TEADAL

Privacy-Enhancing Technologies Toolbox

Eduardo Brito
Cybernetica AS

WWW.TEADAL.EU

TEADAL

Towards Privacy-Aware Federated Data Lakes

Privacy-preserving technologies are indispensable tools in **data-driven applications**, especially in settings where **sensitive data** needs to be **protected**, while maintaining their **utility**.

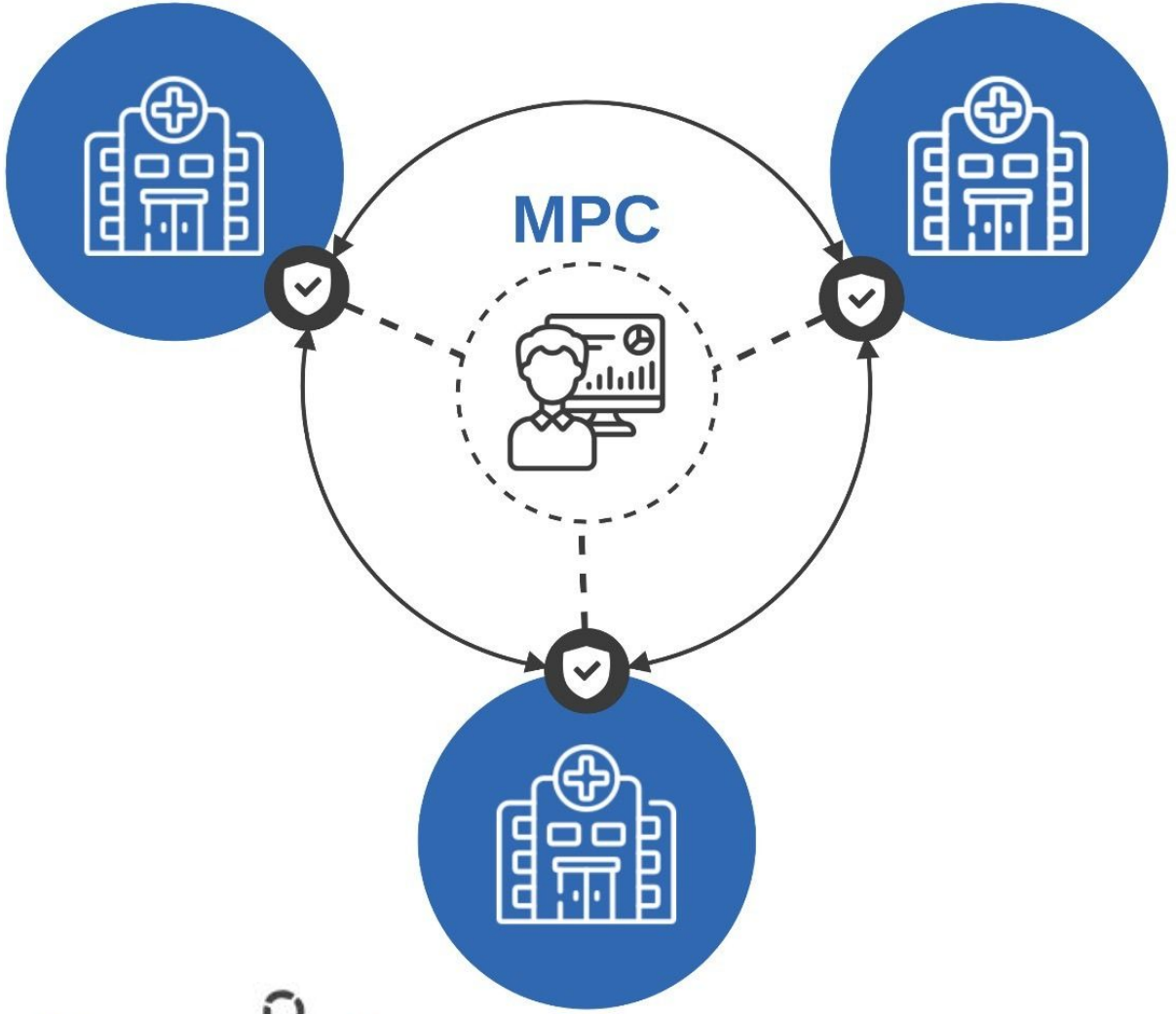
Three key technologies are:

- Secure Multi-Party Computation (MPC),
- Trusted Execution Environments (TEEs),
- Zero-Knowledge Proofs (ZKPs).

Overall, these technologies make it possible to perform **generic computations** on sensitive data without compromising its **confidentiality**.

TEADAL

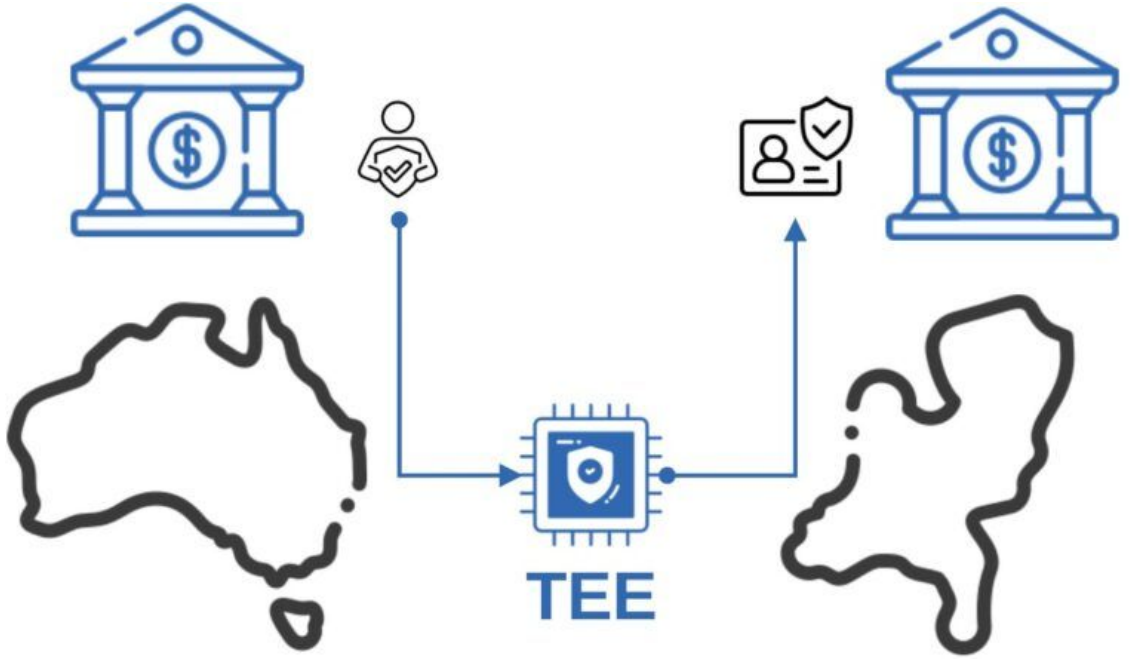
Secure Multi-Party Computation (MPC): Combining Data Without Compromise



sharemind
BY CYBERNETICA

TEADAL

Trusted Execution Environments (TEEs): Ensuring Confidentiality in Data Insights



sharemind
BY CYBERNETICA

TEADAL

Zero-Knowledge Proofs (ZKPs): Concealing Details, Proving Validity

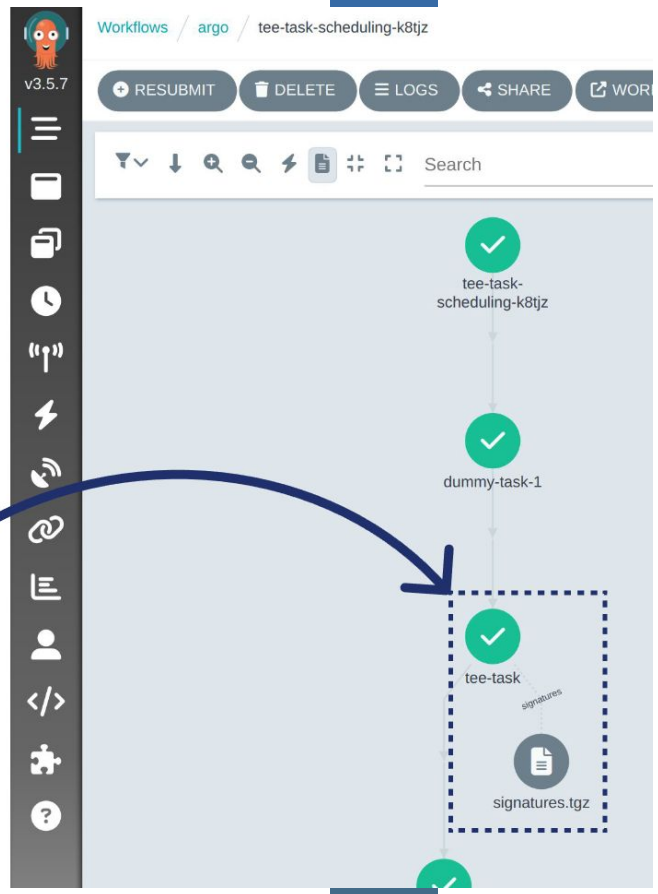
ZKSC ZK-SecreC

Sharemind MPC tooling and technology

We have successfully demonstrated **Sharemind MPC** runtime integration with TEADAL baseline technologies.

We demonstrated how to encode privacy-preserving computations in the **SecreC** programming language and ran the demonstrator with three computing nodes, generating a large **output** dataset from three **private** input datasets.

```yaml
apiVersion: argoproj.io/v1
kind: Workflow
...
templates:
- name: tee-workflow
  steps:
  - - name: dummy-task-1
      template: dummy-task-1
    - name: tee-task
      template: tee-task
    - name: dummy-task-2
      template: dummy-task-2
...
- name: tee-task
  podSpecPatch: '{"runtimeClassName":"kata-qemu-tdx"}'
  container:
    image: nixos/nix:latest
    command: [sh, -c]
    args: [
      "nix-shell trustops.nix && zip signatures.zip signature.*"
    ]
    volumeMounts:
    - name: workdir
      mountPath: /tmp/vol
  outputs:
    artifacts:
    - name: signatures
      path: /tmp/vol/{{workflow.name}}/signatures.zip
...
```

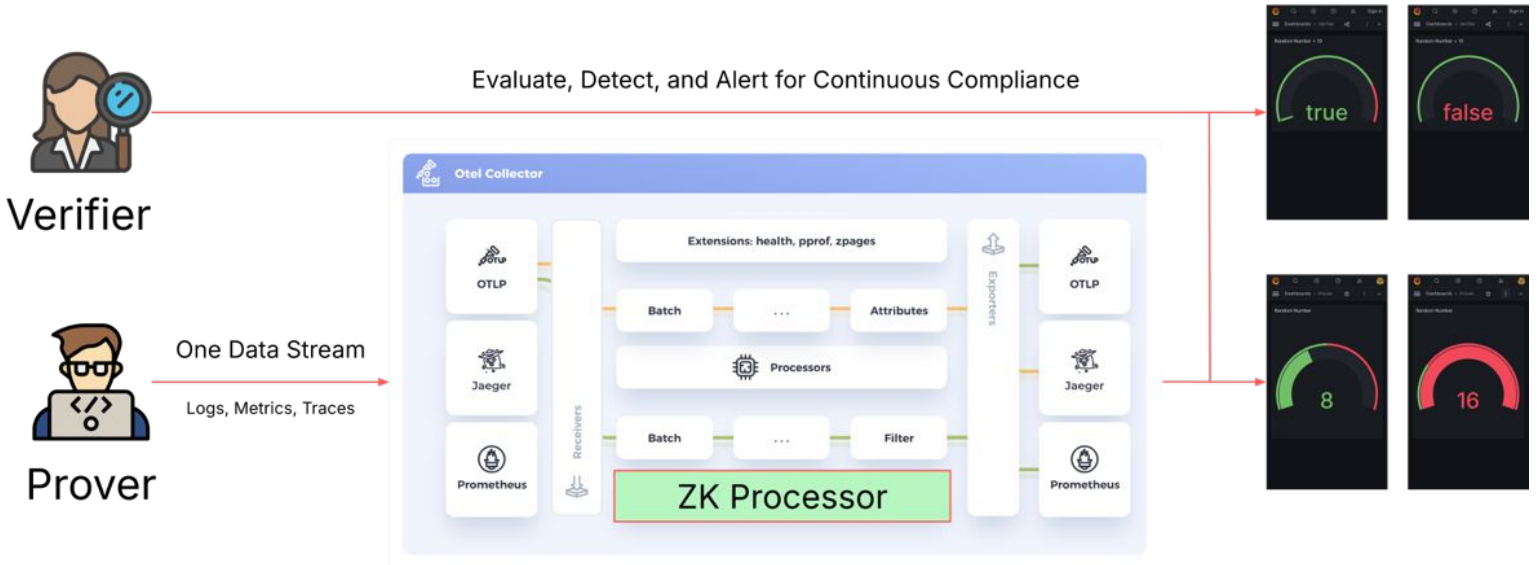


TEE-based Pipelines

We demonstrated the programmability, integration, and execution of **privacy-preserving data pipelines**, in a distributed setting consisting of a multi-node Kubernetes cluster.

Private tasks in a pipeline are **offloaded and orchestrated** to run on trusted confidential computing units, even if the host system is untrusted.

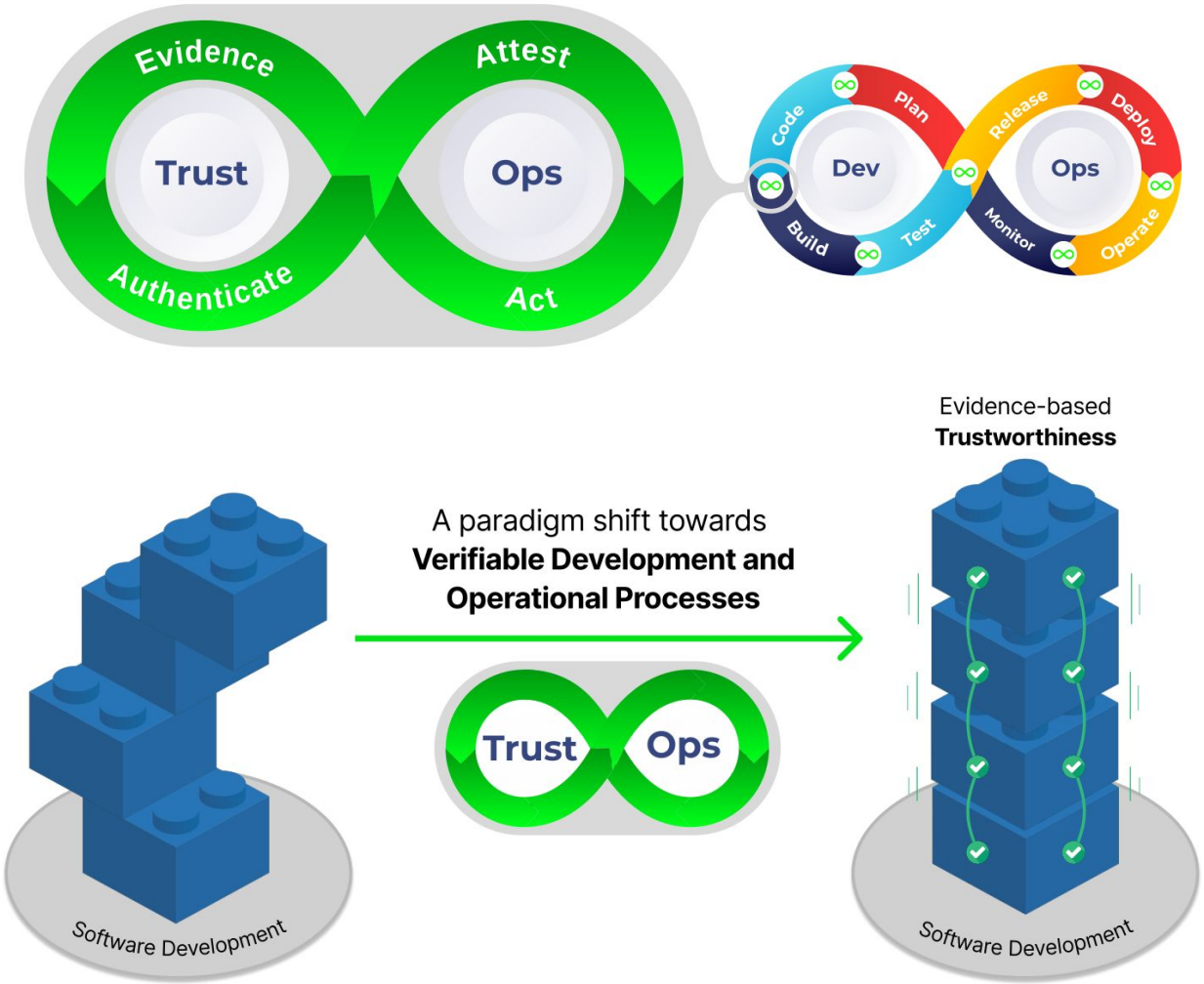
ZK-enabled Monitoring



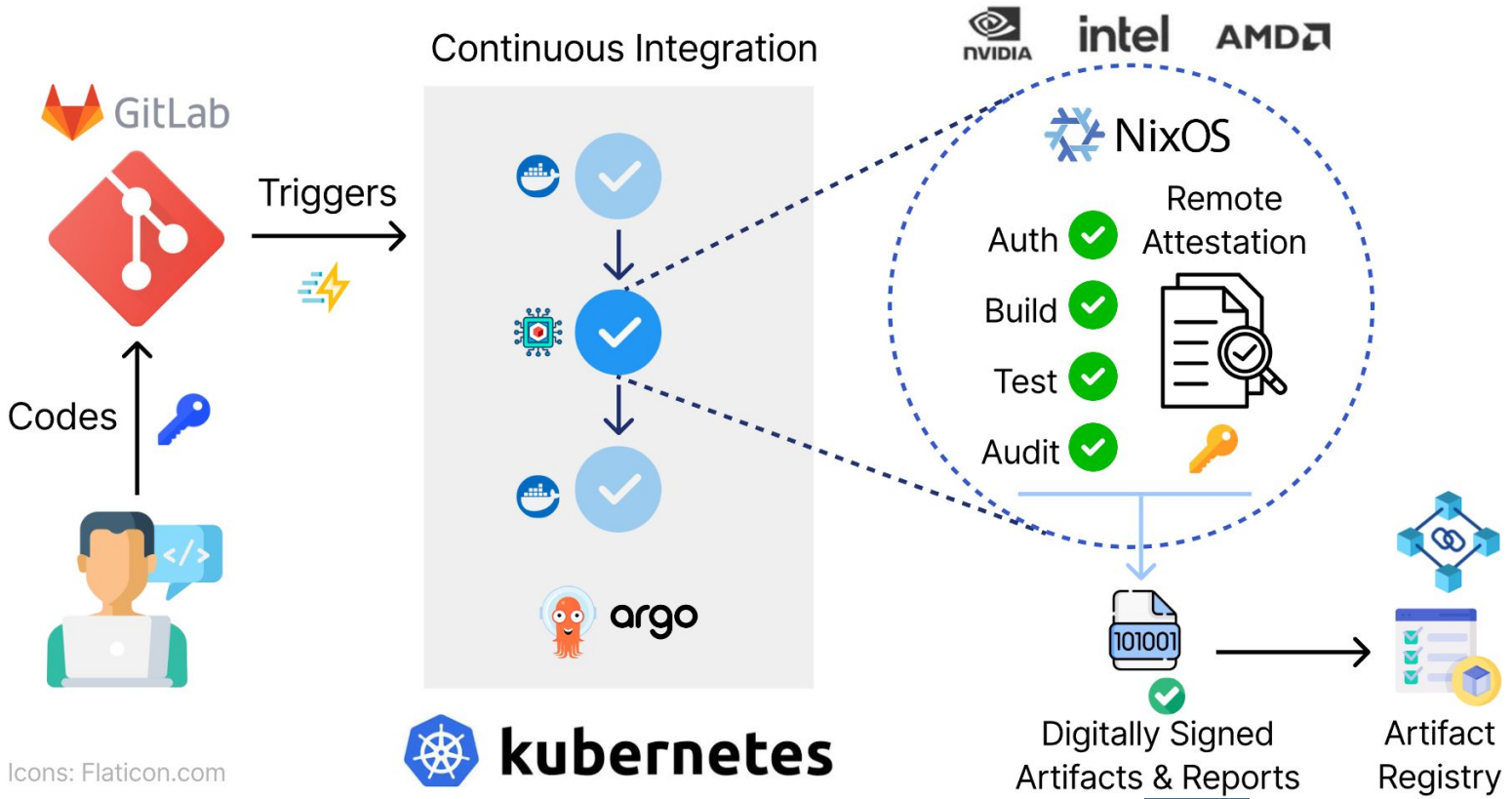
We have successfully encoded **verifiability statements** in ZK-SecreC, specifically for SLA verification.

We created an initial prototype and demonstrated its integration with **monitoring and observability** tooling used in TEADAL.

TrustOps: Continuously BuildingTrustworthy Software



Brito, Eduardo, et al. "Trustops: Continuously building trustworthy software." *International Conference on Enterprise Design, Operations, and Computing*. Cham: Springer Nature Switzerland, 2024.

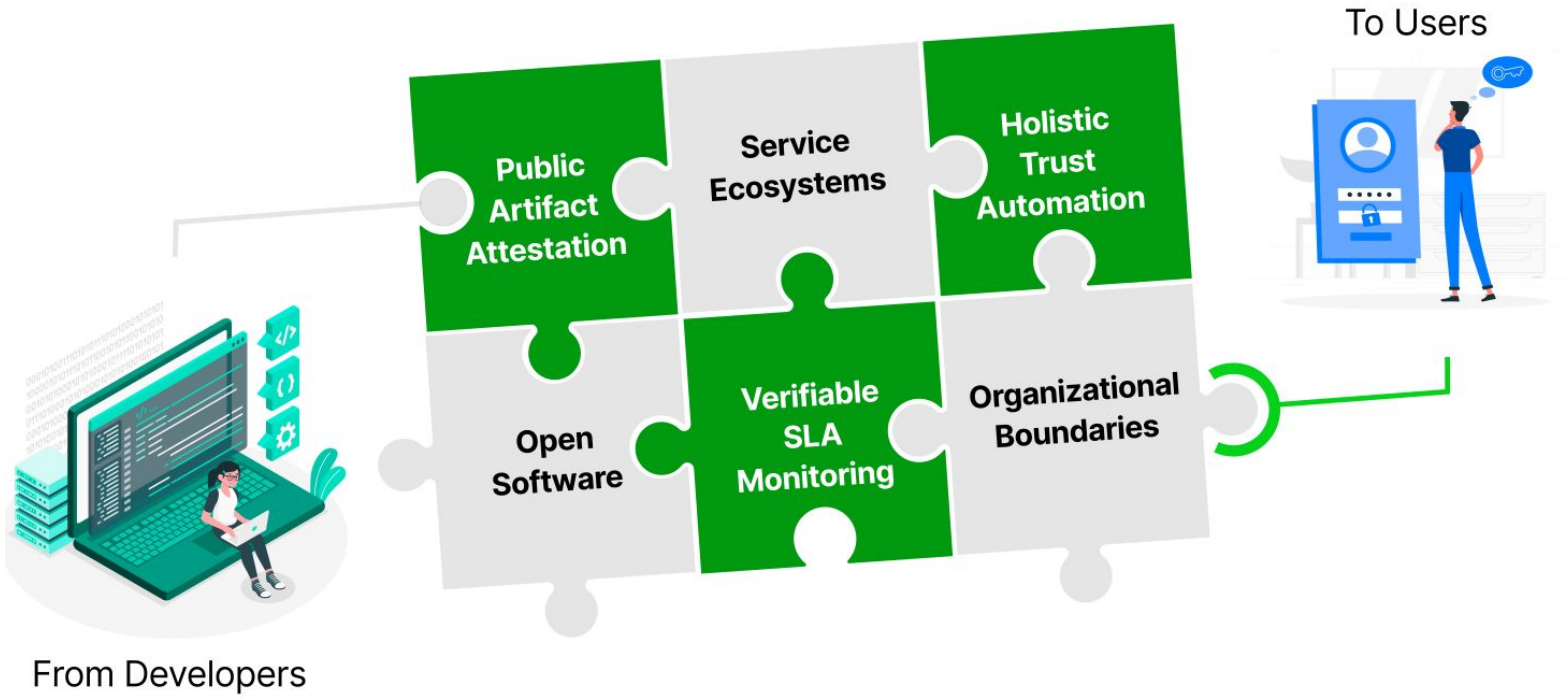


Trustworthy CI Pipelines

Following **TrustOps** principles, we created a first prototype of a **Trustworthy CI pipeline** and demonstrated its potential integration with TEADAL-related baseline tooling.

We developed a prototypical scenario for generating **attestable artifacts** from build, test, and audit phases of a piece of software.

Towards Securing the Software Supply Chain



TEADAL work opened **new research directions and collaborations** towards exploring the mechanisms prototyped within **new domains** such as software supply chain security.

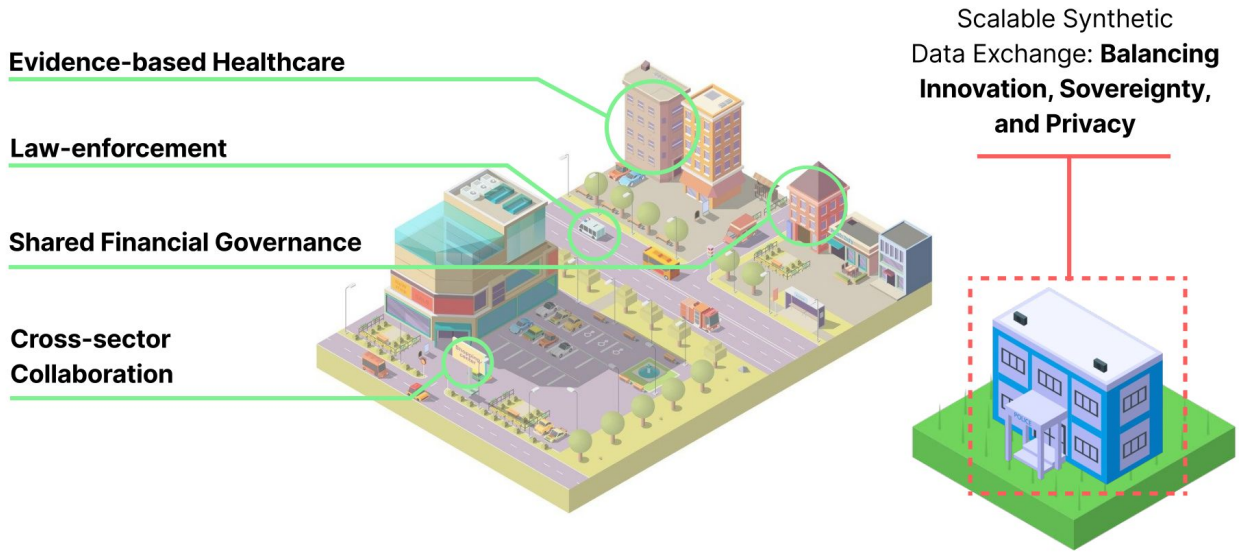
This work also inspired collaboration within **upcoming HE proposals** and **cross-project exploitation** of TEADAL results.

TEADAL

SynthGuard: Redefining Synthetic Data Generation with a Scalable and Privacy-Preserving Workflow Framework

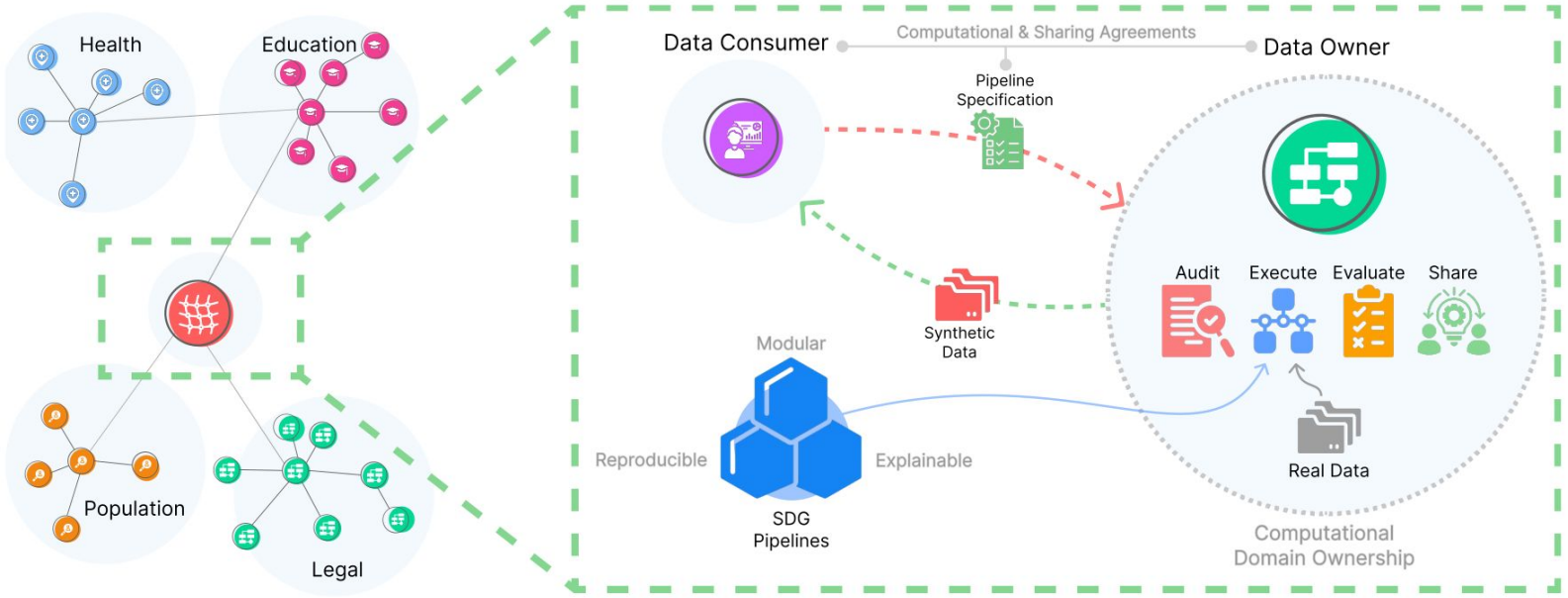
Brito, Eduardo, et al. "SynthGuard: Redefining Synthetic Data Generation with a Scalable and Privacy-Preserving Workflow Framework." International Conference on Availability, Reliability and Security. Cham: Springer Nature Switzerland, 2025.

Legally Constrained Heterogeneous Data Silos



SynthGuard

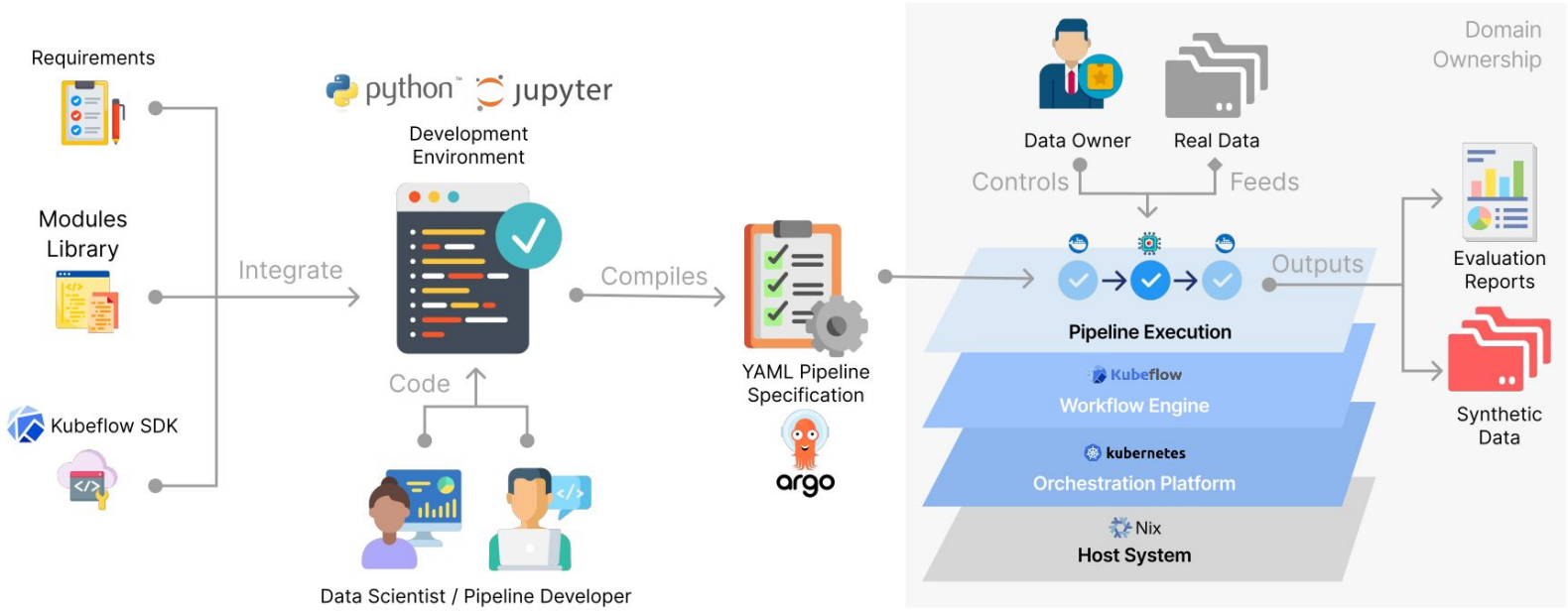
Synthetic Data Generation & Sharing



Inspired in TEADAL methods, we developed a synthetic data generation **architectural approach** for secure synthetic data sharing in constrained data domains.

Our approach targets **data mesh** principles of domain ownership, data sovereignty, and computational governance to enable generating and sharing synthetic datasets.

Synthetic Data Generation Workflow



We demonstrated technological and integration **feasibility** with TEADAL tools and architecture.

In the early project phases, we generated synthetic data for **pilots** and modelled **pipelines** and datasets based on pilot requirements, real dataset schemas, and use case goals. These datasets supported ongoing **validation**.

CYBERNETICA

Conclusion

- *Demonstrated PETs technological and integration feasibility with TEADAL tools and architecture*
- *Successfully generated synthetic datasets aligned with pilot requirements and real data schemas*
- *Established pipelines and workflows for ongoing validation and use case goals*
- *Opened pathways for secure, privacy-preserving data sharing and future applications*

TEADAL

THANKS

TEADAL.EU

@TEADAL_eu

@TEADAL

Funded by
the European Union

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
**State Secretariat for Education,
Research and Innovation SERI**

**TEADAL project is funded by the EU's Horizon Europe programme under Grant Agreement number 101070186.
This work has received funding from the Swiss State Secretariat for Education, Research and Innovation (SERI).**