Contribution ID: **137** Type: **Oral Presentation**

Confidential Computing for Sensitive Data Analysis: The EOSC-SIESTA Approach

Thursday, 19 March 2026 12:06 (22 minutes)

The FAIR principles provide a foundational framework for ensuring that scientific data is accessible and reusable, and their implementation is a central objective of the European Open Science Cloud (EOSC). However, enabling access to sensitive or confidential data while simultaneously preserving privacy, confidentiality, and usability for researchers remains an open challenge. Existing approaches—such as safe rooms, safe pods, and data safe havens—often hinder the development of reproducible research and can appear counter-intuitive in the context of open science and FAIR-compliant data practices.

The SIESTA project addresses this challenge by developing trusted, cloud-based environments designed for the secure management and sharing of sensitive data. These environments are created using reproducible methodologies and are complemented by a suite of services and tools that simplify the secure exchange of sensitive data within the EOSC, leveraging state-of-the-art anonymization techniques. The overarching goal is to enhance the EOSC Exchange services by delivering cloud-based trusted environments capable of supporting the analysis of sensitive data while demonstrating that the FAIR principles can be effectively upheld in such contexts.

At the core of EOSC-SIESTA lies a distributed, cloud-based computing platform built on Trusted Execution Environments (TEEs)—hardware-backed secure enclaves that isolate sensitive code and data from the surrounding operating environment (e.g., AMD SEV-SNP, Intel TDX, ARM TrustZone). The platform supports both Confidential Computing, where entire virtual machines operate as secure enclaves, and Confidential Containers, a Kubernetes-based secure computing solution in which containers serve as enclaves through technologies such as Kata Containers.

In addition, the DevSecOps toolchain will include a comprehensive set of security capabilities, including continuous vulnerability scanning and tracking to identify and monitor risks throughout the software lifecycle; automated misconfiguration detection and prevention to ensure infrastructure and application settings adhere to security best practices; cryptographic verification and signing of build artifacts to guarantee their integrity and authenticity; and robust access and secret management solutions to securely handle credentials, tokens, and other sensitive information across development, deployment, and operational environments.

Primary author: TRAN, Viet (Institute of Informatics, Slovak Academy of Sciences)

Presenter: TRAN, Viet (Institute of Informatics, Slovak Academy of Sciences)

Session Classification: Infrastructure Clouds and Visualisations - I (11:00 - 12:40)

Track Classification: Track 8: Infrastructure Clouds and Virtualizations