EOSC-TITAN and Supporting Secure Processing Environments for Secondary Use of Health Data under the EHDS

Natalia Borgoñós García (University of Murcia)

IBERGRID 2026

28/10/2026

Funded by the European Union

Funded by the European Union under the GA No 101129822. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Executive Agency (REA). Neither the European Union nor the granting authority can be held responsible for them.

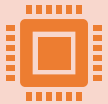
Introduction



European Health Data Space (EHDS) → Is an major policy initiative of the European Commission to improve access to **healthcare data** by making it accessible to citizens, researchers and policymakers across the EU. Data will only be accessed and processed by authorised users for specific and approved purposes.



Secure Processing Environments (SPEs) → Controlled and isolated environment designed to protect sensitive data against unauthorized access.



EOSC-TITAN project → Addresses technical challenges for the deployment of trustworthy and interoperable infrastructures for health-data processing by enriching the **European Open Science Cloud (EOSC)** with a software platform for **Confidential Data collaboration and Secure Data Processing**.

Funded by the European Union

EOSC-TITAN General Overview

- **EOSC-TITAN** will focus on developing an **end-to-end secure data sharing and collaboration platform** that will bring advancements in **distributed access control**, security domain segmentation, application of state-of-the-art **protection for data in use**, as well as **usable and scalable data anonymisation.**
- **The project works on three main areas.**
  - **Domain 1: Confidential data processing enabling confidential collaborative data processing**: memory encryption, confidential computing, remote attestation, confidential GPUs, confidential ML.
  - **Domain 2: Scalable data anonymisation for wide data access:** Differential Privacy, k-anonymity, Secure Multiparty Computation (SMC), Multi-Party Computations (MPC), Zero-Knowledge Proof (ZK-SNARKs), and Homomorphic Secret Sharing (HSS).
  - **Domain 3: Distributed access control and transaction logging using decentralised solutions:** blockchain technologies, network security domains, cloud security zones, access control and management.

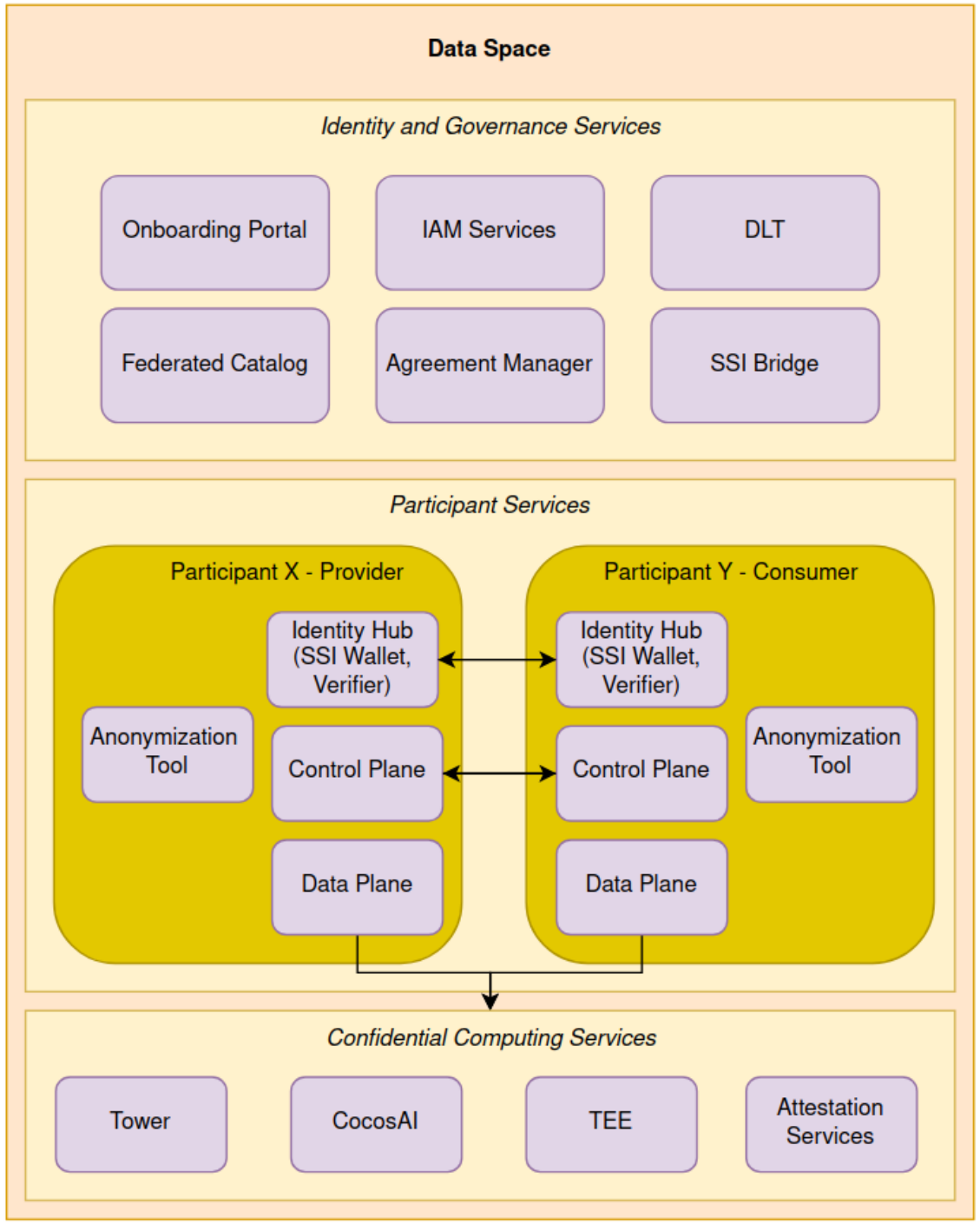
Funded by the European Union

EOSC-TITAN Objectives

Enriching the EOSC with a **software platform solution for confidential data collaboration and secure and privacy-preserving data processing.**

- Objective 1: Collect legal, technical, and architectural requirements and define a **platform architecture for secure sharing of sensitive data** and publishing anonymised data sets in the **EOSC Interoperability Framework IF**.
- Objective 2: **Develop secure data sharing and auditing mechanisms for sensitive data**, including secure data zones, data **access control, and end-to-end data protection** (storage - transfer - processing).
- Objective 3: Develop an end-to-end secure data processing framework for **collaborative and privacy-preserving Machine Learning (ML) using Trusted Execution Environments**.
- Objective 4: **Implement confidential mechanisms, algorithms, and tools** with cloud infrastructure platforms and the EOSC IF, and validate solutions in sensitive data-driven **use cases (government and healthcare)**
- Objective 5: **Disseminate and promote the solutions for data governance** and stewardship through collaboration with EOSC Partnership initiatives, standardisation, and integrating with the EOSC infrastructure

Funded by the European Union



EOSC-TITAN Architecture

- **Identity and Governance Services.** This layer contains the shared services that bootstrap trust in the ecosystem and is based on **Self-Sovereign Identity (SSI)** solutions,
to give participants complete ownership and control over their personal data without relying on central authorities.

- **Participant Services.** A participant is provided with an implementation of an **EDC-based Connector** when accepted and has an assigned identity within the ecosystem.

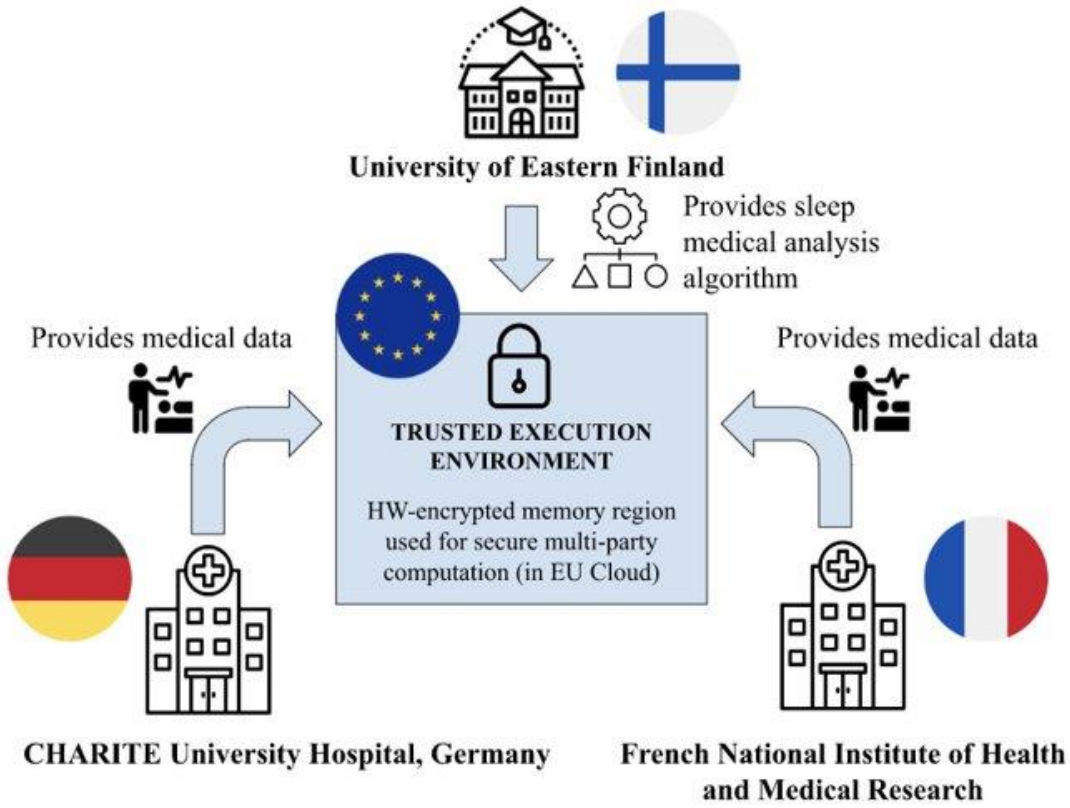
- **Confidential Computing Services** of EOSC-TITAN Architecture, the remote attestation mechanisms they rely on, and one of the processing modes offered to researchers: **Confidential Compute-to-Data Execution.**

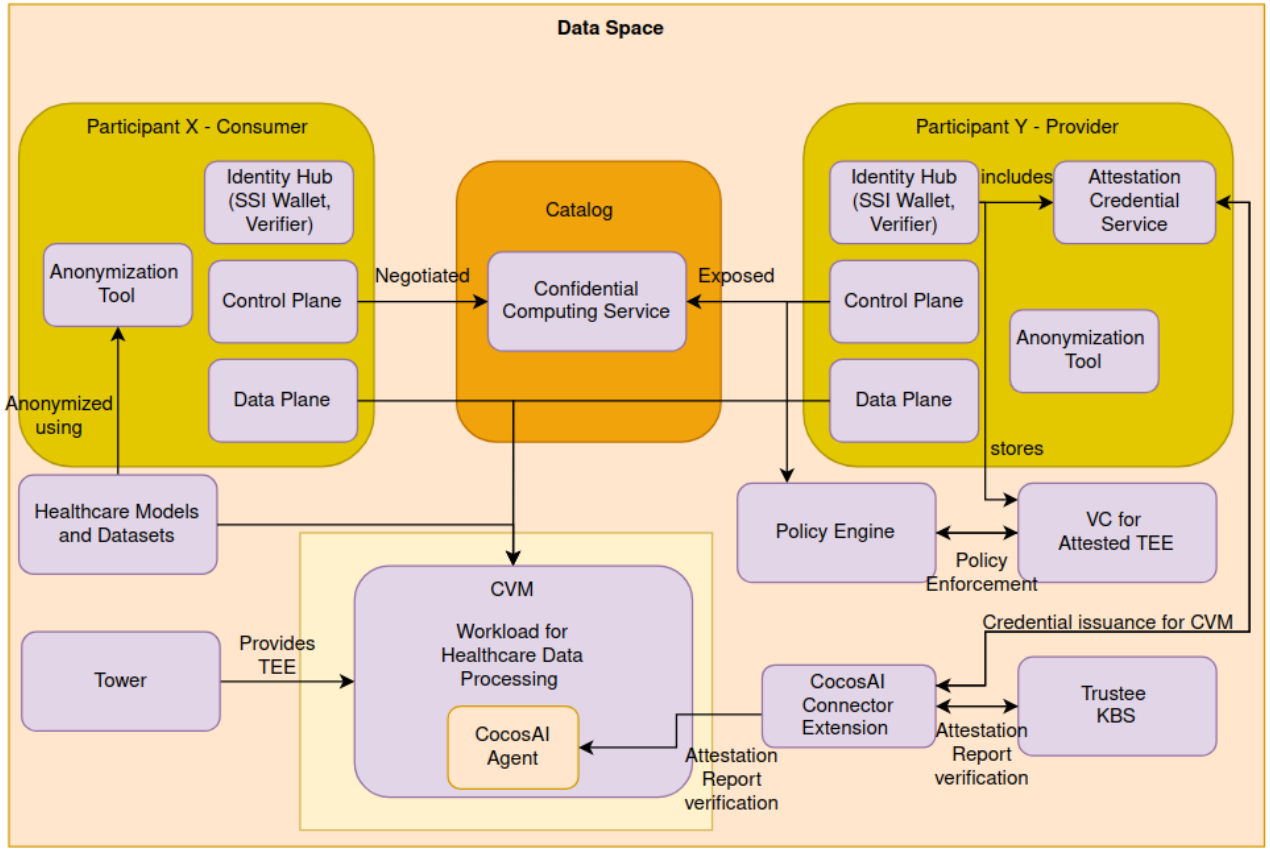
How EOSC-TITAN can provide solutions to SPE

- **EOSC-TITAN** looks for mechanisms to allow **Consumer** and **Provider** (data, processing, confidential processing, AI/ML algorithm service) describe their properties and capabilities using a **FAIR** approach in a **Federated Catalog**, offered in a **Data Space** governance architecture with the corresponding protocols implemented.
- Support deployable and configurable **Connectors** (following **Eclipse Dataspace Components** specifications) with privacy-preserving tools to support and secure the communication between Consumers and Providers.
- Manage identity with **SSI**, applying **privacy-preserving mechanisms**, including a **DLT** and an **SSI-Bridge**, AAI based solution interoperable with EOSC.
- Provide **Confidential Computing** capabilities on demand to support data treatment based on **Trusted Execution Environments**, secure enclave and **Federated Learning** functions, including privacy preserving and anonymization.
- Attest TEEs using **Remote Attestation** mechanisms and integrating them in the data space workflow.

Funded by the European Union

Healthcare Use Case developed in EOSC-TITAN





Funded by the European Union

How EOSC-TITAN covers EHDS requirements?

EHDS Requirements for SPEs	EOSC-TITAN Mechanisms
Restricted access to persons authorised in the data permit	**Distributed access control**, identity and authorisation management
Use only for the **approved purpose**	**Controlled data-sharing policies**: what data, with whom, under which processing conditions
Access only to **data covered by the permit**, with unique individual user identities	**Fine-grained authorisation** bound to individual identities and specific processing tasks
Prevent **unauthorised operations** while processing	**Confidential Computing and TEEs**: data processed encrypted in memory, isolated from host and operator
Verifiable security of the environment	**Remote Attestation**: cryptographic verification of code and environment before data or keys are released
Protection across the data lifecycle	**End-to-end data protection** in storage, transfer and processing
Auditable access and activity logs	Transaction **logging**
Only **aggregated or anonymised results** can be extracted	**Federated ML** and PETs: models or aggregates leave, never raw data
Data **minimisation**	**Federated Learning:** data are not centralised and remain with the provider
Interoperability	**Integration** with EOSC and European data-space architectures

Funded by the European Union

Conclusions

- **EOSC-TITAN** builds on the vision of combining a thorough **understanding of legal and technical aspects** to build solutions for a new paradigm of secure access to sensitive public data and applications and support data-driven science.
- **EOSC-TITAN** translates the **EHDS** requirements for **Secure Processing Environments** into **concrete technical safeguards**. Confidential computing, Remote Attestation, Distributed Access Control and Federated Learning together help ensure that health data can be used for research without ever leaving the control of their owners.
- Solutions envisioned align by design with the objectives of the **EOSC IF**, aiming to increase the value of scientific data assets through wide-spread availability and reduce the costs of scientific data management while ensuring adequate data protection following **EU regulations**.
- While realising the challenges of achieving technical, semantic, organisational, and legal interoperability, EOSC-TITAN will develop **automated technical solutions to manage, govern and bridge the gaps** in semantic, organisational, and legal interoperability.
- EOSC-TITAN's solutions will **help practitioners solve their regulatory and compliance challenges**, as well as semantic, and organisational interoperability challenges. They will be integrated **with EOSC-compliant data sources** and applications already during the project by **publishing them in the EOSC resource catalogue**.

Funded by the European Union

Thank you for your attention

Funded by the European Union

Funded by the European Union under the GA No 101129822. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Executive Agency (REA). Neither the European Union nor the granting authority can be held responsible for them.