PEXA API Activation Manual

The PEXA API Activation manual outlines the PEXA API authentication requirements and set up needed to access the PEXA API test environment.

PEXA API Authentication

PEXA adheres to API best practices to authenticate and authorise access to the PEXA Exchange APIs. To achieve this, PEXA provides the following authentication methods:

- OAuth 2.0
- Mutual TLS

OAuth 2.0 Usage Scenario

- The OAuth 2.0 authentication method is generally used in a business to consumer (B2C) setting. This method allows individual users to access PEXA through an integrated software solution by using their individual PEXA credentials (username, password and Multi Factor Authentication). The OAuth2.0 flow prompts users to log into PEXA with their individual login at the start of every session.
- The authorisation token for the production environment is valid for 12 hours while in the test environment it is valid for 2 hours. The OAuth 2.0 method is best suited to software which has numerous users from different organisations interacting with PEXA under separate subscriber IDs e.g. Practise Management Systems.

Mutual TLS Usage Scenario

- Mutual TLS authentication method is generally used in a business to business (B2B) setting. This method allows an organisation transacting under one PEXA subscriber ID to access PEXA through a single system user. As it is a system user, there is no session expiry. All end users accessing the PEXA integration through Mutual TLS need to be transacting under a single subscriber ID.

PEXA will determine the authentication method best suited to the integrating party.

OAuth 2.0 Overview

OAuth 2.0 is an open-standard authorization protocol that allows authenticated access to resources between unrelated applications, without sharing a single logon credential.

Through the OAuth 2.0 authentication model, PEXA provides an authorisation code grant flow with a 12-hour token expiry in our production environment (and a 2-hour token in our test environment) to enable third-party integrated software to access the PEXA APIs.

OAuth2.0 Test Access Set Up

OAuth2 set up first requires the integrating party to first provide PEXA with a redirect URI and IP address.

Once the redirect URI and IP address has been provided to PEXA, the integrating party will be onboarded to the PEXA Exchange Test Environment.

PEXA will provide the integrating party with test access credentials to enable the integrator to connect to the PEXA APIs using the OAuth2.0 flow, as well as test environment PEXA exchange system users.

For production access, production access credentials will be provided upon the necessary agreement being executed, technical requirements being reviewed by PEXA Security, by the agreed go live date. Prior to the go live date, the integrating party will need to provide PEXA with an additional redirect URI, bring a total of 2 unique URIs - one for test access and the other production access.

Below is a summary of the requirements for the setup of API test access with OAuth2.0:

OAuth 2.0 Integrator Provides	PEXA Provides
Redirect URI	Client ID
IP address	Client Secret
	PEXA Authorisation Server URL
	PEXA Access Token URL
	PEXA API Server URL
	Test environment system users
	Test environment digital signing certificates
	Test environment land title data

Mutual TLS Overview

Mutual TLS (formerly known as Mutual SSL) is an authentication model where two parties authenticate each other's digital certificates to enable trusted access to resources. To achieve this, PEXA adds the digital certificate provided by the integrating partner to its trust store and whitelists the integrating partners IP address.

PEXA also shares the PEXA digital certificate with the integrating partner, which needs to be added to the integrating partners trust store. Once the certificates have been added to the mutual trust stores, the Mutual TLS handshake authentication can take place.

Mutual TLS Test Access Set Up

Mutual TLS set up requires the integrating party to first provide PEXA with a digital certificate and IP address.

Once the digital certificate and IP address has been provided to PEXA, the integrating party will be onboarded to the PEXA Exchange Test Environment.

PEXA will provide the integrating party with test access credentials, the PEXA test environment client-side certificate and the PEXA Test URL, as well as test environment PEXA exchange system users.

For production access, production access credentials will be provided upon the necessary agreement being executed, technical requirements being reviewed by PEXA Security, by the agreed go live date. Prior to the go live date, the integrating party will need to provide PEXA with an additional digital certificate, a total of two certificates - one for test access and the other for production access.

The test certificate can be a self-signed certificate. The production certificate needs to be from a third-party issuing Certificate Authority.

For test and production, PEXA requires the complete certificate chain (including root and immediate).

Below is a summary of the requirements for the setup of API test access with Mutual TLS:

Mutual TLS Integrator Provides	PEXA Provides
Digital Certificate (complete certificate chain including root and immediate)	PEXA Digital Certificate
IP address	PEXA API Server URL
	PEXA Access Token URL
	PEXA API Server URL
	Test environment system users
	Test environment digital signing certificates
	Test environment land title data