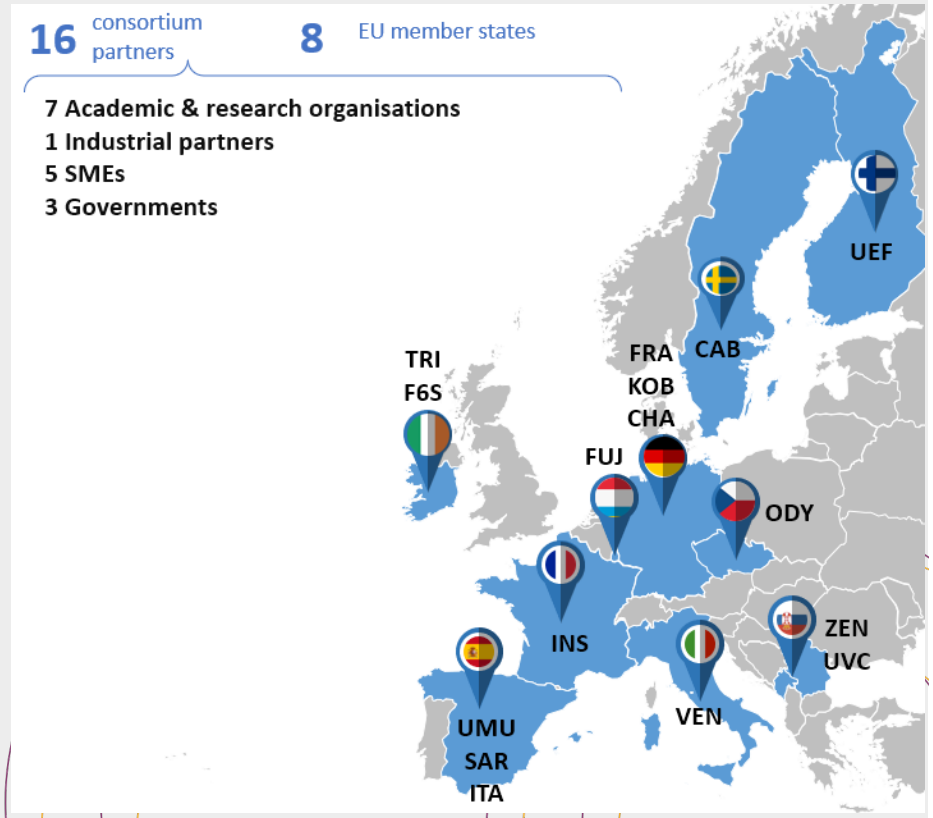
TITAN presentation

Trusted envIronments for confidenTiAl computiNg and secure data sharing

Antonio Skarmeta UMU



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.

Objectives

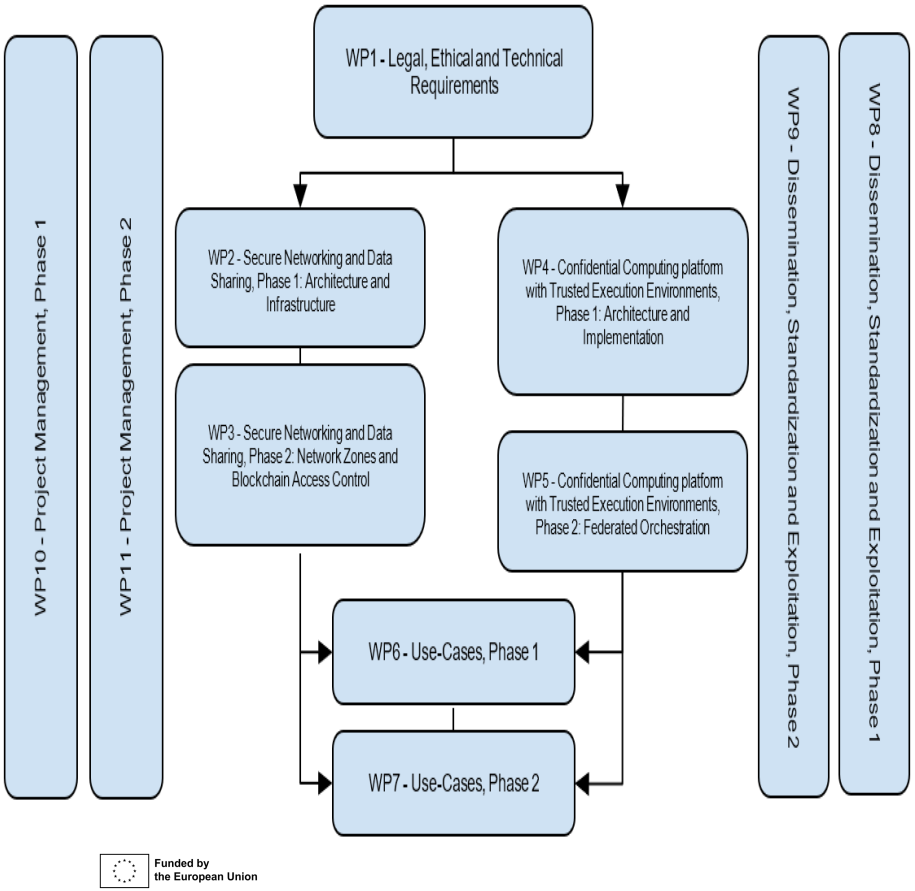
Enriching the EOSC with a **software platform solution for confidential data collaboration and secure and privacy-preserving data processing.**

- 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

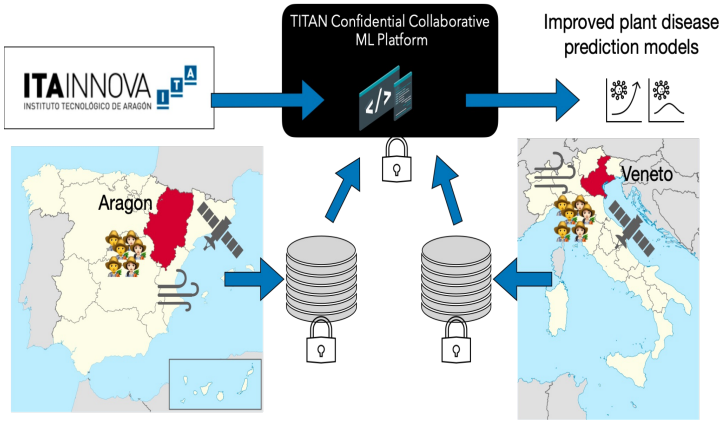
Organization

Use cases

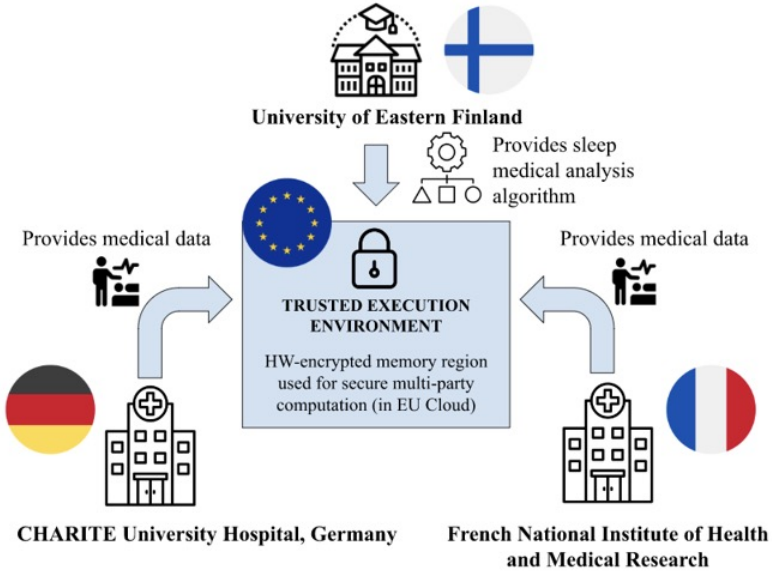


Funded by the European Union

- Use Case 1: Confidential sharing and collaboration with sensitive agrifood government data.



- Use Case 2: Collaborative Use of ML in Healthcare



Vision

New paradigm of secure access to sensitive public data and applications.

- **TITAN will focus on end-to-end secure data sharing and collaboration platform** requires advancements in network security, **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**
- **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

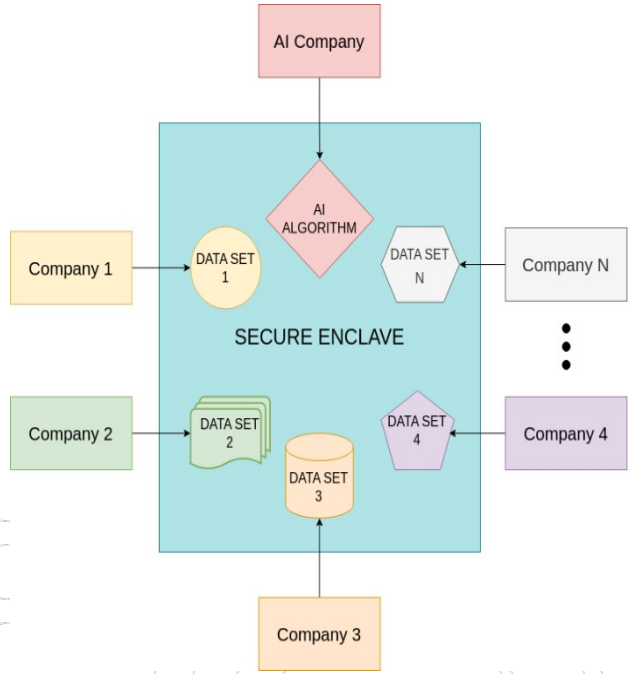
How TITAN can provide solutions to EOSC

- TITAN looks for mechanism to allow consumer and producer (data, processing, confidential processing, AI/ML algorithm service) describe their properties and capabilities using a FAIR approach
- Integrate a SSI and DLT based AAI solution interoperable with DSBA and EOSC
- Provide a matchmaking mechanism based on the meta-models used for describing capabilities to facilitate the put in communication consumer and providers in a data space governance architecture
- Support deployable and configurable connectors (following DSBA architecture) with different privacy preserving and confidential models to support the communication between consumer and providers
- Integrate mechanism to control what to share, with whom and how the data sharing will take place
- Provide confidential computing capabilities on demand to support data treatment based on TEE, secure enclave and federated learning functions

Funded by the European Union

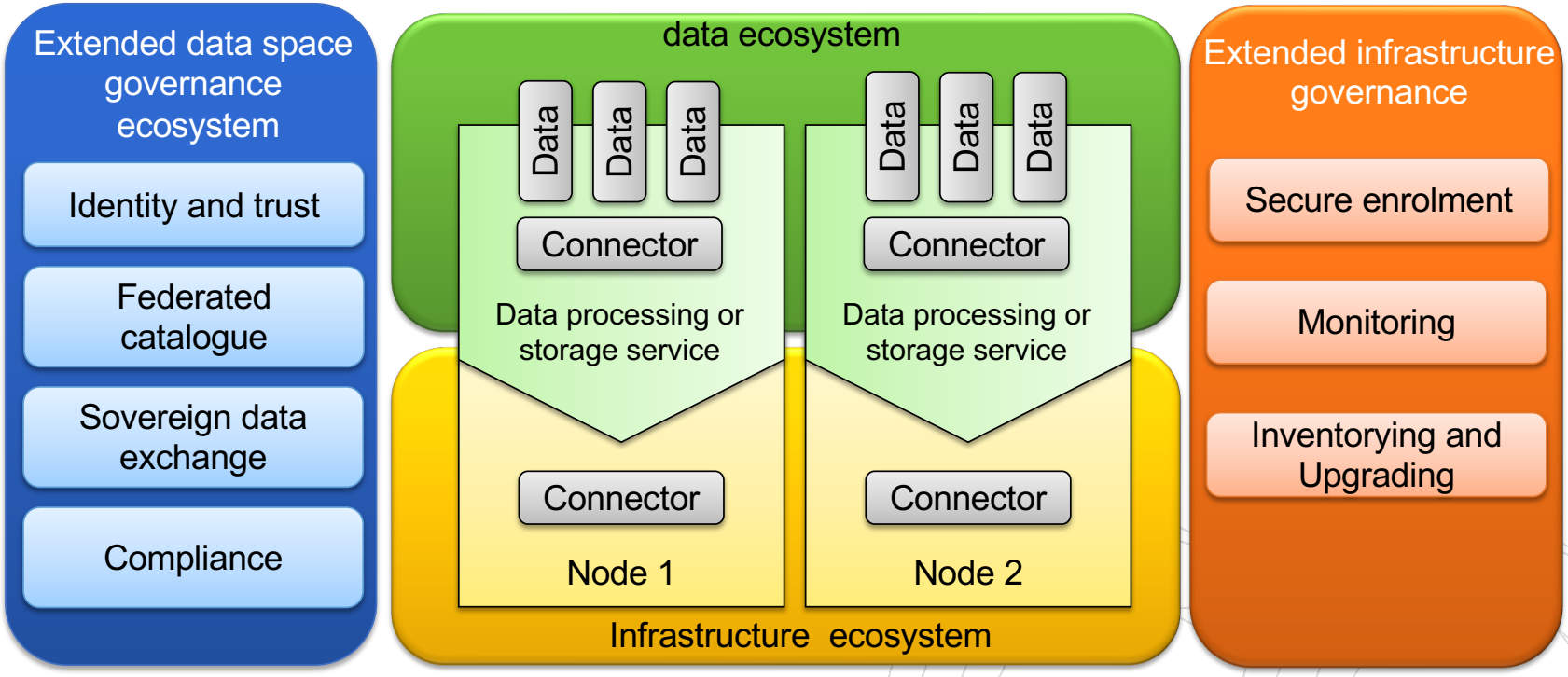
How TITAN can provide solutions to SPE

- TITAN will develop an improved **access control management ecosystem through the application of DLTs**, and more concretely **smart-contract-enabled blockchains**
- **Privacy-preserving, collaborative (confidential multi-party) ML** by combining the aforementioned techniques and leveraging Federated ML. To achieve immutability of the learning data model, the model will be stored on the **distributed ledger**.
- TEEs to implement confidential data processing for the shared datasets
- Discovery, sharing, and federation of heterogeneous data from multiple sources, **semantic interoperability data models**



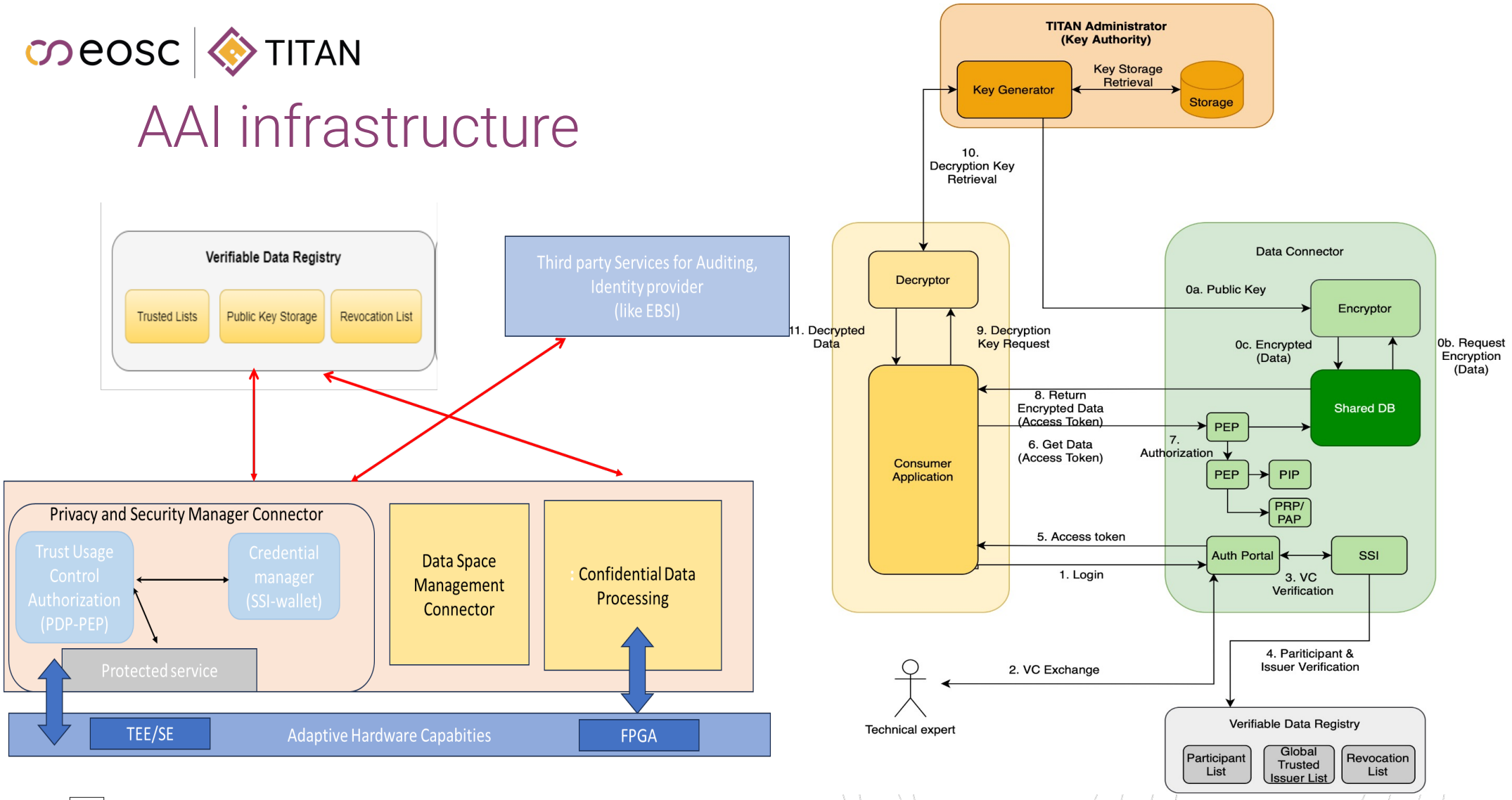
Funded by the European Union

High Level Architecture



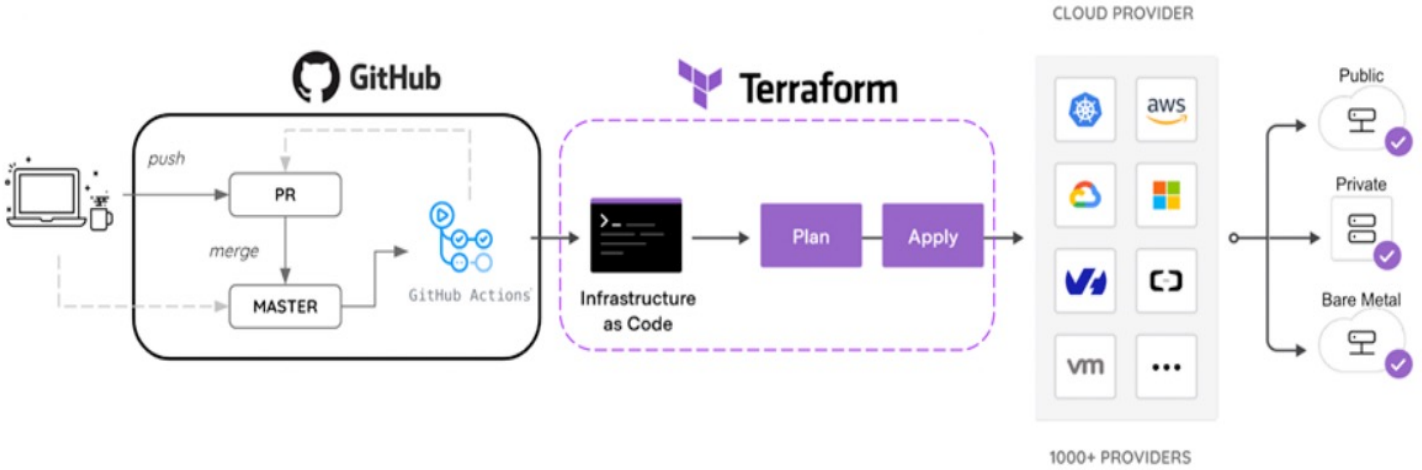
Funded by the European Union

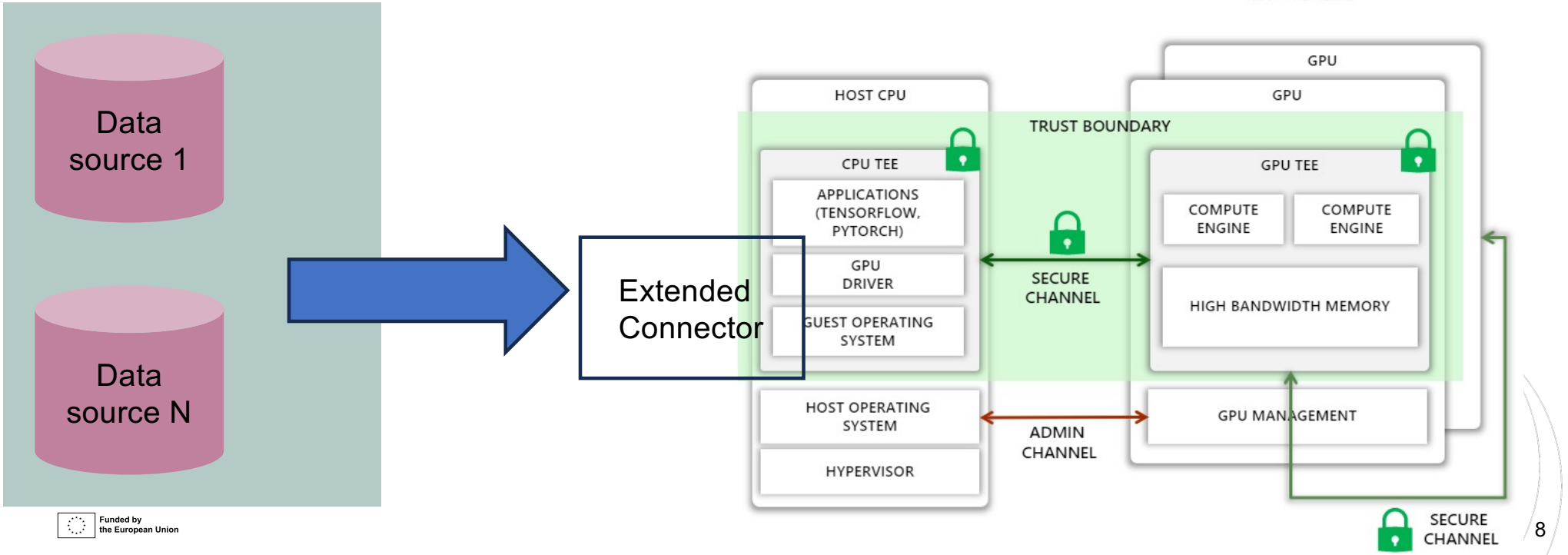
AAI infrastructure



Funded by
the European Union

Confidential Execution of processing over data





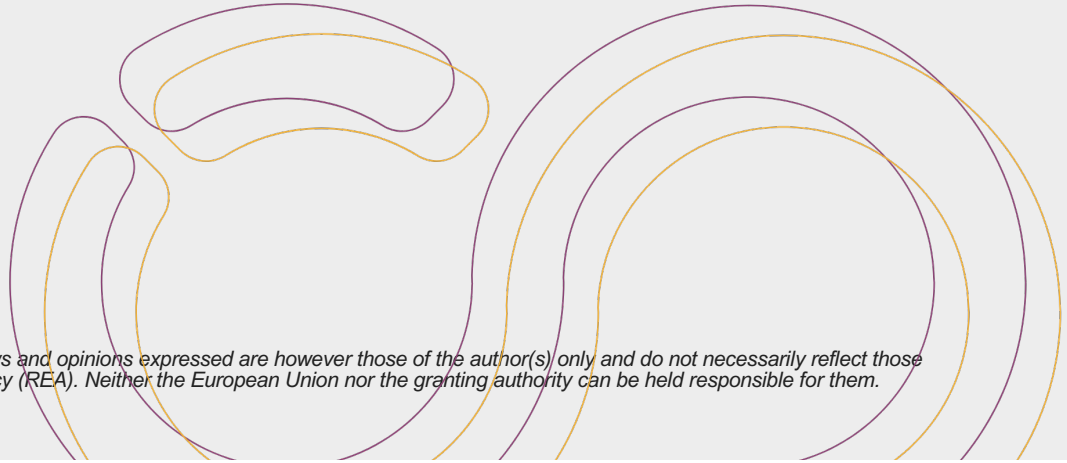
Funded by the European Union

Conclusion

- 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.
- Solutions envisioned in TITAN 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, **TITAN will develop automated technical solutions to manage, govern and bridge the gaps** in semantic, organisational, and legal interoperability.
- TITAN's solutions will **help practitioners solve their regulatory and compliance challenges**, as well as semantic, and organisational interoperability challenges. To validate the utility of TITANs solutions for the EOSC IF and ensure that results are exploitable.
- The developed solutions 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.