, Equifax, LexisNexis, GB Group, OneID
Attribute Provider (AP) **or** Attribute Service Provider (ASP)	The organisation or person providing information to verify an identity	Synectics Solutions, DVLA, UK Passport Office, Credit Reference Agencies
Orchestration Service Provider	The organisation or person ensuring identity credentials are securely shared between parties	Mvine, Signicat, Avast, OneID
Scheme Owners	The organisation or person who creates and runs a scheme for the use of digital identities and attributes.	Home Office, MyIdentity, ConnectID, the Pensions Dashboard, Project Endeavour, OneID



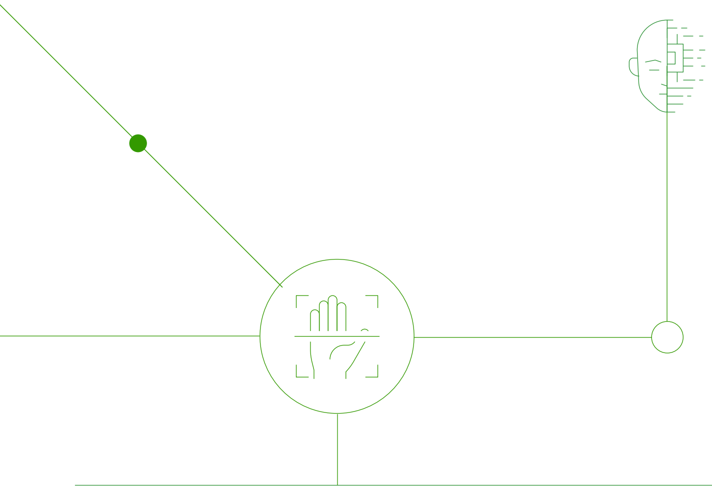
Scheme/guidance specific facts & phrases for understanding the current UK digital ID landscape

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: www.gov.uk/government/publications/uk-digital-identity-attributes-trust-framework-updated-version

> "We are developing a new digital identity framework so people can confidently verify themselves using modern technology and organisations have the clarity they need to provide these services. This will make life easier and safer for people right across the country and lay the building blocks of our future digital economy."
>
> **Digital Infrastructure Minister,**
> Matt Warman



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

This is the latest (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, 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 of 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

The guidance supports the use of **authoritative sources** (including IDPs and ASPs) to check and verify information.

You can read more on GPG45 here: www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual

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.

Identity profiles provide Relying Parties with greater flexibility in how you can verify identity compared to traditional ID proofing methods (such as the "2+2" standard for KYC). For example, different combinations of attributes provide more than one way to obtain a required level of confidence. It is especially beneficial for customers who may previously have been excluded by arbitrary checks against legacy reference data e.g., a yes/no response based on a credit reference agency check.

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, turbo charged by COVID, 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%[1] 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.
- **Improved access to financial services:** Many individuals don't have access to traditional forms of ID needed for many basic financial services. Digital identity solutions can help break down these barriers by supporting validation through alternative ID attributes.
- **Reduced costs:** 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.
- **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.

Single vs Multi Use: Challenges and Answers

The above-mentioned benefits primarily apply to the adoption of Multi Use 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 Multi Use digital ID 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:** Multi Use means multiple Relying Parties (all potentially with very different internal processes) need to 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.

What's exciting is that 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.

[1] – Private sector economic impacts from identification systems, World Bank, 2018.

SECTION 3

What's changed and why it matters

Certification, common standards and use case scenarios

Framework game changers

There are several important game changers that have happened in 2022 or are planned for 2023 that make the UK's successful adoption of digital identities more realistic. Three of these are to be found in the latest iteration of the government's Trust Framework.

1) Following the launch of a certification scheme and governing body in 2022, where IDSPs, ASPs and Identity Hubs meet specified common criteria in order to obtain certification from the UK Accreditation Service (UKAS), it has been announced that the framework is due to be formally adopted into legislation – likely to be in 2023.

2) The real-time awareness that shared fraud signals provide has been referenced as a key mechanism to further reduce identity fraud, with stipulations that framework participants must "have a structured 'shared signals' framework" to "send and receive relevant identity data and intelligence" that indicates fraud.

3) The intention is that a Trustmark will be developed to give those involved confidence in the service they are using – whether that is a bank having confidence in the IDSP or a member of the public having confidence in those handling their data.

Together, these three facts help address concerns around Multi Use digital IDs and are a major step forward in terms of ensuring, and legally enshrining, the common standards needed technically, and for creating the level of confidence needed for financial services to adopt this approach in alignment with their regulatory obligations.

Industry alignment

It isn't just changes to government guidance and policies that seem to be paving the way for digital identity use in the UK.

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 developments with the trust framework and GPG45 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.

Watch and learn

There are also several digital ID schemes and pilots taking place in 2022 and 2023 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 RTW purposes must achieve a minimum Medium Level of Confidence (LOC).

MyIdentity (Etive)

Five IDSPs and one hub service have committed to a new digital identity scheme for homebuying called the MyIdentity trust scheme. It means home buyers and sellers will no longer be repeatedly asked to give their details to all the parties involved - from estate agents to mortgage providers - in the chain of transactions. The scheme is being tested in the FCA's Regulatory Sandbox and pilots will run throughout 2022 and 2023.

ID Connect (TISA)

In 2021 The Investing and Saving Alliance (TISA) carried out a proof-of-concept pilot for its Digital Identity system, where 84% of participants were successful in utilising a Digital ID that could be used to open a new account. In 2022, plans are in place to expand on this by developing a trust scheme that allows consumers to set up and reuse an identity to interact with different financial institutions. This will also be tested in the FCA Regulatory Sandbox.

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 Multi Use 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.

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.

Take it from us: a holistic approach to Digital Identity

At Synectics Solutions, we've also undertaken our own FCA Regulatory Sandbox project with a regulated financial services firm. Pairing our National SIRA database with information from relevant third parties, incorporating eKYC checks and AML screening, we created a holistic validation process that returned proven credentials to one of our partner IDPs, Yoti.

As well as enabling successful customer onboarding, the project established re-usable credentials - held in a digital wallet - that other financial services firms could utilise in the future.

Get in touch

Chris Lewis – Head of Solutions

chris.lewis@synectics-solutions.com

Find out more...

synectics-solutions.com

Get in touch...

01782 664000

info@synectics-solutions.com

SYNECTICS
SOLUTIONS

Synectics Solutions Ltd, Synectics House, The Brampton
Newcastle-under-Lyme, Staffordshire, ST5 0QY

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