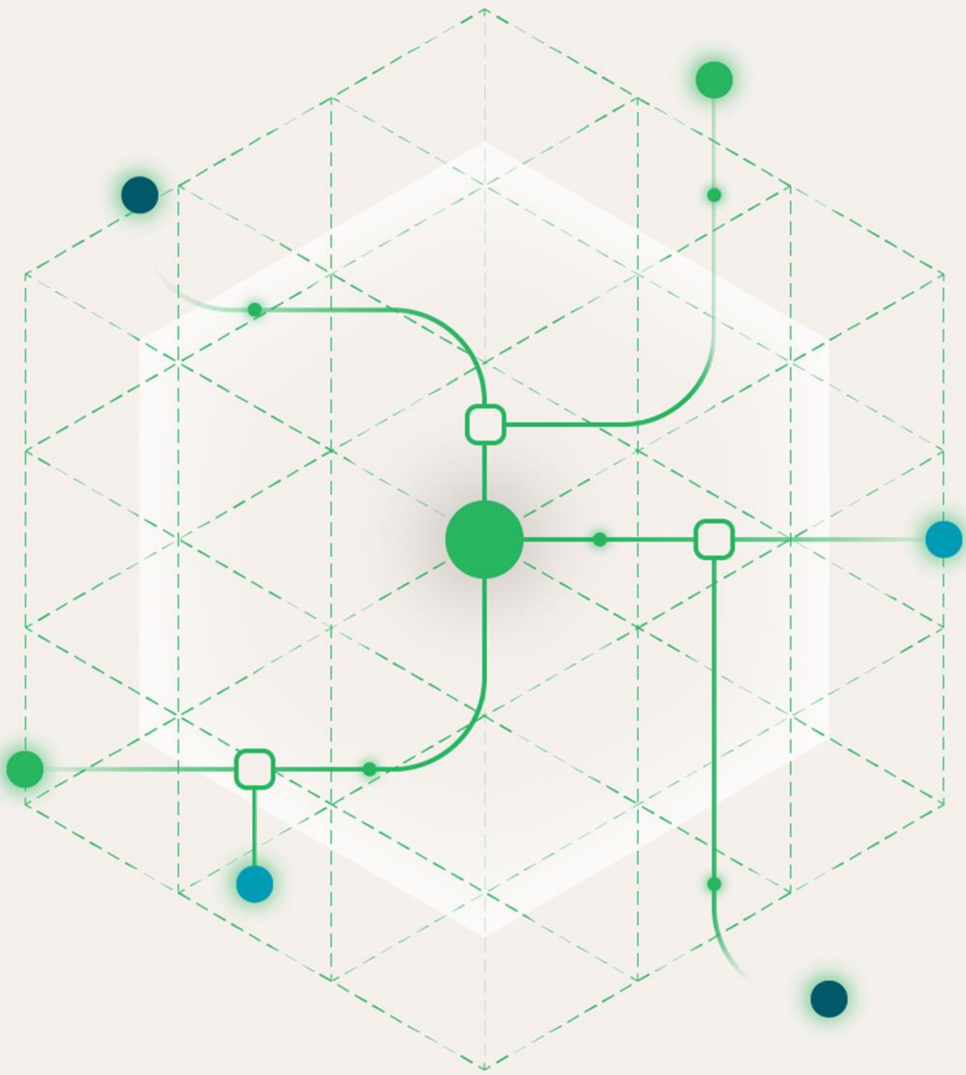


SERVICE DEFINITION

SynID

Synectics Classification: Public

Classification Status: Public

Because our policy is to improve our products and services continually, we may make changes without notice. We have tried to keep the information in our documentation complete and accurate, but we cannot accept any liability for any errors, inaccuracies or omissions in this document.

In the UK, please contact:

Synectics Solutions
Hamil Road
Burslem
Stoke-on-Trent
ST6 1AJ

Tel: 0333 234 3409

Synectics Solutions website: http://www.synectics-solutions.com

Document Information	
Document Owner	Jake Harley
Effective Date	14/04/2022
Last Reviewed Date	27/01/2026
Next Review Date	27/01/2027
Classification	Public

Document Control

Date	Issue	Name	Details	Sign-off
27/01/2026	V2	Jordan Roberts	G-Cloud 15	

CONTENTS

1 EXECUTIVE SUMMARY

SynID is a digital identity verification service delivered by Synectics Solutions. It supports organisations in verifying customer identity while aligning with the UK Digital Identity and Attributes Trust Framework (DIATF).

The service uses a combination of shared intelligence and configurable rules to assess identity attributes and generate standardised identity scores. By reusing existing verified information where appropriate, SynID helps reduce reliance on repeated document checks while maintaining robust fraud and impersonation controls.

2 SERVICE OVERVIEW

SynID enables organisations to assess digital identity by matching new enquiries against historic identity and application data. It is designed to support secure, proportionate identity verification across a range of use cases, including onboarding and access to services.

The service primarily utilises data managed by Synectics Solutions through the National SIRA fraud signal-sharing network and can be supplemented with additional public and private data sources. This multi-source approach helps improve coverage and reduce friction, particularly for individuals who may be underserved by traditional credit-based identity checks.

Synectics Solutions operates as an accredited Attribute Service Provider under the DIATF.

3 CORE SERVICE CAPABILITIES

3.1 IDENTITY ATTRIBUTE ASSESSMENT

SynID assesses identity attributes in line with Good Practice Guide 45 (GPG45), including:

- **Strength**
- **Validity**
- **Identity Fraud**
- **Activity History**

Each attribute is evaluated using a configurable ruleset aligned to DIATF requirements. Outputs are combined to generate standardised scores suitable for downstream decision-making.

SynID does not directly provide the **Verification** attribute, which requires confirmation that the individual accessing a service is the legitimate holder of the claimed identity. Where required, this can be supported through integration with trusted third-party identity providers or through customer-managed verification steps.

3.2 RULES, SCORING AND ORCHESTRATION

SynID's rules engine evaluates identity data and generates individual rule outcomes. An orchestration layer aggregates these outcomes into GPG45-compliant scores, which are returned via API.

For more complex investigations, users can access detailed breakdowns of scores, contributing rules, data sources and assurance levels through a secure dashboard.

Rules can be configured to support additional Know Your Customer checks, such as proof-of-address or proof-of-date-of-birth indicators, where required.

3.3 DATA SOURCES AND COVERAGE

National SIRA acts as the primary data source for SynID. This is supplemented, where required, by additional data sources such as:

- Public sector datasets
- Sanctions and watchlists
- Adverse media sources
- Credit reference agencies

The combination of cross-sector data sources supports broad population coverage and helps reduce unnecessary customer drop-off.

3.4 RECIPROCITY AND DATA SHARING

To support the collective benefits of fraud prevention, SynID allows organisations to contribute confirmed adverse outcomes back into the system, subject to appropriate evidence and governance.

This reciprocal approach helps protect participating organisations from serial identity fraud and impersonation.

4 KEY BENEFITS

- **Reduced Customer Friction:** Minimises repeated document requests by reusing existing trusted data where appropriate.
- **Standards-Based Compliance:** Supports alignment with DIATF and GPG45 requirements.
- **Improved Fraud Detection:** Uses historic adverse indicators to identify potential impersonation or identity misuse.
- **Flexible Deployment:** Supports both single-use and reusable digital identity use cases.

5 SERVICE DELIVERY AND SUPPORT

5.1 IMPLEMENTATION AND ONBOARDING

Implementation of SynID is supported by a dedicated Project Manager who will:

- Provide integration documentation
- Coordinate onboarding activities
- Support user acceptance testing and production deployment
- Deliver training for operational and technical users

Integration is typically delivered via APIs and designed to align with existing customer journeys.

5.2 SUPPORT AND SERVICE LEVELS

SynID is delivered as a hosted service.

- **Service availability:** minimum 99.0% of scheduled uptime per month

Service level commitments may vary where the scope of the solution differs from the standard service and will be agreed during onboarding.

6 TECHNICAL OVERVIEW

SynID is accessed via secure Application Programming Interfaces (APIs).

- Real-time requests trigger rule evaluation and scoring
- Responses return aggregated, GPG45-aligned outputs
- Minimal data (e.g. name and date of birth) can be submitted, with additional data improving assurance levels

The service is designed for straightforward integration into existing systems and verification journeys.

7 DATA SECURITY AND ASSURANCE

Synectics Solutions operates a formal Information Security Management System aligned with ISO/IEC 27001.

The organisation is committed to:

- Protecting information against unauthorised access
- Maintaining confidentiality, integrity and availability of data
- Meeting applicable regulatory and legislative requirements

Risk management activities and periodic assessments are maintained to ensure continued alignment with recognised good practice standards.

8 SUPPORT AND SERVICE MANAGEMENT

Synectics Solutions provides ongoing support for its services to ensure availability, performance and continuity in line with agreed service levels.

8.1 SUPPORT AVAILABILITY

Standard application support is available:

- Monday to Friday, 07:00–19:00 (UK time)
- Excluding public holidays in England and Wales

Support services are delivered in accordance with ITIL-aligned service management practices. Services are actively monitored, and incidents are managed using structured processes to ensure timely restoration, effective communication and appropriate escalation. Where required, incident summary reports and root cause analysis are provided, and outcomes are used to drive continuous service improvement.

Extended support hours, including out-of-hours and weekend support, can be agreed on request, subject to commercial and service agreement.

8.2 ACCOUNT MANAGEMENT

All customers are provided with a dedicated account team, which typically includes a Client Success Manager, Service Delivery Manager and Account Development Manager.

This team acts as a trusted extension of the customer's fraud and financial crime function and supports:

- Ongoing optimisation of the service
- Alignment of service configuration with business objectives
- Strategic planning, benchmarking and roadmap development
- Industry collaboration and knowledge sharing

This engagement model ensures customer requirements are reviewed on a continual basis and that services evolve in line with operational and regulatory needs.

9 DISASTER RECOVERY AND BUSINESS CONTINUITY

Synectics Solutions maintains a formal disaster recovery and business continuity framework designed to ensure service continuity, data protection and controlled recovery in the event of a major incident.

9.1 RECOVERY ARCHITECTURE

Services are delivered from a primary UK-based private cloud environment, supported by a separate secondary disaster recovery environment.

Data and system components are protected through backup and recovery mechanisms aligned to the following standard recovery objectives:

- Recovery Time Objective (RTO): 48 hours
- Recovery Point Objective (RPO): 24 hours

Improved RTO and RPO targets can be agreed on request, subject to service scope and commercial agreement.

9.2 DISASTER RECOVERY PROCESS

In the event of a critical service failure, documented procedures are followed to:

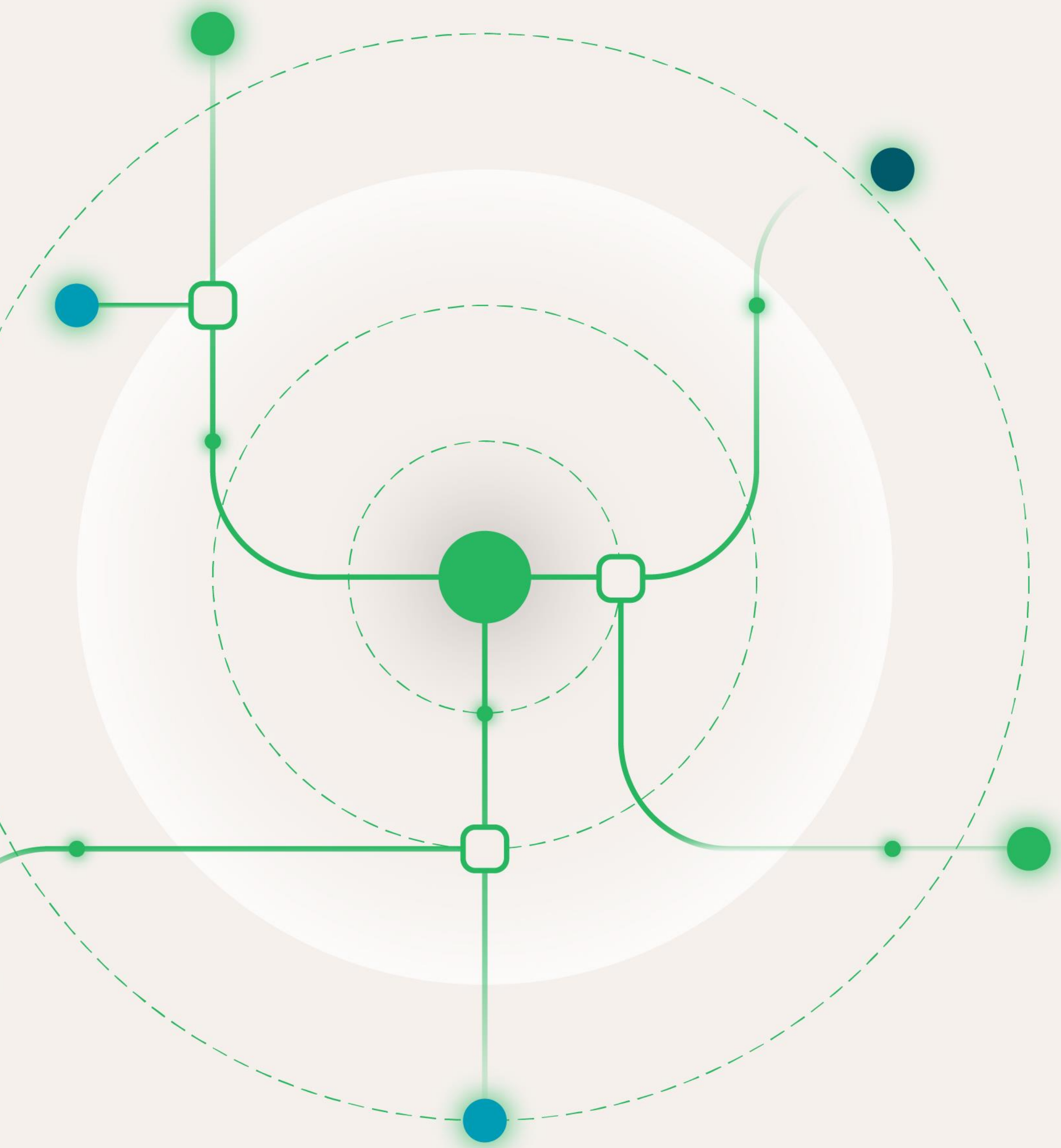
- Assess the nature and impact of the incident
- Invoke disaster recovery controls where required
- Restore services using the secondary environment and available backups

- Validate system integrity and data consistency prior to resuming normal operations

Recovery activities are governed by documented runbooks, clear escalation paths and defined roles and responsibilities to ensure a controlled and auditable response.

9.3 TESTING AND GOVERNANCE

Disaster recovery procedures are tested periodically to ensure effectiveness and operational readiness. Test outcomes are reviewed and used to strengthen resilience, refine recovery processes and support continuous improvement of the overall service.



SYNECTICS
SOLUTIONS