National Federated Compute Services NetworkPlus

Spring Conference
26-27 February 2026

Evaluation of Secure Federated Kubernetes Storage for Trusted Research Environments

Wojciech Turek - University of Cambridge

UNIVERSITY OF CAMBRIDGE

BriCS Bristol Centre for Supercomputing

UCL

KING'S College LONDON

UKRI

This project will explore and evaluate a federated, secure storage solution, enabling researchers to make use of national research infrastructure without losing control of their own security boundaries.

Key Objectives

- Exploration and Evaluation of automated encryption solutions for Kubernetes block storage in TREs, utilising technologies such as Linux Unified Key Setup (LUKS), HashiCorp Vault.

- Evaluate federated key ownership solutions, ensuring each institution maintains exclusive control over its encryption keys

- Evaluate compliance, auditability, and operational security frameworks for encrypted storage, aligning with data security standards such as ISO27001, CAF, SATRE

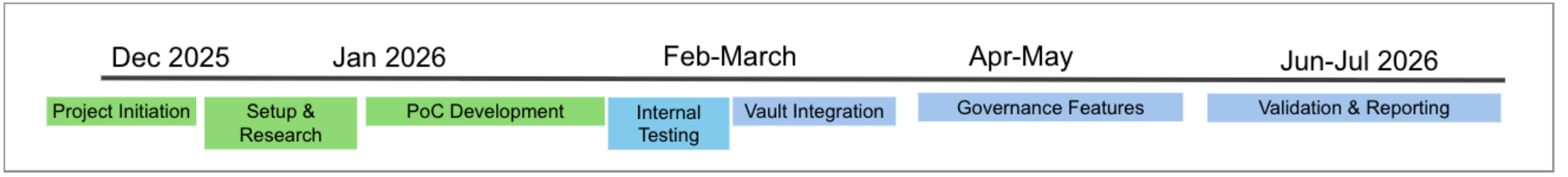
- Drive adoption and knowledge transfer through open-source deliverables with the wider TRE community.

Technical Evaluation and Implementation

- Technologies: Python (Kopf), LUKS/dm-crypt, Kubernetes, CSI, HashiCorp Vault, OpenBao, OpenStack Cinder
- CRD & Operator: Custom Resource triggers orchestration of volume encryption
- Vault Integration: Keys securely generated, stored and retrieved per-volume.

Status and road map

- Prototype Operator developed using the Kopf farmwork to automate block cinder storage.
- Successfully integrated with OpenStack Cinder CSI for dynamic encryption of volumes.
- Custom Resource Definitions (CRDs) designed to declaratively trigger encrypted volume creation via kubectl workflows.
- Operator orchestrates LUKS encryption on the worker nodes ensuring volumes are securely mapped and formatted before use.
- Initial tests confirm encrypted volumes are mounted and usable by pods with no input from users.
- Vault integration with key management is planned for next phase.



Key Benefits and Impact

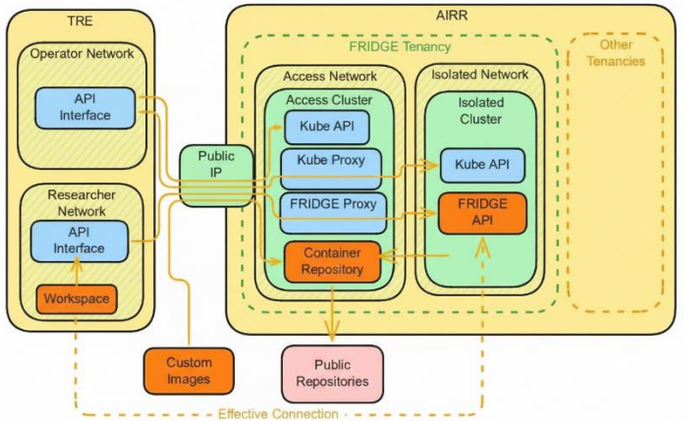
- Transparent and seamless for users and researchers
- Aligned with ISO27001, CAF and SATRE guidance and standards
- Policy enforcement and encrypt volume by default
- TRE operators manage encryption keys
- Suitable for national TRE federation

Use cases

- Federated Research Infrastructure by Data Governance Extension (FRIDGE)
- Pharos AI project – accelerate AI powered cancer care

PharosAI

FRIDGE
A DARE UK PROJECT



UK TRE

Project team

Project Leads

Wojciech Turek (Cambridge)

Co-leads

Sylvie Da Graca Ramos (UCL)

Thomas Green (BriCS)

Matt Penn (KCL)

Project Team Members

Tunde Oyewo (Cambridge)

Paul Browne (Cambridge)

Glyn Chudleigh (KCL)

Jake Watson (BriCS)

UNIVERSITY OF CAMBRIDGE

KING'S College LONDON

BriCS
Bristol Centre for Supercomputing

UCL