responsiv

simple · effective · distinctive

Responsiv Cloud
Open Finance Gateway

RA0023M-PD

Product Description

Responsiv Cloud Open Finance Gateway

Responsiv Cloud Open Finance Gateway is an API hosting service configured and managed to standards of resilience and security expected by Financial Services organisations.

All components of the service, including hosting, data storage, and support are delivered from the United Kingdom. The service includes fundamental capabilities needed to support, monitor, manage, and maintain Open Banking and Open Finance APIs.

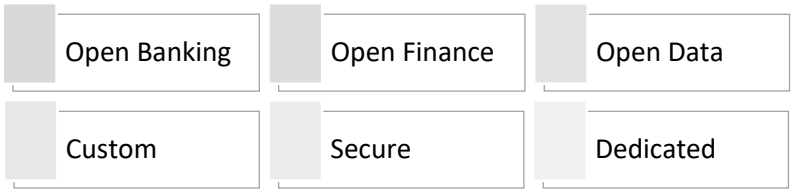
The gateway requires installation of an API Pack to support specific API sets and standards required. Packs are currently available for various versions of Open Banking UK APIs, and Dutch Tax AML APIs.

This product description describes the key features, functions, and capabilities of the product or service. It is not intended to fully document the product or to provide support.

Table of Contents

Service Overview

Responsiv Cloud Open Finance Gateway (RC-OFG) is a secure hosting service with built-in capabilities and management practices to support Open Finance APIs. Packs of APIs are available to extend the service capabilities depending on type of financial organisation.



Open Banking

Open Banking encompasses all aspects of access to bank account information and making payments through programming interfaces.

Users consent to share their banking data and authorise transactions through third party applications. In the United Kingdom Open Banking is led by the Open Banking UK organisation, which publishes standards that Responsiv consider to be robust and mature.

Other standards are available, however, in the UK, adherence to the established standards help assure security and interoperability. Responsiv can develop Open Banking interfaces that can be used and conform to standards of other countries and standards by request.

Open Banking is gaining popularity because the quality of applications and flexibility they represent is generally very good, and in the UK, bank branches are becoming a rarity. The technology allows faster, more secure transactions, and extends the hours of business beyond the working day.

Open Banking in Europe and the UK is governed by the Payment Services Directive version II (PSD2) and Access to Account (XS2) regulations, which regulate the exchange of data between third-party providers and the respective banks.

The current EU Payment Services Directive (PSD2) set forth by the European Banking Authority (EBA) enables certified third-party providers (TPP) to access, with appropriate consent, account information and trigger payments.

Use cases include the ability to aggregate accounts from several banks into a single view, development of self-service capabilities, extending payment options, accelerating the opening of new accounts, and enabling instant credit checks.

The Responsiv Cloud Open Banking API Pack (RA001KE) is the foundational API pack required to support account information and payment initiation APIs required to achieve PSD2/XS2 compliance. APIs are documented and include sandbox support for developers.

- RA001KE-PD Responsiv Cloud Open Banking API-315 Pack
- RL000NE-PD Responsiv Consulting

Open Finance

Open Finance is a data-sharing model that can be used by financial institutions to share information about debt (loans and mortgages), equity, pensions, and other instruments from banking and other sources and third parties.

It is a principle that consumers always own and control their data by giving and rescinding consent, which means the data is authenticated and validated.

The European Commission has published the draft proposal of a Payment Services package, including the third Payment Services Directive (PSD3). PSD3 focuses on the authorisation and supervision of Payment Institutions (PIs) and Electronic Money Institutions (EMIs).

The breadth of possible requirements for Open Finance APIs is breath taking, however, the basic security and authentication, consent management, validation, and routing is the same as for Open Banking. The Responsiv Open Finance Gateway implements the foundation to accelerate development and assure robust and secure solutions.

Use cases include the ability to tailor and personalise financial products, share information to accelerate credit checks and progress purchases, providing customers with access to their transaction histories.

- RL000NE-PD Responsiv Consulting

Open Data

Open Data is the sharing of data by consumers with companies, and governments with citizens. Open Banking and Open Finance are functionally focused with data sharing as a secondary element. Open Data takes a data-oriented perspective about any information that is held by organisations but conceptually owned by an individual.

In principle, Open Data allows a holistic view of financial and other data to be created in real time. For example, gather information about store cards, tax situation, and financial holdings and liabilities.

Digitisation and contactless payments are convenient but can create a gap between the individual and their financial situation, causing them to need to remember to ask the question. Open Data and Open Finance can be used to develop new ways to protect and inform people of their financial status.

Custom

The Responsiv Cloud Open Finance Gateway will be extended using additional packs by request to support the needs of financial service organisations. This may be achieved with standardised packs like the Responsiv Cloud Open Banking API Pack, or by developing customised API and other features, for example collaborating partner data transfers, regulatory APIs, providing partners with access to payment services.

Additional APIs can be added to support specific requirements using the optional Responsiv Consulting products.

Secure

The gateway implements OIDC Hybrid flows to secure APIs, as well as multi-factor authentication, consent management, secure integration with Open Banking UK, and mutually authenticated connections with third parties that use the APIs.

All API traffic is audited, and the availability is monitored for reporting purposes. All service request tickets raised by the gateway itself, or manually, are immutable and controlled by the Responsiv Service Desk.

Connections between the gateway and Client-Side Bridge (CSB) are mutually authenticated, encrypted, and controlled by firewalls to prevent manual access from either side to the other.

Trust Interceptors can be configured to protect API access to services. The service also supports standard API protective protocols, including OAuth2, OpenID, JWT.

This platform has its own inbuilt security arrangements that are separate from the standard Responsiv Cloud Security Service.

Dedicated

Each Responsiv Cloud Open Finance Gateway is a dedicated, single tenant installation on the Responsiv Cloud. This is done to assure that data is properly controlled, and that security access can be separated by customer for administration and other purposes.

Having dedicated installations also means that customers can customise and extend their installation without impact or risk to other customers and can scale independently of other concerns.

On the Responsiv Cloud, each Responsiv Cloud customer is assigned their own “Customer Place”.

This is a walled garden network environment that is private and secure and may span multiple physical locations. Customer places are protected by state-of-the-art firewalls, governance, and management practices. Cloud services and cloud platforms are made accessible from the Customer Place to simplify construction of installations that involve more than one capability.

Responsiv Cloud Platforms are deployed or attached to the customer’s place, creating a secure region of capabilities that can be connected.

Underlying Software

This description is for a Responsiv product that is implemented using a combination of capabilities delivered by pre-existing products. References to those products and their documentation are required to improve understanding of the capabilities that are available and how to access them using the available tooling. Responsiv makes no claim that our product provides all documented features. If a feature is of particular interest, please seek clarification with Responsiv.

Developers use a low-code graphical development environment that allows them to move into Extended SQL, Java, and other languages that may be more appropriate for a particular problem, or that already exist and can be reused.

Accessing the Service

The service is hosted in Responsiv Cloud datacentres located in the UK and accessible over the public Internet or using optional dedicated MPLS[1] connections. Refer to Cloud Service Terms and Conditions for information about hosting providers.

Public Connections

Third Party Connections are used by trusted third parties that are accessing the platform from the public, untrusted, internet.

Responsiv Cloud Open Finance Gateway is an internet facing service that allows trusted third parties (TPP) to access APIs hosted on the service. Only authorised third parties can access the API catalogue and they must have a mutually authenticated and authorised TLS connection to do so.

Access to the public is not allowed and will be rejected by the first level of firewall protection.

Data Connections

Data Connections are used by systems inside your private network to connect to and from the Cloud Service using specific protocols. All data connections must pass through a "Client-Side Bridge".

Connections between the gateway and the Client-Side Bridge are tunnelled over encrypted, mutually authenticated virtual private networks (VPN), or transport layer security (TLS) connections. These connections are explicitly allowed through our firewalls from a named set of Internet Protocol (IP) addresses.

User Connections for Consent Management

User Connections are allowed to enable account holders to provide consent for a third party to access their data or initiate actions on their behalf, for example to make a payment.

When a trusted third party makes a request on behalf of an account holder, the consent system is asked for consent. If the consent is not available, then a redirect is sent to the account holder to gain consent. The result is stored for the duration of the transaction or for a permitted time.

Consent is managed on an account basis and accessed on an individual customer basis. Account holders can access the consent management to list consents and revoke them.

Administrative Connections

Administrative Connections are used by our administrators to allow administration of the platform, including patching and upgrades. These connections are not directly accessible to customers or from public internet connections.

Customer Place Connections

Each Responsiv Cloud customer is assigned their own "Customer Place".

This is a walled garden network environment that is private and secure and may span multiple physical locations. Customer places are protected by state-of-the-art firewalls, governance, and management practices.

Responsiv Cloud Platforms are deployed or attached to the customer's place, creating a secure region of capabilities that can be connected. Responsiv Cloud Security Service is attached to each platform and to the Customer Place.

Platforms and Services deployed to the same Customer Place can be connected or clustered to deliver reliable and available business solutions. Platforms and Services deployed in separate Customer Places cannot be directly connected.

User Management

The service is connected through the Client-Side Bridge (CSB) to an appropriate identity store that is fully managed inside the financial organisation. The store is expected to use the LDAP protocol and be organised with account holders in groups that are aligned and named for their accounts (IBAN). Users can be removed or added to the service by adding them to the financial organisation's identity store.

The gateway determines account ownership from an IBAN by requesting the members of the appropriate group.

The customer record must include email address, person name, and other information to allow consent to be procured, and to properly control access.

[1] See optional services

Scope of function and responsibility

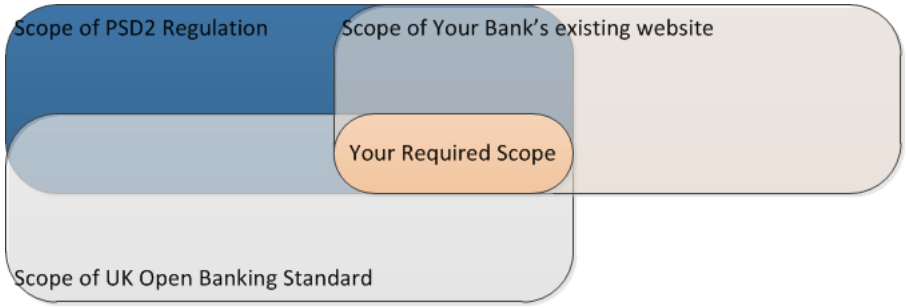
The Responsiv Open Finance Gateway forms a connection between a suitably registered and authorised Third Party Payment Provider (TPP), and the bank. The connection inspects traffic originating from the TPP and checks security markings and other credentials before allowing it to pass to the bank. This includes managing account holder consents and providing test environments for TPP developers. This product does not perform anti-money-laundering, denied parties checking, fraud detection, or any other regulatory or legally required actions. It makes no direct connection to any payment clearing and settlement infrastructure.

The payment provider remains entirely responsible for mandated legal and regulatory actions required prior, during, and after processing the request. Responsiv has no responsibility or liability for the effects of the request after passing it to the bank.

Features

Responsiv Cloud Open Finance Gateway supports the basic functions needed by the API packs to properly operate in a secure and reliable way.

Compliance with the PSD2/XS2 regulations requires in-scope organisations to provide APIs with equivalent functionality to that available through their website for all functionality that is in scope for the regulation as shown in the diagram below.



Organisations using this product as part of a strategy for regulatory conformance remain responsible for all communication with the regulator and for assuring their own conformance. The Responsiv Open Banking as a Service is an enabler and facilitator for you to become compliant with regulations, however it does not make you compliant in and of itself.

Consent and Limits Management

The service checks consent for all actions initiated by the TPP.

Consent is stored and lifecycle managed to allow consent to be given for a single transaction, or for a defined period. Consent is requested by sending an email to the account holder to request consent. Consent management, including granting, revoking, and listing consents is provided by the interface using a one-time password.

Consent management can be extended to set limits on payment values. This is a custom extension.

Open Banking Integration

The cloud service manages certificates and connections with the Open Banking organisation.

Email Notifications and Redirects

Emails must originate from the financial-organisation's own email service. The Client-Side Bridge allows the cloud service to integrate internally to access the email system. Redirections are sent to lead account holders back to the cloud service hosted website that manages the request.

TPP Developer Portal

The developer portal presents a catalogue of available APIs and instructions on how they can be used.

Sandbox

Third Parties that wish to use the APIs can test their implementation using the inbuilt sandbox. The sandbox allows the cloud service to respond with realistic test data to API requests. Routing to the sandbox happens after security checks, which allows the TPP to properly test their processes.

Reporting

Report data is collected continuously about the performance of APIs hosted by the system. Data is intended to provide everything needed for periodic regulatory reports. If anything is missing or the regulations change, then let Responsiv know.

Report Section	This Period	Last period	Year to Date	Notes
Header				
Cloud Service	Responsiv Cloud Open Finance API Packs included. Platform Capacity			
Report Period	From To			
Service Availability	Period Duration Uptime Downtime Available			
API Summary	API Name API Number of Calls API Average Latency API Error Returns API Successful Returns API Average Call Duration API Peak Load/minute	ALL	ALL	
API Detail (Repeats for each API)	API Name API Number of Calls API Average Latency API Error Returns API Successful Returns API Average Call Duration API Peak Load/minute			

Optional Services

This service requires at least one API pack (RA001KE) to be installed. Optional services are available to extend the capabilities or capacity of Responsiv Cloud Platforms and other products.

RA001KE-PD Responsiv Open Banking API-315 Pack

This pack contains a set of APIs that extend the Responsiv Cloud Open Finance Gateway to deliver the core API functionality needed to satisfy PSD2/XS2 regulations partially or wholly to the stated OBUK API standard. The exact needs to satisfy the regulation will vary depending on your specific website offerings and are subject to change as the regulation changes. In all cases it remains your responsibility to assure regulatory compliance.

RA00CA4-PD Responsiv Unity Client-Side Bridge

This product is used by Responsiv Cloud Platforms to manage secure connections between the internal systems and a Responsiv Cloud Platform. It can be configured to perform integration between standardised API calls made by a cloud platform, and one or more internal systems.

The advantages of having a Client-Side Bridge (CSB) include (1) Protocols can be changed from those used internally (REST, Webservice, RPC, etc) to MQ or compressed formats to pass across the Internet or into the Responsiv Cloud, (2) the bridge is a single point of control for all ingress and egress of data, the indirection allows for internal systems to change their network locations, and be replaced or upgraded, without changes to the Cloud service or platform.

The Responsiv Cloud Open Finance Gateway uses the Client-Side Bridge to secure payment requests and allow the bank to control upgrades and movements of internal systems without impacting the Open Finance Service. In this case, the CSB requires configuration to integrate with the Security, email, DNS, Core Banking System, and Payment infrastructure. This product checks for duplicate payment requests and security features of the request received. It does not perform AML, Denied Parties, KYC or any other regulatory requirements associated with payment processing. The Responsiv Open Finance products do not process payments, they pass requests for payments to payment systems.

RT00094 Responsiv Assist Flex Support

Responsiv Cloud Open Finance Gateway is a supported and fully managed platform.

Responsiv Assist Flex Support is an annual agreement that allows customers to make service requests asking for help with development, designs, problem resolution, and other mentoring and support subjects. This service also allows Responsiv support to extend from the platform to include user applications and other aspects of your installation.

Responsiv Assist Services can be used to configure the gateway and Client-Side Bridges, and to perform service preparation.

RA001RD, RA001SE Responsiv Cloud Connection Service

Create private, dedicated network connections between your systems and the Responsiv Cloud. Improve security, reliability, and performance. Remove the need for VPN and reduce the cost of data egress from Azure and other super-scale clouds. Establish connections from your existing WAN network, such as a multiprotocol label switching (MPLS) VPN, provided by a network service provider. A one-time connection applies.

RL000NE Responsiv Consulting Professional Services

Responsiv Consulting Professional Services can be used to configure and customise the gateway and Client-Side Bridge(s), and to perform service preparation.

RA0028J-PD Responsiv Unity MQ DMZ Gateway

This product complements the Responsiv Unity Enterprise Messaging products and provides a lightweight, secure component that operates in a DMZ to facilitate secure messaging between clouds by allowing secure messaging to pass through a DMZ network topology and architecture. This allows your messaging connections to connect self-hosted systems in your private datacentre to systems in different clouds and to Responsiv Cloud Platforms. This product can participate in MQ clusters and HA configurations.

An initiating queue manager connects to this product network address and passes details of the target queue manager. The product passes the details on by creating a new connection using different port numbers to prevent information about your internal address ranges from leaking across the DMZ. The product does not store any information and does not participate in transactional activity on the channel - making it transparent to the connected end points.

Connections are expected to be secured using TLS controlled in the normal way for IBM MQ Channels. This Responsiv Unity Node includes operating system, port forwarding software and monitoring functionality.

Developer and Administrator Tooling

Not Applicable.

All aspects of the Gateway are managed and maintained by Responsiv.

Service Management

Responsiv manages this service, including active health monitoring, patching, upgrades, and general maintenance. The service is available 7x24.

Service Preparation

Deployment of Responsiv Cloud Open Finance Gateway and Responsiv Unity Client-Side Bridge(s)

A dedicated instance of the platform will be deployed and tested for your use. The deployment will include any purchased API packs.

The optional RA0028J Responsiv Unity MQ DMZ Gateway can be installed to allow a "bounce" through the DMZ if required by the organisation's security department.

RA00CA4 Responsiv Unity Client-Side Bridge is then installed in the trusted part of your network. Client-Side bridges will be deployed according to the agreed pattern. In specific circumstances Responsiv can host the Client-Side Bridge, however this is not recommended.

A minimum of one bridge must be deployed, ideally in your data centre to host integration that is specific to your organisation, network topology, and data representations.

Standard Bridge deployment patterns for a single data centre are (1) One bridge deployed in a single datacentre for basic connectivity, or (2) Two bridges deployed in a single datacentre and clustered for resilience. Multiple datacentres can be accommodated by deploying the same pattern to each location.

DNS Name Attachment

The DNS name that will be used to access the service is generally required to be branded for the financial organisation. Responsiv will provide the information needed for you to create the name.

Branding TPP Portal

The gateway includes consent pages and a TPP developer portal that can be branded with your name and graphics. Basic documentation is also provided without branding of any kind, which can be branded or left as-is.

Responsiv is not responsible for writing documentation, maintaining, or otherwise managing the documents. We will deploy changes on your behalf in response to a service request.

Branding Sandbox Data

Realistic test data is provided that can be branded for the appropriate organisation. By default the bank is Responsiv Bank, and the accounts are randomly named.

Configuration of Responsiv Unity Client-Side Bridge(s)

The Client-Side Bridge (CSB) must be configured to integrate to internal security, and the sources of data and function that are needed to support the API packs installed on the gateway. This can be extended at any time to accommodate customisations and new API packs.

Email Connection

The service requires the ability to send emails using your email address. This requires an email address to be created for this purpose (e.g., OpenFinance@MyCompany.co.uk), and connection to the internal email system. The CSB will receive the email and forward it to the email system. This is used to enable consent management.

Identity Store Connection

The bridge needs to be connected to the security (account holder) system to allow it to associate users with accounts, and to retrieve information about users, including email addresses. This is used to enable consent management.

Support for XS2 APIs

The XS2 APIs require access to transaction information and other data. In most financial cases this is the core banking system that holds account information. The Client-Side Bridge will receive the request for data and must be integrated with the appropriate sources.

Support for PSD2 APIs

The PSD2 APIs require access to the payment infrastructure. This service does not perform any anti-money-laundering (AML), denied party checks, credit checks, or other required functions. Integration to payment services must assure that these things are performed by the payment systems.

Service Level Agreement

This service is supported by Responsiv from our UK offices.

The service includes product/platform support only and is triggered by automated monitoring built into the platform or manually accessed from our website https://responsiv.co.uk/support-hub/support/.

The service level agreement (SLA) for Responsiv Cloud services (RL000F6 Responsiv Support Services Addendum v1.0) can be found here: https://responsiv.co.uk/wp-content/uploads/2023/11/TC-RL000F6-Aug2023-Responsiv-Support-Services-Addendum-v1-0.pdf. The SLA defines support available for the platform including support hours of availability, response times, severity level, Service Down definition, the claim process and other support information. Responsiv provides the Customer with the following availability service level agreement (SLA). Responsiv will apply the highest applicable compensation based on the cumulative availability of the Cloud Service as shown in the table below.

Upgrade and Patching Schedule

We expect to perform a single upgrade annually and to install security and critical patches efficiently as they become available. Patches are categorised as follows:

- Security – Patch specifically or including for a security flaw or weakness.
- Critical – Patch will be required to be applied before support attempts to resolve a problem.
- Optional – Specific function bug resolution. Optional depending on use cases.

Continuous Improvement

Responsiv does not commit to future development or support beyond our contractual obligations. Responsiv Cloud Platforms and Responsiv Cloud Services are continually developed and maintained.

New features may be provided as optional expansions to the base platform, or may be installed as standard.

Format and Charging Measures

This product is available in the following formats:

- Single tenant Responsiv Cloud Service

This product is charged based on the following measures:

- Peak API invocations per second.

Charging measures are based on an annual subscription for the platform and specific APIs supported. API packs include maintenance and support for the included APIs. The gateway annual change includes hosting, software licenses, and managed service.

Capacity is deployed to support a peak aggregate API call rate of 120 API calls per minute with consistent latency performance inside the service. Overage charges will not be added if the number of calls exceed this number, however latency may become unacceptable.

Architecture

The Responsiv Cloud Open Finance Gateway is deployed as a cloud service into a "Customer Place" on the Responsiv cloud.

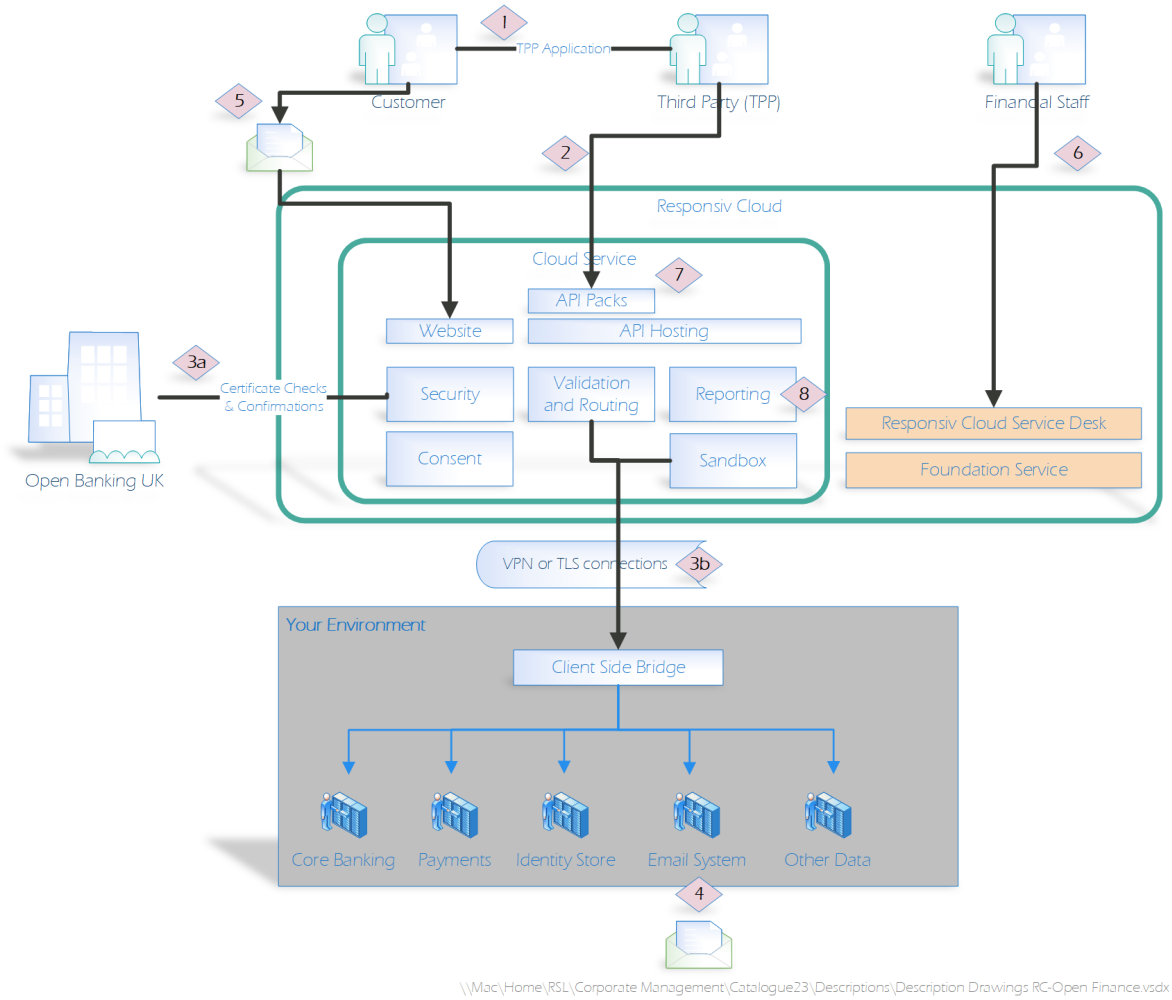


Figure 1; Service Architecture

[1] A financial services customer uses an application provided by a third party (TPP) to request information or action (make a payment). The TPP authenticates with the cloud service and passes the request.

The cloud service inspects the request and [3a] asks Open Banking UK (or alternate) certificate authority whether the certificate and signature are valid.

Assuming that security checks are passed, the request is routed to the sandbox, or over a secure connection [3b] to the Client-Side Bridge.

The Client-Side Bridge passes the request to an appropriate core system for processing and passes the response back to the cloud service.

[4] If the action requested does not have consent, then the identity store will be asked for an email address, which is used to send a consent request [5]. The customer uses the link to access an in-built website to provide consent and to manage pre-existing consents.

[6] Financial Staff can raise questions and highlight problems manually by accessing the Responsiv Cloud Service Desk on responsiv.co.uk/support.

[7] APIs are deployed from an API pack to configure the service to specific requirements for each financial institution.

[8] Reports are generated and made available for regulatory reporting.

Infrastructure Architecture

This service is delivered as a production service only. The implementation is a single-tenant installation with secure separation.

The gateway and service is constructed in a modular format to allow individual organisations to assemble their preferred solution in a consistent and predictable manner. This checklist covers the following modules:

- Responsiv Cloud Open Finance Gateway: Provides the software components needed to support the capabilities of an Open Finance platform.
- API Packs: provide the specific external APIs required by you, for example TPP, Payment, Account Information, Mortgages etc.
- Client-Side Bridge: Once the cloud service is provisioned, connectivity to the bank infrastructure is required. This includes items such as VPN configurations and DNS setting.

Physical Location

Responsiv operate cloud platforms from locations that are hosted by different cloud providers and chosen for qualities of service and benefit optimisation.

Cloud providers include Red Centric, IBM Cloud, AWS, and Microsoft Azure.

Responsiv Platform data processing and data storage is, by default, performed in the United Kingdom.

All data centres used by Responsiv are Tier 3, ISO27001 certified locations, with 7x24 security and electrical backup facilities.

Supported Protocols

Responsiv Cloud Security Service supports the following protocols:

LDAP and Active Directory

Lightweight Directory Access protocol (LDAP) is a standard protocol for accessing directories. It is more commonly used to refer to implementations that include a database and accessed using the protocol. LDAP defines a standard schema to consistently describe characteristics of people and in particular, their usernames and passwords. Active Directory is a Microsoft product that has an LDAP interface and provides identity and access management (IAM).

OpenID Connect (OIDC)

OpenID Connect simplifies verification of user identity based on the authentication performed by an Authorization Server and allows the target system to obtain user profile information using APIs. This is an authentication protocol based on OAuth 2.0.

OAuth 2.0

Open Authorisation (OAuth) version 2.0 is a standard to allow a websites and applications to access resources hosted externally on behalf of a user. It is part of a framework of specifications (IETF RFC 6749 and 6750).

OAuth2 compliant server.

SAML 2.0

Security Assertion Markup Language (SAML) is an XML based language used to describe security assertion/tokens carried in the security header of network connections. Tokens authenticate the user's identity and are understood by Responsiv Cloud Security Service, which can be configured to trust specific issuers. The result is that users can access protected resources without being challenged for credentials.

SAML compliant server.

JWT

JSON web token (JWT) is an open standard (RFC 7519) used to securely transmit information as a JSON object. JWT can be configured to secure APIs on the Responsiv Cloud Platforms.