Aridhia Informatics – DARE UK TREvolution Final Report

Author: Ross Stiven **Date:** 24/03/2026 **Version:** 1.0

Summary:

This final report details initial work carried out by Aridhia under the DARE UK TREvolution project, specifically a proof of concept (PoC) integration of a secure TRE workspace with a federation component based on the GA4GH Task Execution Service. It builds on the work detailed in our interim report published in November 2025 and provides:

- Overview of PoC Components
- Summary of interim report
- Completed Work
- Future Improvements

Overview of components:

The components of the federation PoC are an Aridhia DRE workspace and the Federated Node, an open source software component for data federation.

Aridhia Workspaces:

The Aridhia DRE is a Trusted Research Environment (TRE). It is certified under ISO27001/27701 and HITRUST, and is also compliant with the DARE UK SATRE specification for TREs.

The DRE has two primary components FAIR Data Services, a metadata catalogue, and Workspaces a secure platform for collaborative data analysis. FAIR was not used to implement the PoC.

Each DRE workspace provides users with a number of tools for collaborative research, but only two of its features were required for the PoC:

- A workspace database for hosting data
- A workspace container registry for publishing containerised code.

The Federated Node:

The Federated Node (FN) is an open source software component for federated analysis, derived from the GA4GH TES.

The FN is based on the Common API. The Common API was developed by the International Covid Data Alliance, and is an open standard for a federated data

sharing API which includes the TES endpoints. The FN takes this standard and develops it into a deployable software component for executing federated tasks.

A deployed FN must be associated with:

- one or more databases which hold the federated data,
- a container registry from which it retrieves the analytical code.

In the PoC these resources are provided by the DRE workspace.

Summary of interim report

The interim report detailed how these components could be manually configured to allow federated analysis of data held in the database of a secure workspace. Figure one below shows this at a high level:

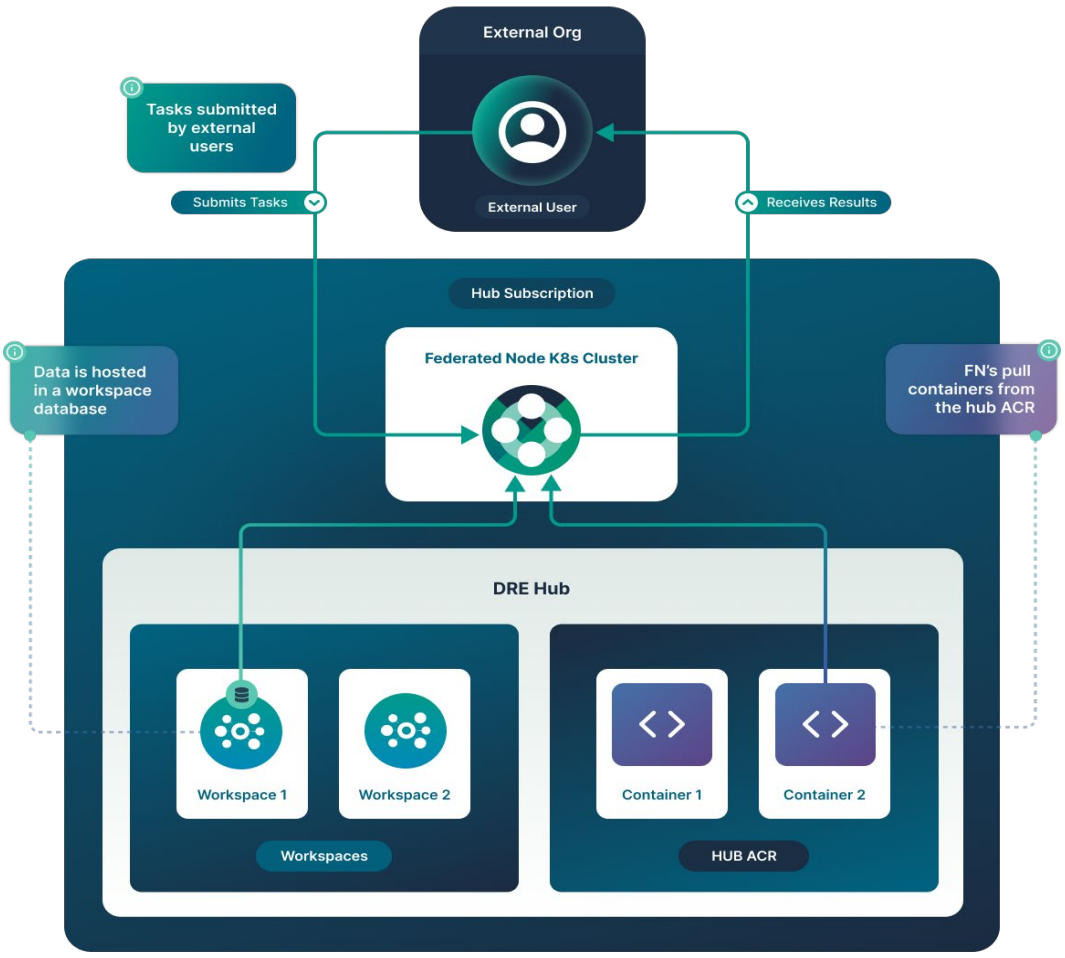

Figure 1 - high level overview of Federation PoC

The interim report identified security and a clear separation of concerns as the strengths of this approach, and identified the heavily manual set up process as its biggest weaknesses.

Given these conclusions we decided to prioritise automating the set up process as far as possible for the remainder of the project.

Three possible areas were identified for improvement:

Automating the Issue of FN auth tokens:

Users require a valid authentication token to interact with a Federated Node, for the PoC this had to be manually delivered to the workspace by a member of Aridhia staff, reducing the number of manual steps in this process is a key consideration for scalability. A PoC version of this was completed during the project, see completed work below.

Allow workspace users to self-serve connections between workspace database and FN:

A related issue to the above, making it possible for users in a workspace to map their data to an external FN. A helper app was created and released on our open source GitHub project, see completed work below.

Introduction of a workspace federation condition:

Our working assumption is that where a workspace is federated researchers will not want to use it for other purposes, introducing a federation condition which limits access to the workspace and blocks data ingress would prevent this. This work was not completed during the DARE UK project, see future improvements below.

Figure 2 below shows how these fit in the workflow for connecting a Workspace to a FN.

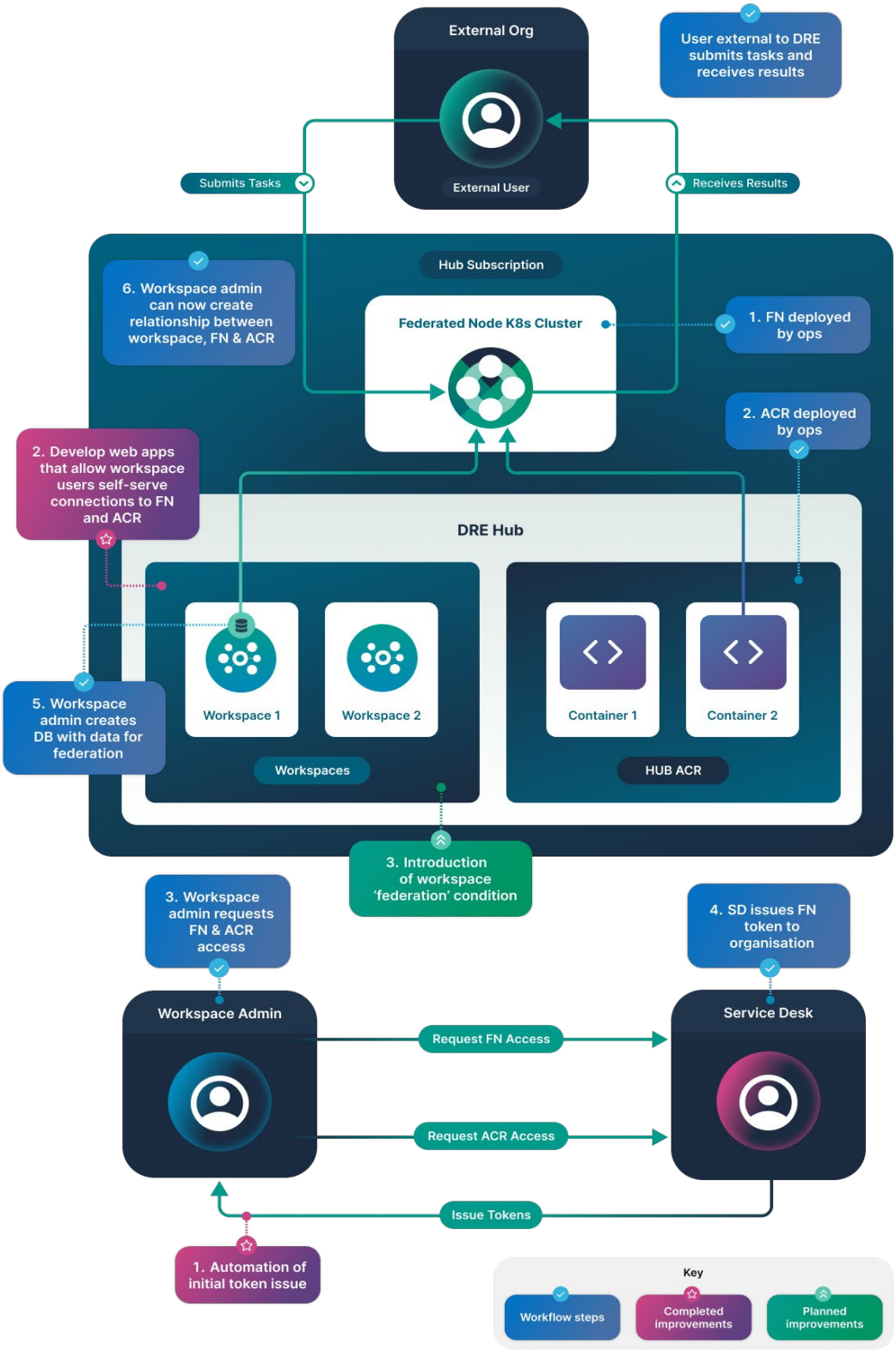

Figure 2 - configuration workflow

Completed Work

Automating the Issue of FN auth tokens:

This was achieved by building on two existing features of Aridhia Workspaces:

- Organisations
- Workspace secrets

The Organisations feature allows a Workspace hub to be segmented into distinct organisations with their own members, workspaces and resources.

The Workspace Secrets feature allows the administrator of an individual workspace to securely store auth tokens and connection details for external services that all users of that workspace can then interact with.

In our previous manual workflow the Aridhia service desk would have had to issue a token separately for every workspace that wished to interact with a FN. To assist in the automation of FN auth tokens we have:

1. Extended the workspace organisation feature to include organisation level secrets
2. Enabled organisation administrators to apply these secrets to individual workspaces within their organisation
3. Made these secrets available to users of the workspaces where they have been applied.
4. Allowing the workspace administrator to connect their workspace to their organisation's Federated Node.

This means that the service desk only has to issue one authorisation token per organisation, and organisation level administrators can apply these to workspaces within their org as required.

Allow workspace users to self-serve connections between workspace database and FN:

Once a workspace has been connected to a FN, the workspace administrator needs to be able to map their data to the FN. To make this process more user-friendly we have created an open source helper app for the Federated Node which allows users to easily map their database to a deployed FN. This is available from the Aridhia Open Source GitHub project:

https://github.com/Aridhia-Open-Source/Federated-Node-Example-App/blob/main/miniapps/mapping-fn/app.R

Confidential ● Copyright © Aridhia Informatics Ltd. ● www.aridhia.com ● info@aridhia.com

Protective Marking: Internal

Future Work

We were unable to complete the following work during the project, but we believe it should be considered in future priority discussions:

Introduction of a workspace federation condition:

As detailed above, we considered extending the Aridhia DRE conditions framework to include a specific federation condition. This would allow workspace administrators to automatically apply a restricted configuration to workspaces connected to a FN, limiting user access and restricting data ingress and egress. We considered this a lower priority than improving and automating the set up process, and therefore did not have time to carry out this work during the project. However, we still believe this would be a useful feature for any TRE that offers a data federation capability.

Integrating the FN with the 5 Safes TES Submission Layer:

5 Safes TES was developed by DARE UK, and its submission layer allows researchers to initiate federated data analysis tasks in multiple connected nodes simultaneously. Integrating the FN with the submission layer would allow it to act as a node of the network, receiving tasks and returning results.

We did explore the possibility of integrating the FN with the 5 Safes TES submission layer during the project, and believe we understand the small number of changes that would be required to make it possible. We were unable to complete this work during the project, but plan to revisit it later in 2026.