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".

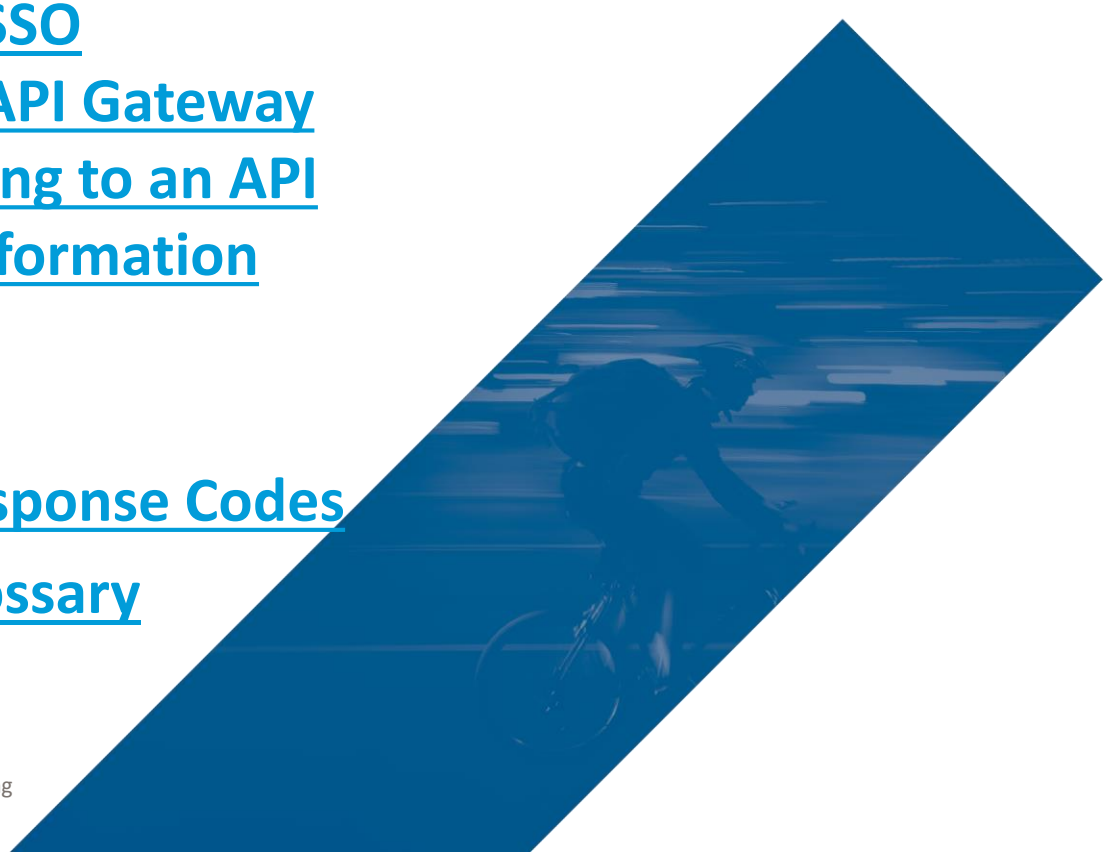
17 May 2021

Agenda

1. LIMOSS
2. LIMOSS SSO
3. LIMOSS API Gateway
4. Subscribing to an API
5. Useful information
6. Support

Annex A: Response Codes

Annex B: Glossary



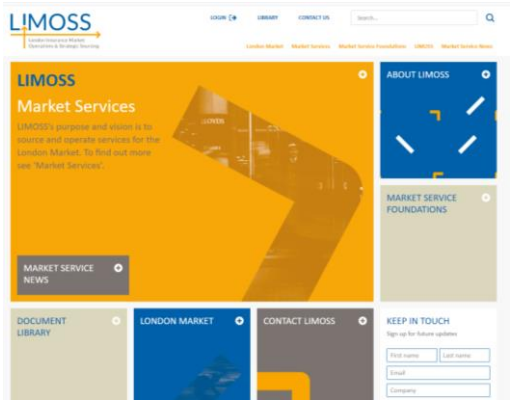
LIMOSS

Introduction to LIMOSS

Mission: Professionally source and operate common market services for the London Market

Good to know

- Not-for-Profit
- Single point of contact for key market services: simplifies integration, provides expert advice and reduces costs
- Owned by Lloyd's, IUA and LMA. Cross-market board including LIIBA representation
- Actively seeks market direction (E.g. market governance forums)



Other LIMOSS Services

- ESP (Electronic Submission Portal)
- SSO (LIMOSS Single Sign On)
- LIMOSS API Gateway
- DDM (Delegated Data Manager)
- MBG (Market Business Glossary)
- SDC (Structured Data Capture)
- ME (Message Exchange)
- Gemini (Expert fees)
- DXC contracts manager for IUA and LMA

Learn more at LIMOSS.London or email servicedesk@limoss.london

LIMOSS SSO Suite of Tools

Easier for

- End users to **access** Market Services
- In-house systems to **integrate** with other LIMOSS/Market solutions
- End users and systems to **securely share** data across the Market

3 Key Components[1]:

LIMOSS Single Sign On (SSO)

Users can access LIMOSS and other Market solutions using the same username and password.[2]

LIMOSS API Gateway

Secure and simple method for integrating market firms' IT systems with LIMOSS and other Market solutions.

LIMOSS Secure Data Exchange (SDE)

Optional easy-to-use tool for securely exchanging data between Market participants. Can be accessed via online interface or via API.

SDE User Video

(https://vimeo.com/302815716)

1 – Commercial Agreements may collectively refer to these components as "Common Services"
2 – LIMOSS SSO does not see or store user passwords

LIMOSS SSO

Introduction

LIMOSS SSO

Introduction to LIMOSS SSO

Simple Authentication Solutions

- Provides authentication for multiple market services – E.g. DDM; SDE; LIMOSS API Gateway
- Allows users to access Lloyd's services with LIMOSS SSO user accounts
- Online registration for organisations and users

Industry Standard Technology

- Built around a managed Azure Active Directory (AAD) tenant, using MS-Azure B2B
- Tenant contains guested-in user accounts registered within organisational entity groups
- Tenant also holds details of published APIs and registered client apps

Designed for use by London Market Organisations

- On-boarding involves KYC and contractual protocols
- Access is free to non-Carrier organisations
- Email servicedesk@LIMOSS.London for full charging details

Works for all Azure Presences

- LIMOSS SSO works for all end users, even if they do not have a managed Azure presence
- A managed Azure presence is recommended for developers and API calling accounts

LIMOSS SSO

Introduction to LIMOSS SSO

"Authorised Contact" Approval Process

- All Service Requests must be approved by an "Authorised Contact" in each organisation.
  - E.g. Approval to add/remove user accounts; Approval to subscribe to an API
- Organisations must have a minimum of 1 Authorised Contact but there is no upper limit
- LIMOSS Recommends having different Authorised Contacts in lower environments

Authentication not Authorisation

- Having a LIMOSS SSO account gets a user account 'into the lobby'. Accounts are unable to access any SSO protected app/API unless the relevant service owner allows it.

LIMOSS SSO (including SDE and the API Gateway) exists in 3 environments:

1. **SANDBOX** – Development environment suitable for building APIs and Apps. This environment is suitable for developers but not for business users or live data
2. **PRE-PROD** – Test environment for integrating APIs and Applications. This environment is suitable for developers but not for business users (except for UAT/MAT) or live data.
3. **PROD** – Live production environment where business users and live APIs/Applications exist. APIs/Apps in development cannot be added to the PROD environment.

- Organisations must be on-boarded in PROD before accessing SANDBOX or PRE-PROD
- Environments are standalone. E.g. An App in SANDBOX cannot call an API in PRE-PROD

LIMOSS API Gateway

Introduction

LIMOSS API Gateway

A brief introduction

- LIMOSS API Gateway is a synchronous, RESTful-based API Gateway
- It allows “Subscribers” in any approved organisation to securely call numerous API Endpoints provided from multiple API “Publishers”.
  - E.g. PPL are an API Publisher; Vendors/Market Firms will act as Subscribers.

- The API Gateway enforces 4 requirements for every API call:
  1. The organisation is known and registered for the API Gateway (using X509 SSL certs)
  2. The user account calling the API is known and authenticated.
     - Depending on how the APIs are published and how the subscribing app is developed, the account can be a service account OR an end user’s account. Whichever model is used, the account must be registered in LIMOSS SSO[1].
  3. The application calling the APIs is registered in LIMOSS SSO
  4. The organisation is authorised to call the specific API

- A successful API call will be passed through to the back-end platform E.g. PPL. The platform will perform additional authorisation checks on the account requesting the information before the API call is returned
- A list of response codes and suggested actions is at Annex A

1 – Alternative STS (Secure Token Service) can be used but this is not recommended

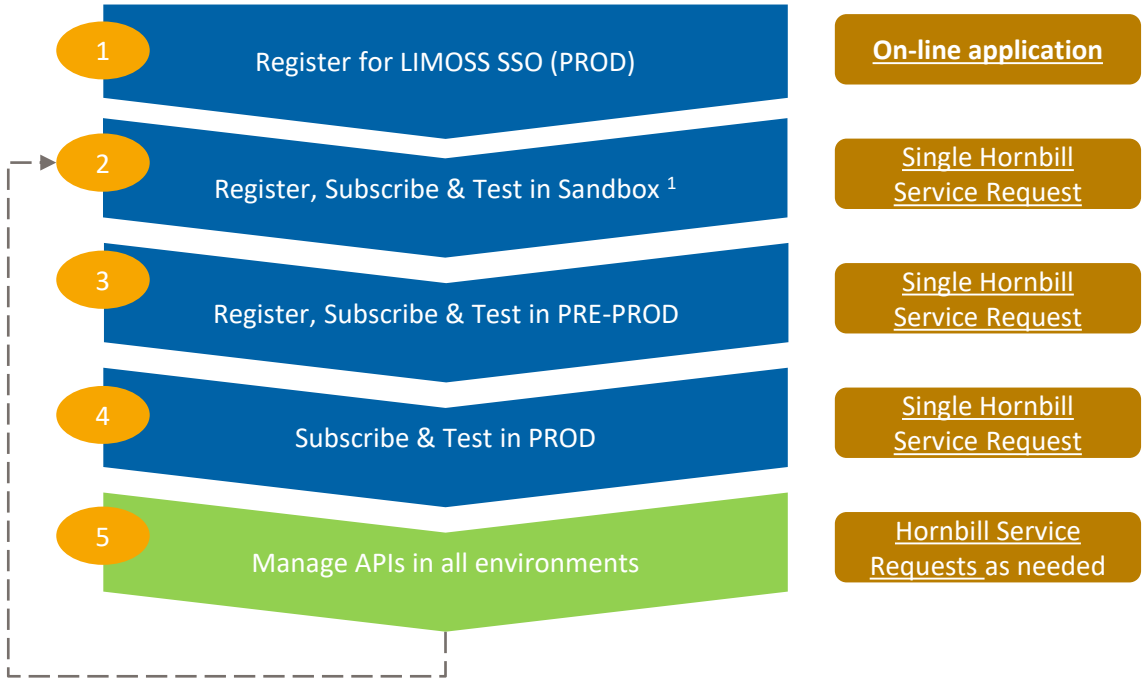
Subscribing to an API

Overview

Subscribing to an API

High level view of Subscribing to an API

- Subscribing to an API via the LIMOSS API Gateway is a 5-step process:
  - First step is to register for SSO in PROD (one-time only requirement)
  - Steps 2-5 can be repeated as often as necessary for multiple different APIs
  - 3-5 working days should be allowed for each Service Request to be fulfilled



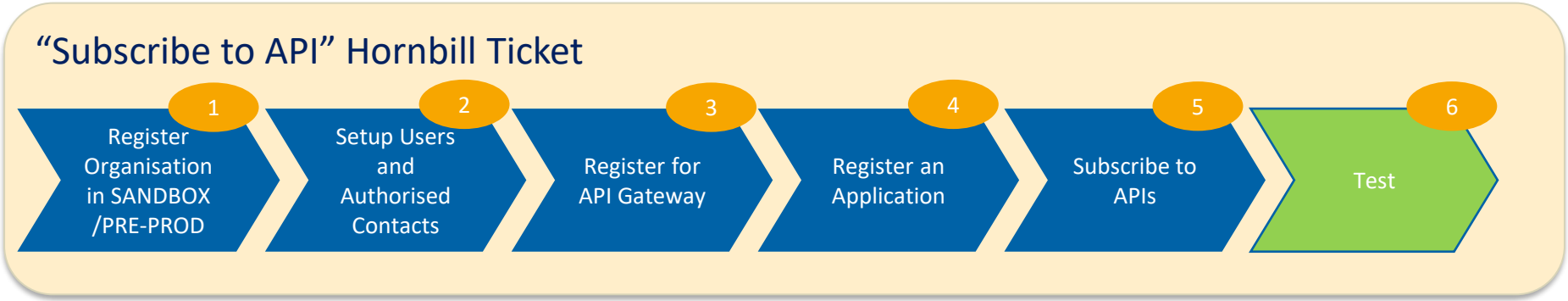
For help with the on-line application or Hornbill contact servicedesk@LIMOSS.London

1- Not all APIs are provided in SANDBOX and PRE-PROD

Subscribe to an API - Breakdown

LIMOSS
London Insurance Market Operations & Strategic Sourcing

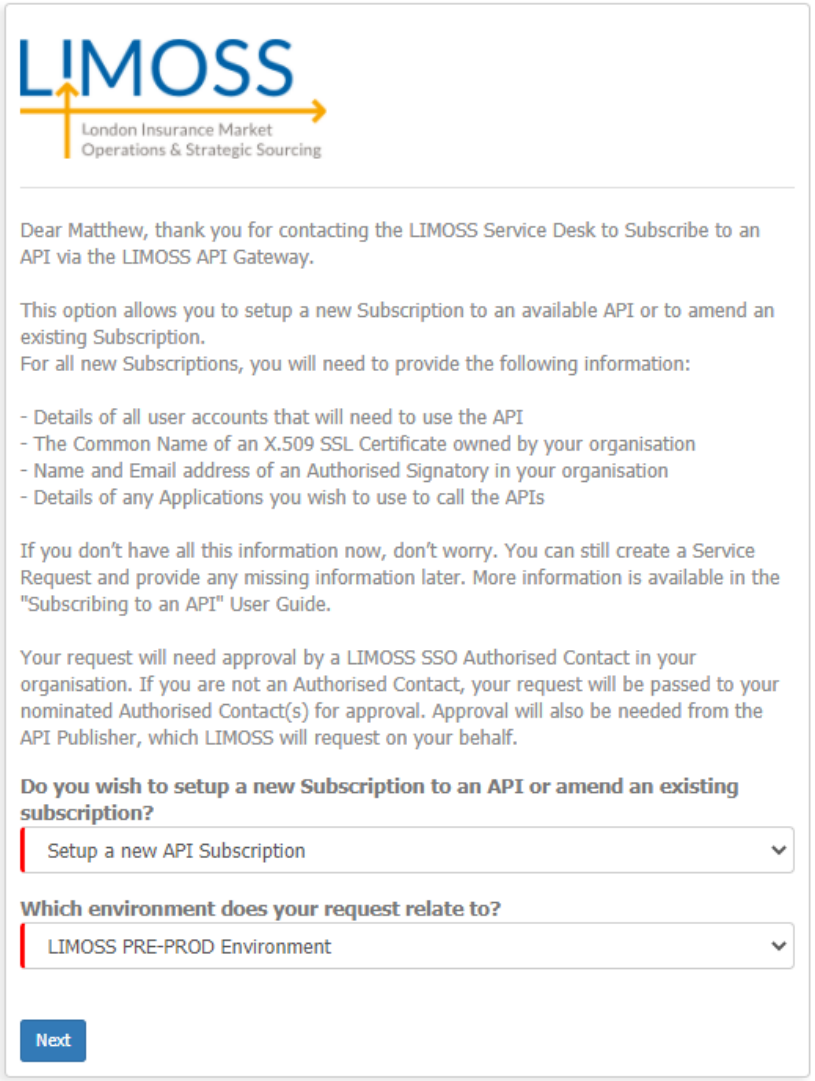
Individual steps involved in Subscribing to an API



Tasks 1-5 are actioned by LIMOSS after a 'Subscribe to API' request is submitted via Hornbill

Notes
1 – Actioned automatically if organisation is not already registered in that environment
2 – Additional user accounts can be added/edited/removed at any time
3 – The subscribing organisation must provide an X.509 SSL Certificate for each environment
4 – At least one web app or native app must be registered. This will generate the App-ID and App-Secret needed when the client app calls an API.
5 – Devs can select from the list of available APIs. Not all APIs are available in both SANDBOX and PRE-PROD environments. Additional legal agreements exist for some APIs.
6 – The API Publisher may require test evidence prior to approving API subscription in a higher environment

Hornbill



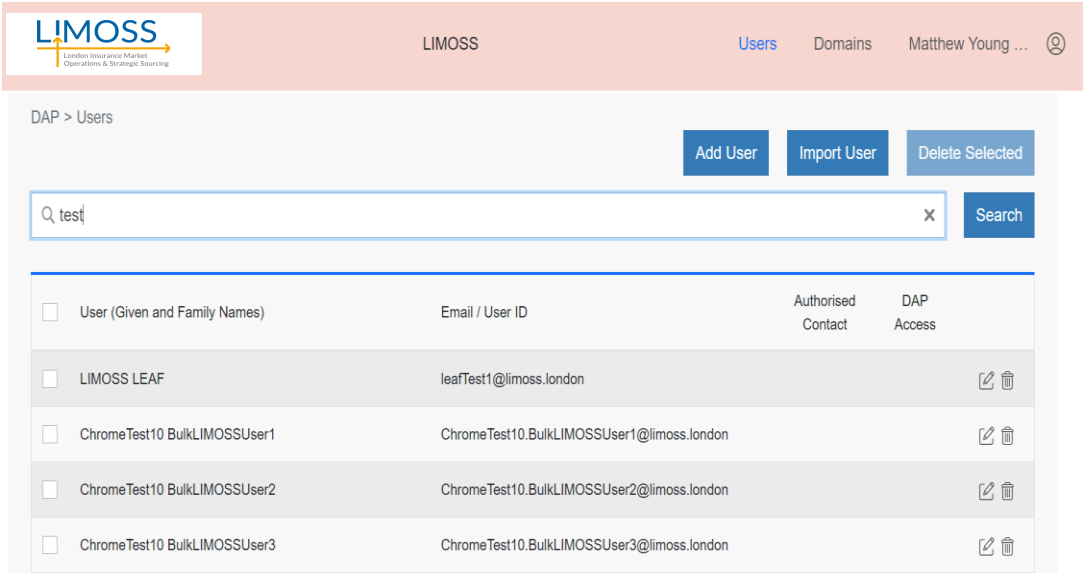
- Online intuitive portal
- Available to users with LIMOSS SSO PROD accounts
- Users can raise Service Requests and Incidents for most LIMOSS Services
- Guides users through relevant questions when subscribing to an API
- Accessible at customer.hornbill.com/limoss and from the LIMOSS SSO Portal

For help with Hornbill contact servicedesk@LIMOSS.London

Devolved Admin Portal (DAP)

DAP is a self-service tool for adding, editing and removing User Accounts in LIMOSS SSO

- Online intuitive portal
- Accessible to Authorised Contacts only
- Real-time management of user accounts and approved domains
- Learn more at DAP User Guide
- Available in SANDBOX, PRE-PROD and PROD environments



For help with Devolved Admin Portal contact servicedesk@LIMOSS.London

LIMOSS API Gateway

Useful Information

Useful Information

Certificates

X509 Certificates

- All organisations using the API Gateway must provide an X509 certificate for each environment
- Both the cert Common Name (CN) and Public Key must be shared with LIMOSS
- Same certificate *may* be used in SANDBOX & 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
- X509 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 price of certificates can vary but free certificates do exist
    - E.g. https://letsencrypt.org
    - LetsEncrypt appears under "Internet Security Research Group (ISRG)" on MS list
- The decision of which CA to use lies with the subscribing organisation.
- LIMOSS does not recommend or endorse any CA

Useful Information

Throttling; Security Model Review; Security Essentials

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

LIMOSS API Security Model Review

- LIMOSS is conducting a market-wide review of the current API Gateway security model
    - E.g. Possible relaxation of need for X509 certificates in lower environments
- Any changes will require full governance approval
- Current design will allow greater flexibility and easier on-boarding for developers but is intended to allow backwards compatibility

Security Essentials

- Organisations must not share the following information with any 3rd parties:
    - App-ID and App-Secret
    - User account passwords
    - X509 Private Key
- Inform the LIMOSS Service Desk immediately if any of these details are compromised

Useful Information

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:
  - In lower environments ONLY: Request user invite link via LIMOSS Service Desk
  - For all environments: 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
- All accounts in LIMOSS SSO should have an SMTP email that matches their User ID

Contact servidesk@LIMOSS.London for further details

LIMOSS Support

Service Desk & Escalation Points

LIMOSS Support

Support and Escalation Points

LIMOSS Service Desk provides support for LIMOSS SSO, LIMOSS SDE and LIMOSS API Gateway

Hornbill Self-Service Portal
(Requires PROD LIMOSS SSO Account)

Online Form

Email
ServiceDesk@LIMOSS.London

Open 8am-6pm (UK) Mon-Fri (excluding Bank Holidays)


LIMOSS
London Insurance Market
Operations & Strategic Sourcing

Annex A

API Gateway Response Codes

LIMOSS API Gateway Response Codes 1/2

Code	Response	Response Description	Suggested Action
200	OK	Standard response for successful requests	No action needed
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
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
500	Gateway 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

LIMOSS API Gateway Response Codes 2/2

Code	Response	Response Description	Suggested Action
400	Error validating token: malformed amr	Error is thrown when the provided token's AMR claim values are incorrect	Raise to LIMOSS Service Desk as Incident
400	Error validating token: malformed appid	Error is thrown when the provided token's AppId claim value is incorrect	Raise to LIMOSS Service Desk as Incident
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
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 X509 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
403	Authorization failed	Error is thrown when the token validation is failed	Raise to LIMOSS Service Desk as Incident
403	Client certificate validation failed: expired certificate	Error is thrown when the provided certificate is expired	Check X509 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 X509 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 X509 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 X509 Certificate is correct, in date and registered with LIMOSS Service Desk Check that correct domain name has been provided in API Call

Annex B

Glossary

CMS Vendor Subscriber

LIMOSS API Gateway Response Codes 2/2

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.
API	Application Programming Interface
App	Application
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
SDE	Secure Document Exchange
SSO	Single Sign On
T&C's	Terms and Conditions
URI	Uniform Resource Identifier
URL	Uniform Resource Locator