9-10 Bath St, Bath BA1 1SN
sales@quidos.co.uk
01225 667570 | quidos.co.uk

Service Definition Document (Draft) – SNUG

Document version: 0.01
Last updated: 13/01/2026
Service: SNUG (web application and API)
Supplier: Quidos Ltd

1. Service summary

SNUG is a property energy-insight service for UK domestic dwellings. It uses official EPC information where available and generates an up-to-date estimated rating and improvement recommendations using a government-approved RdSAP calculation engine. SNUG is available as a web application and as an API for integrations.

If a property does not have an existing EPC, SNUG can use a geospatial lookup to find the nearest comparable property with similar characteristics and use that as a baseline for an indicative result.

2. Who the service is for

Typical users include:

- local authorities and housing teams
- retrofit coordinators and installers
- energy advice services
- organisations running property portfolio analysis
- software partners integrating energy insights into their platforms

3. Service features

- postcode/address property search and identification
- retrieval of official lodged EPC data where available
- RdSAP-based recalculation to generate an updated estimated rating
- tailored improvement recommendations
- what-if scenario modelling through input changes and recalculation
- geospatial comparable-property fallback where EPC data is missing
- API access for partner integrations and automation
- cached results for faster repeat queries

4. Service benefits

- reduces manual effort to obtain and interpret energy performance information
- speeds up identification of retrofit opportunities via recommendations
- enables fast scenario testing without commissioning a new EPC
- supports portfolio-scale analysis via API integration

- improves consistency by using a standard calculation approach

5. Service interfaces

SNUG can be accessed via:

- Web interface: browser-based results and what-if interaction
- API interface: HTTPS endpoints returning structured responses (JSON/XML)

API highlights (summary):

- API key authentication via request header X-API-KEY
- content negotiation via Accept header (application/json or application/xml)
- supports UPRN-based retrieval and OS Places address payload workflow
- supports recalculation by submitting updated Derived RdSAP inputs

OpenAPI specification: [TBA]

6. Onboarding and setup

Web interface:

- users access SNUG via a supplied URL and follow onboarding instructions provided by Quidos
- authentication model (if any): X-API-KEY where no personal data is handled, can integrate with Key Cloak where required.

API:

- Quidos issues an API key and provides environment endpoints (DEV/LIVE)
- buyers implement an integration flow (for example: UPRN lookup, or OS Places DPA payload submission)
- buyers are responsible for obtaining and validating OS Places address payloads where that workflow is used

7. System requirements

Web interface:

- modern browser (Chrome/Edge/Firefox/Safari current versions)
- JavaScript enabled
- internet access with TLS 1.2+ HTTPS support

API consumers:

- HTTPS-capable HTTP client
- ability to store and protect API keys
- ability to allowlist SNUG domains if required by network controls

8. Service constraints and dependencies

- OS Places dependency: where using the OS Places workflow, the caller must supply valid OS Places DPA output
- data availability: some outputs depend on the availability and quality of source datasets
- response times / throughput: [INSERT EXPECTATIONS, LIMITS, AND RATE LIMIT POLICY]
- scheduled maintenance windows: None at present.

9. Hosting, resilience and availability

Hosting:

- SNUG is hosted on AWS in the UK (AWS Europe (London) region – eu-west-2)
- service data is stored and processed in the UK

Architecture:

- serverless design using API Gateway and Lambda
- asynchronous failure handling supported using dead-letter queues
- infrastructure-as-code (Serverless Framework / CloudFormation) with CI/CD pipelines for repeatable deployments and rapid rollback

Availability SLA (baseline):

- target availability: 99.0% per calendar month
- measurement method: Cloud Watch log files in AWS
- exclusions: planned maintenance and events outside reasonable control

Service credits (baseline):

- 98.0% to <99.0%: 5% credit
- 95.0% to <98.0%: 10% credit
- <95.0%: 25% credit
- credit application method: Credit applied to next invoice
- claim window: 30 days
- Credits are capped at 25% of the monthly charges for the affected month and are the Customer's sole remedy for SLA breach.

10. Security governance

- certification: Cyber Essentials Plus

11. Information security policies and operational controls

Policies followed for SNUG operations include:

- Information Security Policy
- Access Control and Acceptable Use
- Incident Response
- Vulnerability and Patch Management
- Change Management
- Backup/DR
- Logging/Monitoring
- Data retention/classification

Control implementation includes:

- mandatory MFA; named identities; least-privilege access
- joiner/mover/leaver process
- approvals for production access
- peer review for code changes

12. Configuration and change management

- all service code and infrastructure definitions are stored in version control
- changes tracked through their lifetime using pull requests, version tags, and deployment records
- changes assessed for security impact during review (permissions, data handling, auth, logging, dependency changes)
- changes recorded in JIRA. depending on complexity of issue, it may be a single ticket up to multiple tickets or epic.

13. Vulnerability management (supplier-defined controls)

- threat intelligence sources: AWS Security Bulletins and NCSC advisories
- credential leakage prevention: git-secrets scanning
- tracking: vulnerabilities and actions recorded in JIRA with priorities/ownership

Patch targets (baseline):

- critical/actively exploited: within 48 hours
- high: within 7 days
- medium: within 30 days
- low: within 90 days

14. Protective monitoring

- monitoring of API Gateway and Lambda logs/metrics for anomalies (traffic spikes, elevated error rates, latency, auth failures, timeouts/throttling, DLQ activity)
- CloudWatch alarms generate internal email alerts
- target response: begin investigation within 1 hour for high severity alerts
- actions and evidence recorded in JIRA

15. Incident management

Pre-defined processes:

- runbooks for common events (API errors, dependency failures, DLQ growth, rollback, suspected credential exposure)

User reporting:

- Quidos support helpline
- Freshdesk incident support

Incident communications:

- incident updates for significant incidents (impact, timing, mitigations, current status)
- post-incident report available on request (timeline, root cause, corrective actions)

16. Outage reporting

- internal: CloudWatch alarms to operational email distribution lists
- external: API health-check endpoints can be called by buyer monitoring

17. Access restrictions in management interfaces and support channels

Management:

- AWS IAM and IAM Identity Center with MFA and role-based access control
- restricted administrative access and approval-based production access
- audit logging of administrative activity

Support:

- Freshdesk access restricted to authorised support staff
- helpline and ticket handling includes identity verification before discussing account-specific information
- escalation path for sensitive requests

18. Independence of resources

- API Gateway and Lambda scale elastically to handle demand
- throttling/concurrency controls and queue-based buffering reduce noisy-neighbour risk
- monitoring and alerting to maintain consistent performance under load

19. Data handling, retention and offboarding

- Data classification and retention: No personal data retained in the core dataset; no data retention ruleset defined.

- backups: 24-hour further details on request.
- disaster recovery targets: details on request.
- offboarding: Core dataset will not contain company specific data, if company specific data is ingested as part of ETL process then it would be deleted as per the contract between the two companies.

20. Support

- support hours: Live support hours 9am-5pm Monday to Thursday 9am -4:30pm Friday
- support channels: Quidos phone line 01225 667570 or via support.quidos.co.uk

21. Pricing and commercial terms

- pricing model: See Pricing Documentation
- minimum term: 12 Months
- invoicing: Monthly
- additional services (optional): Onboarding / custom API inputs / Outputs / Data Cleansing / Training

22. Contacts

- Service enquiries: 01225 667570
- Support: Quidos helpline 01225 667570 or support.quidos.co.uk
- Security contact: support.quidos.co.uk