Pelican Network
Single Sign-On (SSO) & OpenID Connect Integration Guide

Phase 1: Overview

This document provides technical specifications and implementation guidelines for integrating Single Sign-On (SSO) with the Pelican Copy Trading platform. By federating your identity layer with Pelican using OpenID Connect (OIDC) built on OAuth 2.0, broker clients authenticate using their existing credentials on your platform. Pelican provisions user profiles and handles session verification automatically without prompting users to register or log in twice.

Phase 2: Core Protocol & Security Requirements

Protocol Flow:	Authorization Code Flow + PKCE	Proof Key for Code Exchange using the S256 code challenge method is mandatory. For an architectural walkthrough of standard OIDC authentication, refer to the OpenID Foundation guide
Discovery Document:	OpenID Provider Discovery (/.well-known/openid-configuration)	Your STS must expose a discovery endpoint allowing Pelican to resolve endpoints and keys (JWKS) dynamically.
Token Authentication:	client_secret_post	Supported token endpoint client authentication method.
Required Scopes:	openid email profile address	Mandatory scopes for identity assertion, account creation, and user metadata mapping.

Note: The address claim is required to supply the user's country code, which is used to enforce regional regulatory compliance.

Phase 3: Configuration & Parameter Exchange

3.1 Provided by the Broker to Pelican

Prior to initiating sandbox integration testing, the broker must supply the following parameters:

Authority URL (iss): The base URL of your Identity Provider / STS (e.g., https://sso.broker-domain.com).

Client ID (client_id): The unique client identifier provisioned for Pelican inside your STS (e.g., pelican_copytrade_broker).

Client Secret: The confidential client secret configured for Pelican's client ID (if required by your STS setup).

3.2 Provided by Pelican to the Broker

Whitelist the following redirect and callback endpoints within your Identity Provider:

Post-Login Redirect URI:
https://identity.copy-trade.io/signin-oidc-{brokercode}

Post-Logout Redirect URI 1:
https://identity.copy-trade.io/signout-callback-{brokercode}

Post-Logout Redirect URI 2:
https://identity.copy-trade.io/signout-{brokercode}

Note: Replace {brokercode} with the unique broker identifier assigned by Pelican. These callback URIs remain inactive until Pelican configures your Authority URL and Client ID on the platform.

Phase 4: Required OIDC Identity Claims

Pelican relies on claims embedded within the signed ID Token (or returned by the /userinfo endpoint) to complete Just-In-Time (JIT) account provisioning and regional suitability compliance.

4.1 Claim Specifications

Claim Key	Type	Description
iss	**String URL**	**Issuer identifier representing your STS/IdP authority.**
aud	**Array / String**	**Target audience; must match the assigned Pelican client_id.**
sub	**String**	**Unique, immutable user identifier in your broker database.**
email	**String**	**User's verified email address.**
name	**String**	**Full display name.**
given_name	**String**	**User's first name.**
family_name	**String**	**User's last name / surname.**
profile	**String**	**User profile or account reference string.**
address	**Object**	**Nested structure containing user geographic metadata.**
country code	**String**	**Standard ISO 3166-1 alpha-2 uppercase country code (e.g., 'BR', 'GB').**
country	**String**	**Full country name (e.g., 'Brazil', 'United Kingdom').**
iat	**Integer**	**Epoch timestamp when the token was issued.**
exp	**Integer**	**Epoch timestamp when the token expires.**

4.2 Standard Payload Example (Decoded ID Token JSON)

```
{
  "iss": "https://sso.broker-oidc.com",
  "aud": [
    "pelican_copytrade_broker"
  ],
  "sub": "71185",
  "email": "test-oc48@brokercode.com",
  "name": "Elsa Grimes",
  "given_name": "Elsa",
  "family_name": "Grimes",
  "profile": "Elsa Grimes",
  "address": {
    "country_code": "BR",
    "country": "Brazil"
  },
  "iat": 1768516943,
  "exp": 1768520543
}
```

Phase 5: Architecture & Implementation Steps

```
[Trader / Client]
    1. Clicks Copy Trading on Broker Portal
        ▼
[Pelican Platform / Identity Server]
    2. Redirects to Broker STS Authorization URL (/authorize)
        ▼
[Broker Identity Provider (STS / IdP)]
    3. Validates active session / authenticates user
    4. Issues Auth Code & redirects to Pelican Callback URI
        ▼
[Pelican Identity Server]
    5. Exchanges Auth Code for ID Token via client_secret_post
    6. Validates signature via Broker's JWKS and extracts claims
        ▼
[User Authenticated & Profile Provisioned]
```

Step 1: Configure Pelican as a Client in Your STS

Register a client for Pelican inside your Secure Token Service (e.g., Duende IdentityServer, Auth0, Keycloak, or Okta). Enable the Authorization Code Flow with PKCE (S256), whitelist Pelican's redirect URIs, and ensure that identity claims (sub, email, name, address.country_code) are mapped to the issued ID token.

Step 2: Share Authority Details with Pelican

Provide your Authority URL, Client ID, Client Secret (if applicable), and confirm that your OIDC discovery endpoint (/.well-known/openid-configuration) is publicly accessible.

Step 3: End-to-End Sandbox Validation

Execute login and session termination test flows in the UAT environment. Confirm that user accounts are automatically provisioned with their correct country code and profile details, and verify that post-logout callbacks cleanly clear sessions.

Phase 6: Additional Considerations

Password & Credential Management:

Credential management, MFA, password resets, and account lockout procedures remain 100% under your control. Pelican never receives or stores raw trader passwords.

Country Code Compliance:

The address.country_code claim is mandatory for regional regulatory compliance and filtering strategy discovery based on client residency.

Mobile Client Storage:

For native apps, store tokens using Keychain Services (iOS) or Android Jetpack Security EncryptedSharedPreferences (Android).

Contact

+44(0)203 475 4516

www.pelicannetwork.io

support@pelicantrading.io