Service Definition – Origin Secured Event Chain & Trust Orchestration Infrastructure

1. Service Overview

Service name: Origin Secured Event Chain & Trust Orchestration Infrastructure
Service type: Trust infrastructure API's and governed administrative gateways

Origin Secured provides trust infrastructure that enables organisations to issue, endorse, and verify cryptographic proofs of information through an event-based trust fabric. The service operates as an overlay to existing systems, allowing trusted assertions to be verified without requiring system-to-system integration or centralised data storage.

The platform enables organisations to issue challenges whilst being able to create, verify, manage and revoke cryptographically signed trust artefacts (e.g., assertions, endorsements, credentials and digital licences) and to maintain an immutable evidence trail of trust decisions and lifecycle events.

Typical outcomes include:

- Verifiable "proof of authority" at the point of action (not assumed by session/login alone)
- Reusable assurance evidence that can be verified across delivery partners without re-running checks or sharing underlying data
- Deterministic revocation and governance of credentials/permissions
- Reduced need for bespoke trust, audit and verification components in each programme

---

2. What the Service Does

The service provides the following core capabilities:

- Creation and lifecycle management of cryptographically signed assertions and digital licences, issued and endorsed by recognised authoritative organisations rather than by the platform itself (issue, update, expiry, suspension, revocation)
- Deterministic, tamper-evident recording of trust events using an event chain based on cryptographically signed events and verifiable references, without transactional semantics
- Verification APIs for relying parties to validate artefacts and current status (including revocation)

- Support for governance through contextual assertions and digital licences that allow relying systems to enforce their own policies based on verifiable trust evidence (organisations, roles, permissions, rules)
- Fine-grained access control and consent-led data sharing
- Evidence support for audit and regulatory reporting (traceable event history)

---

3. Service Scope

Included

- UK-hosted cloud trust infrastructure
- Tenant configuration, artefact management, event logging and provenance
- Governance controls through administrative gateways
- APIs for integration with external systems and delivery partners

Not Included

- Primary identity proofing / KYC checks (performed by accredited third parties)
- Issuance of government identity documents
- Buyer-specific business process automation or bespoke line-of-business applications
- On-premise deployment

Primary identity checks are performed by accredited third-party providers and consumed by the infrastructure software as verifiable inputs.

---

4. Intended Users

The service is intended for:

- Central government departments
- Arm’s length bodies and regulators
- Local authorities
- Public sector delivery partners
- Accredited identity, assurance, and audit providers

Users interact with the service through:

- API-based administrative gateways
- Secure APIs for system-to-system integration
- Mobile Application

---

5. Deployment Model

Origin Secured is delivered as cloud-hosted trust infrastructure, providing logically isolated trust domains that are independently governed and managed by communities and authorities through administrative gateways and APIs.

Where hosted by Origin Secured, the infrastructure operates within UK-based cloud environments suitable for public sector use, with cryptographic separation and access controls enforced between trust domains. Origin Secured does not have access to customer data, licence payloads, or endorsement content. Data is encrypted and controlled by the relevant authorities or communities, and is only accessible to parties explicitly authorised by them.

---

6. Security

Security is designed into the service by default and includes:

- Encryption in transit using industry standard protocols
- Encryption at rest in the cloud environment
- Strong authentication and role-based access control
- Cryptographic signing of trust artefacts and events
- Immutable, append-only event records
- Centralised logging, monitoring and alerting

The service is designed to align with recognised security frameworks including ISO/IEC 27001 principles and NIST Zero Trust Architecture.

---

7. Data Protection and Privacy

Origin Secured supports GDPR-compliant processing and privacy by design.

Key characteristics include:

- Data minimisation and selective disclosure patterns
- Separation between event metadata and underlying data payloads
- Configurable retention and deletion policies
- Support for correction and revocation workflows
- UK data residency

The service can operate as a data processor or data controller depending on the buyer's configuration and use case.

---

8. Availability, Resilience and Disaster Recovery

The service is designed for high availability and resilience through:

Resilience & DR Controls

Capability	What is provided
Redundancy	Redundant cloud infrastructure for critical components
Backup	Automated backups of service data and configurations
Recovery	Documented recovery procedures to restore service after failure
Monitoring	Centralised monitoring and alerting for availability and performance
Disaster Recovery	Documented DR procedures covering restoration steps and communications

Availability Commitment

Item	Definition
Service Availability Target	**99.9% per calendar month (production instances)**
Service Window	**24x7x365**
“Available” means	**Service is reachable and usable for normal operation via published interfaces**

Measurement period	**Calendar month**
Calculation	**Availability (%) = 100 × (Expected Availability − Unexcused Downtime) / Expected Availability**
Reporting precision	**Expressed to one decimal point, rounded to nearest 0.1%**
Scope	**Availability applies to production instances only**

Availability is expressed to one decimal point, rounded to the nearest one-tenth of a percentage point.

Planned maintenance is normally performed outside UK business hours where reasonably possible. Availability commitments apply to **production** instances of the Software.

---

9. Support Model

Support Channels & Hours

Item	Detail
Support channels	Online case portal (primary), phone, email (emergency support only)
Standard hours	09:00–17:00, Monday–Friday (UK time), excluding UK public holidays
Out-of-hours	Emergency phone support for Critical incidents affecting production availability/outages

Scope	Technical support for errors and technical issues relating to Software operation
Exclusions	Implementation services, programming, bespoke report generation, customer environment issues unrelated to Software

Severity Levels

Priority	Definition (summary)
Critical	Production service down / business-critical functionality inoperable for all users; no workaround
High	Major functionality impacted or severe degradation; impacts many users/major workflows; no reasonable workaround
Medium	Service usable; non-critical functional impact; workaround may exist
Low	General usage questions / feature requests; no functional impact

Response, Resolution & Update Targets (Business Day targets)

Priority	Initial response target	Target time to workaround/resolution	Update cadence
Critical	1 hour	4 hours	Every hour until workaround or resolution
High	4 hours	10 days	Daily until workaround or resolution

Medium	1 business day	14 days	Every 3 business days until workaround or resolution
Low	1 business day	30 days	Every 5 business days until workaround or resolution

Notes:

- Targets apply during Business Days and are not a guarantee of performance.
- OS may reclassify severity where evidence indicates a different impact level and will notify the Customer with reasons.
- Availability and support commitments apply to production instances unless otherwise agreed.

---

10. Onboarding and Offboarding

Onboarding

- Tenant setup and access provisioning
- Initial configuration and governance setup
- Integration support via APIs
- Documentation and implementation guidance

Offboarding

- Export of customer data in agreed formats
- Secure deletion of customer data
- Termination of access credentials

---

11. Service Constraints and Dependencies

- Internet connectivity required
- Integration via documented APIs
- Dependency on third-party identity or assurance providers for primary verification

---

12. Pricing Model (Summary)

Offered on subscription and/or usage-based pricing depending on configuration; pricing is defined in the G-Cloud Pricing Document.

---

13. Compliance and Standards Alignment

The service is designed to support alignment with:

- UK GDPR
- Digital Identity and Attributes Trust Framework (DIATF)
- Government Security Principles
- Public sector audit and assurance requirements

---

14. Service Summary

Origin Secured provides reusable, UK-hosted trust infrastructure that enables public sector organisations to implement digital trust, assurance, and governance securely and consistently across multi-party ecosystems—without building bespoke trust systems for each programme.