LIMOSS
London Insurance Market Operations & Strategic Sourcing

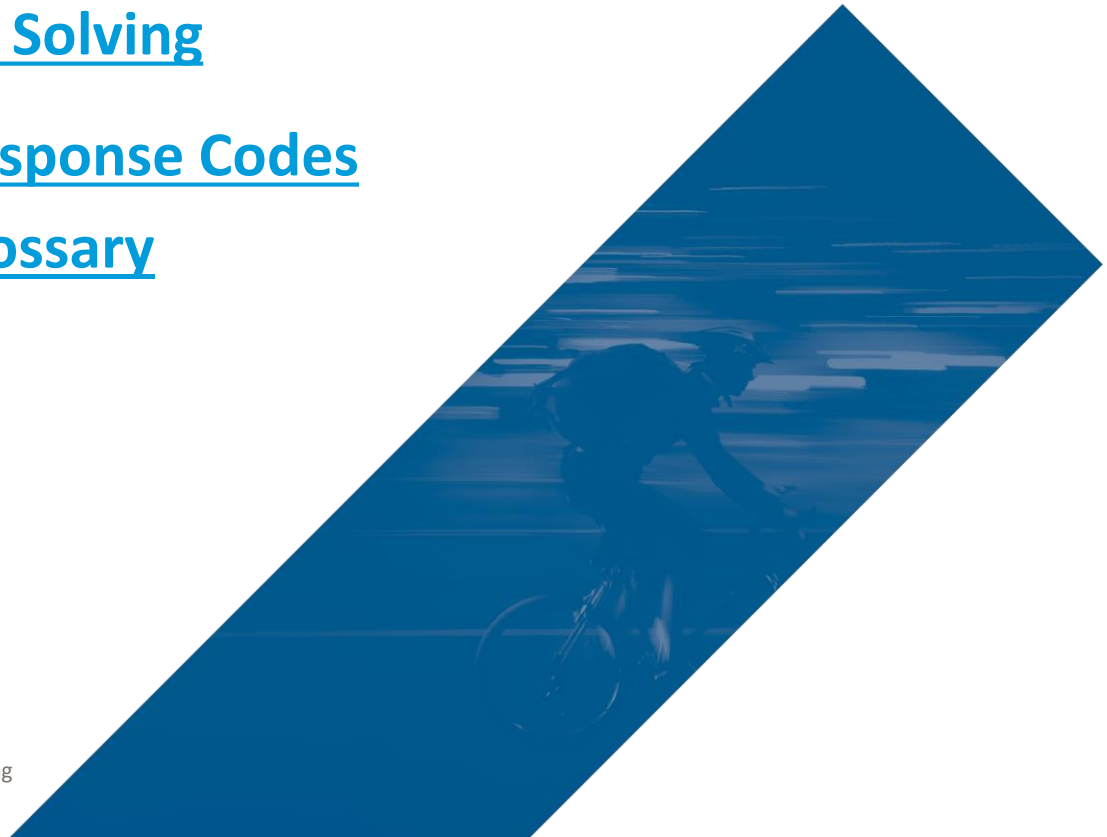
Subscribing to an API

LIMOSS API Gateway

- This document is issued by LIMOSS for guidance purposes. Reasonable care has been taken in providing this information but errors or omissions may exist.
- Queries, corrections and suggested improvements should be sent to the LIMOSS Service Desk.
- All personal and commercial data provided by a Subscriber's organisation, or their partner organisations, whilst using the LIMOSS API Gateway will be processed in accordance with the relevant contractual agreements or the LIMOSS Privacy Notice. LIMOSS will share personal data provided with partner organisations for the sole purpose of delivering the service(s) requested.
- All URLs are correct at time of publishing. LIMOSS is not responsible for external links.
- Documentation is constantly updated. To ensure the latest version is always available, this file should be opened from the LIMOSS website if possible.
- Nothing in this guide is intended to create a new contractual agreement.
- Commercial agreements applicable to this service may refer to LIMOSS SSO, LIMOSS SDE and LIMOSS API Gateway under the term "Common Services".

Oct 2024

Contents



LIMOSS API Gateway

Introduction

LIMOSS API Gateway

A brief introduction

- LIMOSS API Gateway provides a secure, standardised interface for publishing and consuming APIs relevant to the London insurance Market
- A synchronous, RESTful-based API Gateway is provided via Microsoft Azure API Management
- Organisations need to be approved and exist in LIMOSS SSO to be able to use the API Gateway
- "Subscribers" can securely call numerous API Endpoints provided by multiple API "Publishers" E.g., PPL is a Publisher; Vendors/Market Firms are Subscribers
- The API Gateway enforces 4[1] requirements for every API call:
  1. The organisation is known and registered for the API Gateway (using X.509 SSL certs)
  2. You may use any of the following OAuth 2.0 Token Grant flows: On-behalf-of (OBO), Resource Owner Password (ROPC), Implicit, Authorisation Code Flow (ACF) and Client Credentials flow (CCF[1]). If your organisation is not using CCF, the Service account calling the API must be known and authenticated
     - » Depending on how the APIs are published and how the subscribing app is developed, the account may be a service account OR an end user's account
     - » Whichever model is used, the calling account **must** be registered in LIMOSS SSO[2]
  3. The application calling the APIs is registered in LIMOSS SSO
  4. The organisation is authorised by the Publisher to call the specific API
- A successful API call will be passed to the back-end platform E.g., PPL
- The platform may perform additional authorisation checks on the calling account
- A list of response codes and suggested actions is at Annex A
- 3 independent instances of the API Gateway exist: SANDBOX, PRE-PROD and PROD

1 – If your Organisation is using Client Credentials flow; Service account is not required
2 – Alternative STS (Secure Token Service) can be used but this is not recommended

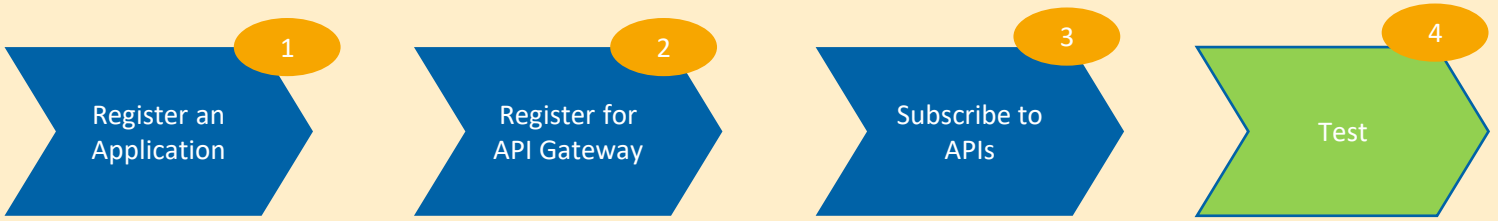
Subscribing to an API

Overview

Subscribe to an API - Hornbill

Individual steps involved in Subscribing to an API

"Subscribe to API" Hornbill Ticket



Your Organisation needs to have been onboarded to LIMOSS SSO with Authorised Contacts and users set up, prior to being able to request to "Subscribe to an API".

For ease, the request has been split into three options, thus allowing flexibility in allowing you to select one or more option at a time, depending on the information you have and what you need to achieve.

Subscribers should subscribe and test in Sandbox[1] and/or Pre-prod prior to Subscribing to an API in Production

If you require any guidance, please contact servicedesk@LIMOSS.London.

Notes

1 - At least one web app or native app must be registered. These apps must adhere to LIMOSS's minimum security standards and successfully clear LIMOSS's security due diligence process. On registration, an App-ID will be generated and depending on your Token grant method, an App-Secret will be passed back to the requestor, as this information is needed when the client app calls an API

2 – The subscribing Organisation must provide a Common Name taken from their X.509 SSL Certificate for each environment

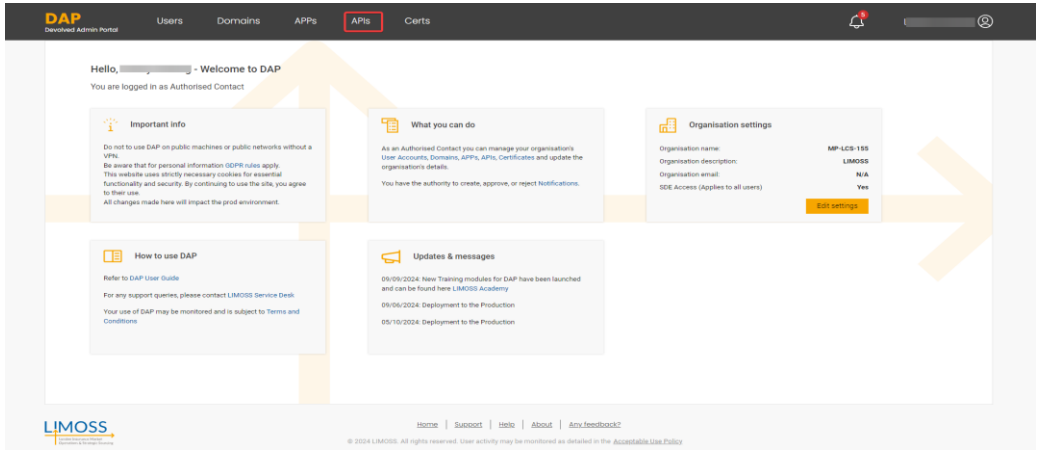
3 – You may then select from the list of API's available in each environment. N.B. You may need to separately sign the API Publishers' commercial agreements. Design/security standards for the Gateway and specific API Specs are available to approved API subscribers

4 – API Publishers may require test evidence before allowing API registration in PRE-PROD/PROD

[1] Some APIs will be available in PRE-PROD and PROD only. Confirm with the API Publisher

Subscribe to an API via DAP

With the introduction of a new version of the Devolved Admin Portal (DAP), Authorised Contacts, or a Dev Manager[1], can Subscribe to an API using the DAP application for their Organisation.



The information required to do this, is the same as if you were requesting a Subscription to an API via the Hornbill form; this method puts the setting up of a Subscription into your own control.

Training material for this new version of DAP can be found via our LIMOSS Academy website, and within DAP itself, you will also find a user guide available to you.

If you require any guidance, please contact servicedesk@LIMOSS.London.

Notes

- The Devolved Admin Portal is environment specific, so you will need to use the Sandbox version, when you are setting up a subscription for Sandbox testing.

[1] Dev Manager is a new role in Devolved Admin Portal which allows the user to manage Apps, APIs and certs for their Organisation.

Information needed

- To successfully Subscribe to an API, you will need to ensure you have the following information:

  - If using a Token Grant method which is not CCF, you will require a Service or user account(s) that will call the API (not required for CCF)
    - See user accounts guidance
  - The Common Name from your X.509 SSL Certificate that will identify your organisation
    - See certificate guidance
  - An Application from where the API call will be made from
    - See application guidance

LIMOSS API Gateway

Useful Information

Useful Information

Certificates

X.509 Certificates

- All organisations using the API Gateway must have an X.509 certificate for each environment
- The Common Name (CN) of X.509 certificate must be shared with LIMOSS
- The same certificate *may* be used in SANDBOX and PRE-PROD (although LIMOSS advise against this)
- The certificate provided for PROD must not be used in SANDBOX or PRE-PROD
- It is the organisation's responsibility to ensure certificates are kept in-date and that any changes to the CN (Certificate Name) are passed to LIMOSS Service Desk 4 weeks in advance
- X.509 certificate must not be self-signed, wildcard or SAN certificate
    - SAN certificates can be used for a single path only
- Certificates must be sourced from a certificate Authority on the Microsoft list of approved CAs
- The decision of which CA to use lies with the subscribing organisation
- LIMOSS does not recommend or endorse any CA

Useful Information cont.

Token Grant Flow Methods; API Specs

Token Grant Flow Methods

- LIMOSS API Gateway supports the following OAuth 2.0 methods: Implicit, Resource Owner Password Credentials (ROPC), Authorisation Code Flow (ACF) and our preferred method, Client Credentials Flow (CCF)
- If you wish to use a Grant Flow method other than CCF, we ask that you have a technical discussion with LIMOSS first, before proceeding
- If you are looking to move from ROPC to CCF, please contact the LIMOSS Service Desk

API Specs

- All APIs published via the LIMOSS API Gateway have an API Specification document/Swagger
- The API Spec will be provided to Orgs, once they have subscribed to a specific API (These will be provided either by the LIMOSS Service Desk or the API Publisher)
- The API Spec details the business use case of the API, how to call it, expected responses and code samples
- LIMOSS is not responsible for the API Specs relating to 3rd party APIs

Useful Information cont.

Throttling; Security Essentials; API Call Logging

Throttling

- Throttling prevents a back-end solution being overwhelmed by a large volume of API calls
- Throttling is activated now for some APIs
- All client apps should be able to handle Response Code 429 (See Annex A)
- Throttling is not an exact science - some calls either side of throttling rate may be accepted/rejected: https://docs.microsoft.com/en-us/azure/api-management/api-management-access-restriction-policies#LimitCallRateByKey

Security Essentials

- Organisations must not share the following information with any 3rd parties:
    - App-ID and App-Secret
    - The password of the Service or user account (if this is required) should NEVER be shared
    - X.509 Private Key
- Inform the LIMOSS Service Desk servicedesk@limoss.london immediately if any of these details are compromised

API Call Logging

- All API Subscribers are advised to include a logging function in their client application
- As a minimum, the logging should include, Date/Time of all API calls; API Response Code; API Transaction ID
- This logging will assist subscribers, LIMOSS and 3rd party API publishers to triage any problems or incidents involving API calls

Useful Information cont.

Email Invitations; Aligning User IDs;

Email Invitations

- All LIMOSS SSO accounts receive an email that they must click to confirm their registration
- All accounts in LIMOSS SSO should have an SMTP email that matches their User ID
- 2 exceptions apply in all Environments:
  - For Service Accounts only: Request user invite link via LIMOSS Service Desk
  - For any account: Use Azure 'Guest Inviter' status as detailed in On-Boarding Guide

Aligning User IDs

- The User IDs registered in LIMOSS SSO should match the User ID held in the market service
- When using a "Native application" (a non-web-based application) in the LIMOSS API Gateway, all user accounts must be created in a managed Azure Active Directory

Contact servicedesk@LIMOSS.London for further details

App Registration – App Type

"Native Apps" and "Web Apps"

Web App

- A Web App is any app or solution that is accessed via a URL

Native App

- A Native App is any app or solution that is not accessed via a URL
- All apps that exist as a standalone instance on a local computer or server are Native

Web Apps vs Native Apps

- The App Type (Web or Native) is needed when registering an App in the LIMOSS API Gateway
- Once registered, the "App Id" will be returned by the LIMOSS Service Desk

An App ID provided for a Web App can NOT be used with a Native App
An App ID provided for a Native App can NOT be used with a Web App

- If Postman is used to conduct Dev/Testing, the Postman App must be registered as a 'Native App' (assuming that it is a local instance of Postman, running on a developer's own computer/server and not a web-based instance of Postman)
- If the solution being developed will be a web-based app (accessible via URL), then this app must be registered as a 'Web App' ***only if*** the web app itself will call APIs
- If the solution being developed is web-based – but it integrates with a native backend app – and only the back-end app calls the APIs, the app must be registered as a 'Native App'
- Contact servicedesk@LIMOSS.London for further advice

App Registration – App Settings

Sign-In URL; App Credentials

Application Homepage URL

- For Native Apps: OPTIONAL: Put https://localhost/[port number] or 'N/A'
- For Web Apps: MANDATORY: Provide the homepage URL for your App

Sign-In URL

- For Native Apps: NOT REQUIRED
- For Web Apps: MANDATORY: Provide the URL where users are expected to sign-in to your app. This URL may also be known as the 'Reply URL' and may be the same as the Application Homepage URL

App Credentials

- Once an App has been registered, the following App Credentials will be provided:
  - Tenant ID
  - App ID (or Client ID)
  - App Secret (or Client Secret)

The App Secret must NOT be included in API calls when using Native apps
The App Secret MAY be included in API calls when using a web app

- App Credentials must be securely protected and never shared with unauthorised parties
- The LIMOSS Service Desk must be informed immediately if App Credentials are compromised

Testing

Pre-Testing Checks

Before running major testing, pre-test API calls should be run to ensure the following 4 criteria:

1 - Valid certificate registered:

- The X.509 cert must be registered in the environment where testing will take place
- The certificate Common Name used in the API call must match the details held by LIMOSS
- The certificate must be in-date and the correct Private Key[1] must be used in the API call
- The organization should acquire the public certificate in .pfx format to successfully conduct connectivity testing with the LIMOSS API Gateway. Note that LIMOSS neither stores nor requests the public file.

2 - Organisation subscribed to API(s):

- The organisation that has registered the certificate must be subscribed to the relevant API(s) in the environment where testing will take place

3 – If you are using a Token Grant method which is not CCF, a Service (or user) account is required:

- The Service (or user) account that will call the API(s) must be registered and activated in the environment where testing will take place
- The accounts must be borne in Azure and must NOT have MFA activated
- To check if an account is registered, log-in to the relevant portal with the account's credentials: Sandbox Portal; Pre-Prod Portal; Prod Portal
- If required, the Service or user account(s) must also be registered with the API publisher

Note – If you are using CCF grant method the need this step is not required

4 - App registered:

- The App used for testing must be registered in the environment where testing will take place
- The correct App credentials must be entered in the API call

1- The Private Key must never be shared with LIMOSS Service Desk or unauthorised parties

LIMOSS API Gateway

Problem Solving

API Call Problems

1) Environment: Confirm which LIMOSS SSO environment the API is being called in: SANDBOX, PRE-PROD or PROD

- The 3 LIMOSS environments are totally separate. Credentials registered in one environment won't work in any other

2) Service or User Account: If using, check the account calling the API is active by logging-in to the relevant portal with the account's credentials: Sandbox Portal; Pre-Prod Portal; Prod Portal

- If the portal can be accessed with the account credentials, the account is active in this environment
- Are account credentials mis-typed in the Postman call or App coding? If needed, is account registered with API publisher?
- Is the account hosted in an Azure tenant and is MFA inactive for the account in that tenant?

3) API subscription: Ask LIMOSS Service Desk to check that your organisation is subscribed to the relevant API in this environment AND ask them to confirm the URI for the API

- Is the API URI provided by LIMOSS mis-typed in the Postman call or App coding?

4) X.509 certificate: Ask LIMOSS Service Desk to confirm the Common Name (CN) for all certificates registered for your organisation in this environment

- Is the certificate "Private Key[1]" mis-typed in the Postman call or App coding?
- Is the certificate in-date?
- Read the guidance on X.509 certs

5) App registration: Ask LIMOSS Service Desk to confirm the App Credentials[1] for the App in this environment AND whether the App is registered as a Native or Web App?

- Is the "App ID[1]" or "App Secret[1]" mis-typed in the Postman call or App coding?
- Is the App being used to call the API the same type (Native/Web) as the App registered in LIMOSS?
- Read the guidance on App types and App Settings

6) Check the API Response Code: If you can make an API call, you will receive an API response code.

- Check the response received against the list of API Response codes and complete the suggested actions

Still not working? Email servicedesk@LIMOSS.London to report an issue (SANDBOX/PRE-PROD) or Incident (PROD)

1- App Credentials & Cert Private Keys must never be shared with unauthorised parties

Trying to call an API?

A successful API call needs the API subscription, the X.509 certificate *and* the client app to be registered correctly in the current environment. The Service or User account, is only relevant for non CCF Token Grant Methods

If any of these components are incorrectly configured, the API call will fail

1 Are the environments aligned?	2 Is the Service[1] or user account active?	3 Is the organisation subscribed to the API?	4 Is the X.509 certificate correctly registered?	5 Is the client app correctly registered?	Successful API Call?
✓	✓	✓	✓	✓	YES ☺
✗	✓	✓	✓	✓	No ☹
✓	✗	✓	✓	✓	No ☹
✓	✓	✗	✓	✓	No ☹
✓	✓	✓	✗	✓	No ☹
✓	✓	✓	✓	✗	No ☹

[1] This is not relevant if you are using CCF


LIMOSS
London Insurance Market
Operations & Strategic Sourcing

Annex A

API Gateway Response Codes

LIMOSS API Gateway Response Codes 1/3

Code	Response	Response Description	Suggested Action
200	OK	Standard response for successful requests	No action needed
400	Error validating token: malformed amr	Error is thrown when the provided token's AMR claim values are incorrect	Client may need to generate a new token. Raise to LIMOSS Service Desk as Incident if necessary.
400	Error validating token: malformed appid	Error is thrown when the provided token's AppId claim value is incorrect	Client may need to generate a new token. Raise to LIMOSS Service Desk as Incident if necessary.
400	Trace header length exceeded	Error is thrown when the provided trace header length is more than 24 symbols	Raise to LIMOSS Service Desk as Incident and client should check the header.
401	Bearer missing in Authorization token	Error is thrown when the provided token Bearer prefix is missed	Raise to LIMOSS Service Desk as Incident
401	Client certificate is missing	Error is thrown when the certificate is missed	Check X.509 Certificate is correct, in date and registered with LIMOSS Service Desk
401	Authorization token is missing	Error is thrown when the token is missed	Raise to LIMOSS Service Desk as Incident; client should ensure Authorization token is included
403	Authorization failed	Error is thrown when the token validation is failed	Raise to LIMOSS Service Desk as Incident. Client may need to generate a new token.
403	Client certificate validation failed: expired certificate	Error is thrown when the provided certificate is expired	Check X.509 Certificate is correct, in date and registered with LIMOSS Service Desk; specifically, certificate expiry date
403	Client certificate validation failed: incorrect start date	Error is thrown when the provided certificate start date is incorrect	Check X.509 Certificate is correct, in date and registered with LIMOSS Service Desk - specifically, certificate start date
403	Client certificate validation failed: untrusted certificate	Error is thrown when the provided certificate is untrusted	Check X.509 Certificate is correct, in date and registered with LIMOSS Service Desk
403	Client certificate validation failed: unknown domain	Error is thrown when the provided certificate CN isn't set in MPO object	Check X.509 Certificate is correct, in date and registered with LIMOSS Service Desk Check that correct domain name has been provided in API Call

LIMOSS API Gateway Response Codes 2/3

Code	Response	Response Description	Suggested Action
403	Client certificate validation failed: empty domain	Error is thrown when the provided certificate CN is missed	Check X.509 Certificate is correct
403	Client certificate validation failed: not authorized to call this API	Error is thrown when the organization isn't subscribed to API that it is calling	Raise a Service request to Subscribe to the API
403	Token validation failed: malformed token or empty issuer	Error is thrown when the provided failed to parse token or token doesn't have issuer	Raise to LIMOSS Service Desk as Incident
403	Token validation failed: expired token	Error is thrown when the provided token is expired	Refresh or generate a new Token
403	Token validation failed: future date	Error is thrown when the provided token's 'iat' or 'nbf' claims contains future date	The client should generate a new token
403	Token validation failed: incorrect audience. Value: <text>	Error is thrown when the provided token audience is incorrect	The client should generate a new token
403	Token validation failed: incorrect SCP claim. Value: <text>	Error is thrown when the provided token's SCP claim isn't 'user impersonation'	Raise a service request to the LIMOSS Service Desk to update the APP permissions
403	Token validation failed: audience is missing	Error is thrown when the provided token audience is missed	The client should generate a new token
403	Token validation failed: missing claims: <text>	Error is thrown when the provided token claims are missed	The client should generate a new token
403	Token validation failed: user domain is not allowed. Email domain: <text>	Error is thrown when the provided email domain isn't set in MPO object	Raise a service request to the LIMOSS Service Desk for onboarding the Email domain
403	Token validation failed: signature validation failure	Error is thrown when the provided token signature is failure	The client should generate a new token
403	Token validation failed: malformed token or empty issuer	Error is thrown when the provided failed to parse token or token doesn't have issuer	The client should generate a new token
403	Token validation failed: application id is not allowed. Application ID: <text>	Error is thrown when the provided application Id isn't set in GW configuration	Raise a service request to the LIMOSS Service Desk for onboarding the CCF APP ID
404	API operations not found	Error is thrown when the provided API operation isn't found	Raise to LIMOSS Service Desk as Incident
429	Throttling Rate Exceeded	The number of calls per min has exceeded the throttling limit set by the API publisher	Wait for number of seconds stated in header and re-submit API call

LIMOSS API Gateway Response Codes 3/3

Code	Response	Response Description	Suggested Action
500	Gateway error (Internal Server Error)	Investigation by LIMOSS SSO Vendor is needed	Raise to LIMOSS Service Desk as Incident
500	Gateway error: multiple MPOs found		Raise to LIMOSS Service Desk as Incident
500	Error retrieving token certificates: Gateway error		Raise to LIMOSS Service Desk as Incident
500	Error retrieving token certificates: OpenID has no public keys		Raise to LIMOSS Service Desk as Incident
500	Error retrieving token certificates: error calling JWKS url		Raise to LIMOSS Service Desk as Incident
500	Error retrieving token certificates: no JWKS in OpenID		Raise to LIMOSS Service Desk as Incident
500	Error retrieving token certificates: error calling OpenID url		Raise to LIMOSS Service Desk as Incident
500	Error validating token: Gateway error		Raise to LIMOSS Service Desk as Incident

Annex B

Glossary

Glossary

LIMOSS SSO – terms and definitions

Term	Definition
Authorised Contact	A trusted person in a client's organisation that is authorised to approve any Service Request for that organisation within the LIMOSS SSO suite of tools.
ACF	Authorisation Code Flow
API	Application Programming Interface
App	Application
CCF	Client Credentials Flow
CH	Change
CR	Change Request
CS	Common Services. This term may be used in legal and other documentation to refer to LIMOSS SSO, LIMOSS SDE and LIMOSS API Gateway
CSV	Comma Separated Values
DAP	Devolved Admin Portal
IE	Internet Explorer
LIMOSS	London Insurance Market Operations & Strategic Sourcing
MPO	Market Participant Organisation
MUA	Master User Agreement
OBO	On-behalf-of
ROPC	Resource Owner Password credentials
SDE	Secure Document Exchange
SSO	Single Sign On
T&C's	Terms and Conditions
URI	Uniform Resource Identifier
URL	Uniform Resource Locator