Enabling global identity
Protecting digital trust

KERIA Server

GLEIF Testnet Documentation

Public
Version 1.0
2025-07-11

Table of Contents

Version	1.0
Date of version	2025-07-11
Created by	Kent Bull
Approved by	Ivan Mortimer-Schutts
Confidentiality level	Public

About this Document

This document describes the usage of the GLEIF Testnet KERIA serverfor technical users and is aimed at software developers and architects using the vLEI technologies to build line of business applications.

Change History

Date	Version	Description of Change	Author
2025-07-11	1.0	Final Version	Kent Bull

1 KERIA Server Overview

1.1 Getting Started

Using a KERIA server implies usage of a Signify edge wallet, meaning usage of either the SignifyTS (Typescript) or SignifyPy (Python) edge wallet library. Both the training and end-to-end referenced examples below illustrate usage of KERIA and may be used as a getting started guide. Start with the Training example and progress onto the end to end workflow if additional context is needed.

1.1.1 Training Example

The vLEI Trainings repository has a KERIA and Signify training (Github GLEIF-IT/vlei-trainings/jupyter/notebooks/102_05_KERIA_Signify.ipynb) showing the basics with getting up and running for the KERIA agent and corresponding Signify edge wallet (edge controller).

1.1.2 End to End Workflow Example

An advanced setup may be found in the end-to-end testing qvi-software repository in the keria_docker folder (Github GLEIF-IT/qvi-software/qvi-workflow/keria_docker) illustrating how a KERIA server may be set up for production usage. A barebones, headless, task based Signify wallet implementation using KERIA may be found in the qvi-software/qvi-workflow/sig_ts_wallets subdirectory showing the Typescript code for building the various parts an end-to-end issuance, credential holding, and credential presentation workflow.

1.2 Functional Purpose

A KERIA (KERI Agent) server is a necessary component when building wallet or other signing or credential infrastructure on top of the Signify architecture. See the 102_05_KERIA_Signify.ipynb vLEI training for a description of the Signify architecture. Much of the vLEI ecosystem relies on the Signify architecture and thus on KERIA, SignifyTS, and SignifyPy. Thus the GLEIF Testnet provides a KERIA server as testing infrastructure for building proof of concept solutions. The KERIA server URL is noted below.

1.3 KERIA Server URL List

KERIA Server	https://keria.testnet.gleif.org:5641

1.4 Who Runs This

Generally speaking each team or business should eventually run their own KERIA Server infrastructure, or work with an infrastructure to provide a KERIA Server along with witnesses. For the duration of the hackathon GLEIF will provide a testnet with infrastructure on the “testnet.gleif.org” domain as shown below including a KERIA server and five witnesses, among other components.

Component	URL and Port
Witness 1 - wit1	https://wit1.testnet.gleif.org:5641
Witness 2 - wit2	https://wit2.testnet.gleif.org:5642
Witness 3 - wit3	https://wit3.testnet.gleif.org:5643

Component	URL and Port
Witness 4 - wit4	https://wit4.testnet.gleif.org:5644
Witness 5 - wit5	https://wit5.testnet.gleif.org:5645
KERIA Server	https://keria.testnet.gleif.org Ports 3901, 3902, and 3903 are open
vLEI Server	https://schema.testnet.gleif.org:7723
vLEI Reporting API	https://presentation-handler.testnet.gleif.org:9723
Webhook Call Handler	https://hook.testnet.gleif.org:9923

2 OpenAPI Documentation

The OpenAPI 3.0 documentation for the KERIA server may be retrieved from the **/spec.yaml** endpoint. A full URL to the OpenAPI 3.0 documentation looks like the following: https://keria.testnet.gleif.org:3902/spec.yaml

3 Authentication to the KERIA Server

Accessing a KERIA server may only be done using keypairs created at the edge using a Signify client library such as SignifyTS or SignifyPy and then by sending signed requests.

The following three HTTP headers are used automatically by client libraries for authentication to an agent running on a KERIA server. All headers must be

- "**Signify-Resource**": set to the Signify Controller AID prefix.
- "**Signature-Input**": set to the signature of the full HTTP request URL including all request parameters.
- "**Signify-Timestamp**": set to the timestamp the request was made.

The "Signify-Resource" header indicates who is making the request and serves as the primary authentication mechanism upon being cryptographically verified by the KERIA agent for each request.