REPLY

SECURE INTEGRATION, IDENTITY & API MANAGEMENT SERVICES

Service Definition
G-Cloud 15

REPLY
38 Grosvenor Gardens - London SW1W 0EB - United Kingdom - tel +44 (0) 207 730 6000 - fax +44 (0) 207 259 8600
infouk@reply.com

www.reply.com

TABLE of CONTENTS

SERVICE DESCRIPTION

Many public sector organisations expose and consume integrations through APIs and identity mechanisms that have evolved over time without consistent standards or governance. As a result, interfaces are often secured inconsistently, access controls are unclear, monitoring is limited and audit evidence is difficult to produce. This creates unnecessary security risk, slows delivery and makes it harder to safely share data across cloud, hybrid and legacy environments.

Reply's Secure Integration, Identity & API Management Services for G-Cloud 15 address these challenges by embedding security, governance and operational control into the design and operation of integrations. We enable organisations to exchange data safely, reliably and at scale, while meeting public sector security, privacy and assurance requirements.

Our service takes a secure-by-design approach to APIs, identity and integration platforms, covering architecture, build, deployment and ongoing operation. Security controls are embedded from the outset rather than added late, ensuring integrations are compliant, auditable and resilient without becoming barriers to delivery.

Crucially, we balance protection with usability. By establishing clear standards, reusable patterns and consistent governance, we help organisations move faster with confidence, enabling interoperability and reuse while maintaining strong security and compliance over time.

FEATURES
Our service combines secure integration engineering, identity and access management, API governance and continuous monitoring to create controlled, auditable and scalable integration ecosystems.

- **Secure API Design and Management**
  We design and manage APIs using secure, standardised patterns that protect data while enabling reuse. Security controls such as authentication, authorisation, throttling and traffic management are applied consistently across APIs to reduce risk and simplify governance.

- **Identity and Access Integration Services**
  We integrate identity and access controls across systems and platforms, ensuring users, services and applications are authenticated and authorised consistently. This reduces reliance on shared credentials and supports least-privilege access across integrations.

- **API Governance and Lifecycle Management**
  We establish governance across the full API lifecycle, from design and publication through versioning, deprecation and retirement. This ensures APIs remain consistent, secure and reusable while preventing uncontrolled growth and technical debt.

- **Monitoring, Logging and Audit Capabilities**
  We provide centralised monitoring, logging and audit across APIs and integrations, delivering visibility into usage, performance and security events. This supports both operational management and formal assurance requirements.

- **Compliance with GDS and GDPR Requirements**
  Our designs align with GDS guidance, GDPR and public sector security expectations. Compliance is supported through design patterns, documentation and audit trails rather than manual evidence gathering.

- **Secure Data Exchange Across Systems**
  We enable secure data exchange across cloud, hybrid and on-premise systems, embedding encryption, access controls and policy enforcement to protect sensitive information in transit.

- **Threat Detection and Security Monitoring**
  We configure monitoring and alerting to detect abnormal behaviour, misuse or potential security threats across integration platforms. This supports faster investigation and response to incidents.

- **API Performance Optimisation**
  We balance security with performance by optimising API configurations, caching, throttling and routing. This ensures integrations remain responsive while maintaining protection.

- **Integration Security Documentation**
  We produce clear documentation covering API usage, security controls and operational procedures, supporting transparency, auditability and ease of reuse.

- **Ongoing Security Optimisation and Support**
  We provide ongoing review and optimisation of security controls to ensure integrations remain effective as threats, platforms and usage patterns evolve.

BENEFITS

Our Secure Integration, Identity & API Management Services enable public sector organisations to share data and services confidently, without introducing unmanaged risk, security gaps or compliance overhead. Security becomes a foundation for delivery rather than a constraint.

- **Reduced Exposure to Security Threats**
  Unmanaged APIs and inconsistent integration security create an expanding attack surface. By applying secure-by-design patterns, consistent authentication and centralised control, organisations significantly reduce the risk of unauthorised access, data leakage and misuse. Security controls are applied uniformly rather than relying on individual project implementations.

- **Improved Control Over System and Data Access**
  Integrated identity and access management ensures every user, system and service has access only to what it is permitted to use. Fine-grained access controls, token-based authentication and service identities reduce reliance on shared credentials and manual access management, improving accountability and auditability.

- **Consistent API Quality, Security and Reuse**
  API governance ensures APIs are designed, documented and secured to consistent standards. This improves quality, prevents duplication and enables safe reuse across teams and suppliers. As a result, integrations become easier to consume and maintain without compromising security.

- **Improved Operational and Security Visibility**
  Centralised monitoring, logging and audit capabilities provide visibility into who is accessing APIs, how integrations are behaving and where risks are emerging. Operational teams can detect abnormal behaviour early and investigate incidents using clear, reliable evidence.

- **Reduced Regulatory and Compliance Risk**
  Compliance with GDS guidance, GDPR and public sector security expectations is built into the design of integrations rather than addressed retrospectively. Audit trails, access logs and documentation provide clear evidence for assurance, reducing the cost and effort of audits and reviews.

- **Better Control Over Integration Growth**
  Without governance, integrations grow organically and become difficult to manage or retire. API lifecycle management enables organisations to control how integrations are introduced, changed and decommissioned, reducing technical debt and long-term operational risk.

- **Faster Detection and Response to Security Incidents**
  Threat detection and alerting enable security events and misuse to be identified quickly. Faster detection reduces the window of exposure and supports rapid containment and remediation, limiting impact on services and data.

- **Improved Confidence in Interoperability**
  Well-governed, well-secured APIs enable safe interoperability across departments, organisations and suppliers. Teams can integrate confidently, knowing security, performance and compliance requirements are enforced consistently.

- **Faster and Safer Onboarding of New Services and Partners**
  Clear standards, reusable patterns and comprehensive documentation reduce the effort required to onboard new services, suppliers or delivery partners. Integrations can be established quickly without reintroducing security risk.

- **Sustained Security as Platforms and Threats Evolve**
  Ongoing monitoring, optimisation and review ensure security controls remain effective as technology platforms, usage patterns and threat landscapes change over time.

WHAT THE SERVICE INCLUDES

Reply delivers a comprehensive, end-to-end service that embeds security, governance and operational control across the entire integration and API lifecycle.
The service is designed as a continuous operating capability rather than a one-off implementation.

1. Discovery and Security Baseline Assessment

We begin by establishing a clear understanding of the current integration landscape. This includes reviewing APIs, integration flows, identity arrangements and access controls to identify inconsistencies, unmanaged risk and technical debt.
Activities include:

- Mapping existing APIs, integrations and data exchanges
- Assessing authentication, authorisation and credential practices
- Identifying gaps against public sector security expectations
- Understanding regulatory and assurance requirements

This creates a practical security baseline on which improvements can be prioritised.

2. Secure Integration and API Architecture Design

We design secure-by-design integration and API architectures that balance protection with usability. Designs are based on proven patterns that simplify security, governance and operations.
Design activities include:

- Secure API patterns and standards
- Identity, token and authorisation models
- Encryption and transport security
- Throttling, rate limiting and resilience controls

Architectures are aligned with GDS guidance and public sector security principles.

3. Identity and Access Management Integration

We integrate enterprise identity providers and access management services across APIs and integrations. This ensures consistent enforcement of identity and access policies for users, systems and services.
This includes:

- Service-to-service authentication
- Role-based and attribute-based access controls
- Token management and credential handling
- Support for federated access models

4. API Management Platform Implementation and Configuration

We implement and configure API management platforms to provide centralised control over API exposure and consumption.
This includes:

- API publishing, versioning and retirement
- Access control and subscription management
- Developer onboarding and documentation
- Policy enforcement for security and traffic management

API management reduces fragmentation and enables safe reuse.

5. Monitoring, Logging and Audit Enablement

We enable end-to-end visibility across APIs and integrations, supporting both operational management and formal assurance.
Capabilities include:

- Detailed access and usage logging
- Performance and error monitoring
- Audit trails for compliance
- Dashboards for operational and security insight

6. Threat Detection and Security Monitoring

We configure monitoring and alerting to identify abnormal patterns, suspicious access and potential security threats.
Activities include:

- Alert configuration and tuning
- Integration with security operations where required
- Support for investigation and response

7. API Performance and Scalability Management

We monitor and optimise API performance to ensure security controls do not negatively impact usability or scalability.
This includes:

- Latency and throughput monitoring
- Caching and throttling optimisation

- Capacity and scalability review

8. Governance, Standards and Lifecycle Control

We establish governance frameworks that define how APIs and integrations are designed, approved, changed and retired.
This includes:

- Design and security standards
- Lifecycle and change management processes
- Ownership and accountability models

Governance ensures long-term control and sustainability.

9. Documentation, Knowledge Transfer and Enablement

We produce clear, practical documentation covering security controls, API usage and operational procedures. Knowledge transfer supports internal teams and reduces dependency on individuals or suppliers.

10. Ongoing Security Optimisation and Support

We provide ongoing review and optimisation of security controls to ensure they remain effective as platforms, threats and usage patterns evolve.

WHY THIS MATTERS
Together, these services turn integration security from a delivery blocker into a strategic enabler. Organisations gain confidence that data sharing and interoperability are controlled, compliant and resilient, allowing teams to move faster while protecting sensitive information and public trust.

ONBOARDING

Kick-Off Meeting

When we start an engagement with a new client, we begin with a workshop introducing the team (from both Reply and the client), the project objectives, and our anticipated timelines and approach. This workshop is most impactful when the majority of client stakeholders involved in the project are present and involved (either in person or remotely). Where this is impossible, we can hold separate sessions with teams that cannot participate in the kick-off workshop to ensure all stakeholders are engaged and bought into the project's objectives.

Account Management

Designated Account Manager

Each client has a designated Account Manager, who will be the main point of contact throughout the engagement. This individual is responsible for ensuring that delivery progresses and is executed to the standards that Reply and our clients expect.

Fortnightly review meeting

Alongside regular ceremonies and informal daily interaction between the Reply project team and the client, we hold formal review meetings with key stakeholders, usually fortnightly. This includes critical client stakeholders, senior Reply project team members, and the Reply Account Manager. Where appropriate, these meetings will consist of a review of work completed and demonstrations or walk-throughs of deliverables.

Offboarding

Where an engagement continues to completion, unless the client requests an extension or new engagement, all client IT, documents, artefacts and deliverables will be returned to the client. Our team will ensure a complete handover of data and knowledge to client staff. An ongoing support or retained advisory service may be implemented where appropriate to provide additional continuity.

Access to Data

Ensuring secure access to client data upon exit is paramount to maintaining confidentiality and integrity. We begin by conducting a comprehensive inventory of all client data stored within our systems, encrypting it both in transit and at rest using industry-standard protocols. Strict access controls and authentication mechanisms are implemented to restrict access to authorized personnel only, with permissions regularly reviewed and updated. Client data is segregated from other data within our systems, ensuring isolation and protection. Upon exit, all access rights to client data are promptly revoked, including user account deactivation and permission removal. If requested, we securely delete or anonymise client data in accordance with retention policies and regulatory requirements. Detailed documentation and audit trails of data access are maintained, providing transparency and accountability. Before exiting, we verify with the client that all necessary data access has been revoked. Finally, we adhere to legal and regulatory obligations regarding data protection and privacy, ensuring compliance with contractual agreements and applicable laws such as GDPR or HIPAA. Through these measures, we ensure that client data remains secure throughout the exit process, mitigating the risk of unauthorized access or data breaches.

SECURITY

Personnel Security

As a Specialist Cloud Service, the capability being offered is not limited to specific Impact levels (as it is not infrastructure, software or a platform) and can be used, subject to personal Security Clearance levels.

Reply consultants are mostly Security Cleared (SC), some have higher-level Developed Vetting (DV) clearances. We also have a pool of NPPV3 Consultants for Policing work. The majority of our work for both public and private sector clients is at IL2 but we work in the Official, Secret and Top-Secret domains.

Our hard and soft information security processes have been designed and approved by independent CESG CLAS accredited consultants.

Information Security

We are ISO27001, Cyber Essentials certified and our Quality Assurance processes are based upon and compliant with our ISO 9001 accreditation. Our Information Security processes are directly guided by our ISO27001 accreditation. We shall adhere to local information and other security policies and will apply local Security Operating Procedures (SyOPs) as may exist. If such do not exist we shall apply our own SyOPs.

Physical Security

The Main Reply Office (London, UK) is a Police Accredited Secure Facility (PASF) with access controls for each point of entry. All Laptops/Phones must be stored securely overnight. When working on a client-site our consultants adhere to client security policies.

TRAINING & KNOWLEDGE TRANSFER

We enable customer teams throughout delivery by embedding knowledge transfer alongside implementation activities. Training is aligned to organisational roles, ensuring relevance for finance users, operational staff, and system administrators.

Knowledge transfer is delivered through:

- A train-the-trainer approach to establish internal subject matter experts.
- Technical training for administrators covering configuration, security roles, and integrations.
- Walkthroughs of system design, data structures, and operational processes.
- Provision of comprehensive documentation, including user guides and runbooks.

Formal training is supported by ongoing access to expert guidance during delivery and early life support. Where required, refresher sessions or additional enablement can be provided to support organisational change or onboarding of new users.

ORDERING AND INVOICING PROCESS

To begin the process, please contact glue.frameworks@reply.com with details of your organisation, role and high-level requirements.

Our Framework Manager will connect you to our experts and from here we will organise an introductory discussion to go into more detail and shape a proposed engagement that suits your needs.

We invoice for both fixed price and time and materials engagements one month in arrears. For fixed price engagements, this takes place upon completion of the deliverable(s), or in stages, if the size of the engagement is greater than £40,000 excluding VAT.

Payment terms are 30 days net of receipt of invoice.

CUSTOMER RESPONSIBILITIES

To deliver our responsibilities as a partner, we require the following:

- Full access to systems and data that are relevant to the specific project
- Reasonable and timely access to key stakeholders and internal SMEs for information gathering, requirements definition and other critical tasks associated with the delivery of our outputs

Technical and Client-Side Requirements

Other than the system access specified above, there are no specific technical or client-side requirements that would limit our capacity to begin work.

Outcomes and Deliverables

Our engagement's specific outcomes and deliverables will be determined during the scoping phase before beginning the project based on your goals and objectives and the level of depth you require. These will include:

- Workshop(s) to discuss and assess the existing architectural design
- Detailed assessment of design with identification of risks and opportunities
- Report with recommendations and proposed action plan

ABOUT REPLY

Reply is a company that specialises in Consulting, Systems Integration and Digital Services with a focus on the conception, design and implementation of solutions based on the new communication channels and digital media.

Reply partners with key industrial groups in defining and developing business models made possible by the new technological and communication paradigms such as Artificial Intelligence, Big Data, Cloud Computing, Digital Communication, the Internet of Things and Mobile and Social Networking. In so doing, it aims to optimise and integrate processes, applications and devices.

Reply's offer is aimed at fostering the success of its customers through the introduction of innovation along the whole economic digital chain. Given its knowledge of specific solutions and due to a consolidated experience, Reply addresses the main core issues of the various industrial sectors.

Through its network of specialist companies, Reply supports some of Europe's leading industrial groups in Telco & Media, Industry & Services, Banks & Insurance, and Public Administration to define and develop business models, suited to the new paradigms of Artificial Intelligence, Big Data, Cloud Computing, Digital Media and the Internet of Things.

We make innovation happen.

We started with a small team and a purpose: to help the digital revolution happen. Today, we are a team of more than 14,600 people in 16 different countries but we still have the same DNA, made up of agile, vertical task forces and an inner passion for innovation.

We are a decentralised network of specialised companies.

Among Replyers, you will find passionate geeks, visionary strategists, and creative minds, each with sharp skills in a specific business, who cooperate together and never stop learning from each other.

Make forward, act sustainably.

We know a sustainable future is possible and technology can be a strong asset to reach it. As leaders in digital transformation, we push for change and operate in full accordance with the highest ethical standards and with respect for the rights of future generations