TEADAL

TEDAL Components for Trustworthiness

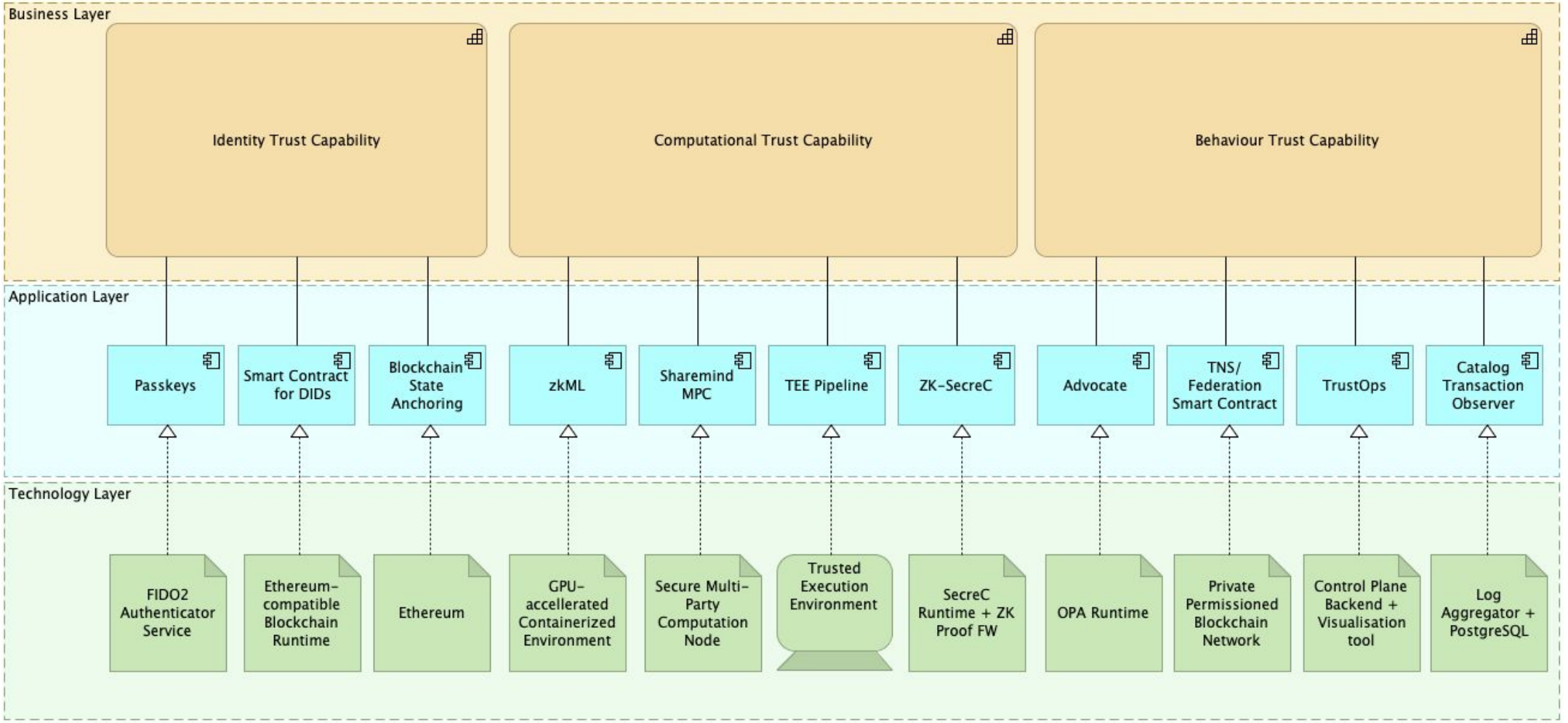
Fernando Castillo

Technische Universität Berlin

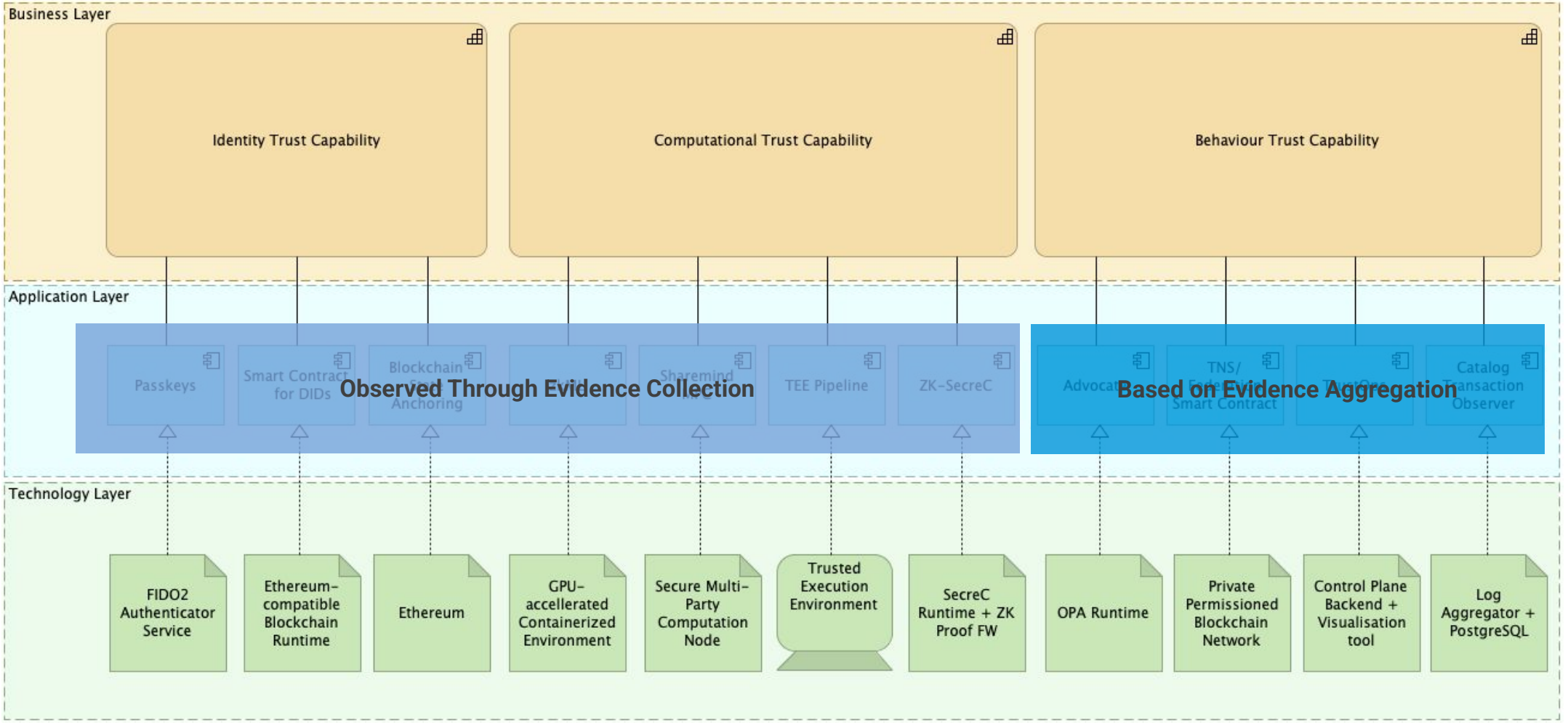
02/10/2025

WWW.TEADAL.EU

Trust Plane Overview



Trust Plane Overview



Passkeys with Blockchain

- Passwordless authentication managed through smart contracts.
- Portable identities linked to DIDs, allowing seamless use across multiple services.
- Access control and governance enforced by on-chain policies.
- Ensures full transparency and compliance in identity management over time.

Decentralized Identity Management with Smart Contracts

- Supports policy-based access, trust delegation, and decentralized governance.
- Ensures auditability of identity actions and access control decisions, providing full transparency for security and compliance.
- Developed an interoperable DID registry supporting cross-platform identity management and decentralized trust.

Blockchain State Anchoring

- Periodically anchoring private blockchain state to public blockchains to ensure a tamper-resistant record of the private blockchain's state

- Enhanced Security: Only approved actors can write on the permissioned blockchain.

- Privacy preserving: Information stored on the private blockchain are not exposed publicly.

- Increased throughput: More transaction per seconds than public blockchain.

- Successfully tested on a development environment using the public Sepolia Ethereum testnet.

Zero-Knowledge Machine Learning (ZKML)

- Easy Zero-Knowledge Inference (EZKL): Library designed to simplify inference verification using Zero-Knowledge Proofs (ZKPs)

- Integration with a TEADAL AI model:
  - Enhanced data security: Input data does not need to be shared to verify the inference process
  - Trustlessness: Decentralized inference verification through smart contract can be validated by any third party without relying on a central authority

Sharemind MPC

- Secure multi-party computation (MPC) framework that enables multiple parties to jointly compute functions over their private data without exposing the underlying inputs.

- Integrated into data pipelines to facilitate secure, collaborative data analysis and aggregation.

- Enhances overall data privacy while supporting collaborative processing in federated environments through evidence logging and auditing.

- Successfully demoed with TEADAL baseline technologies.

Trusted Execution Environment (TEE) Pipeline

- Provide runtime mechanism for executing Privacy-preserving Data Pipeline tasks securely.
- Secure runtime environments can interact with TEADAL's identity management, observability, and evidence collection tools.
- Reinforces trust and ensures that sensitive operations are verifiable and compliant with regulatory standards.
- Successfully demonstrated in the former Shared Financial Data Governance pilot to securely process sensitive financial data while ensuring strict regulatory compliance.

Metric	Without	With
Total Workflow Time (min)	4.15	7.50
CPU Consumption (s per CPU)	27	49
Memory Consumption (s per 100MiB)	6	12
Runtime of Tasks (s)	65.8	141.5
Evidence Size (B per signature)	N/A	294
Cryptographic Operation Time (ms per Op)	N/A	80
Blockchain Commit Time (ms)	N/A	213

Average comparison results of 10 runs: integrating TEEs into CI pipelines introduces moderate, controlled overhead

ZK-SecreC

- High-level, domain-specific language designed specifically for developing zero-knowledge proofs.
- Enforces trustworthy and verifiable programmability.
- Demonstration of consumer-provider SLA verifiability in cloud service provisioning.

Metric	ZK-SecreC	zk-SNARK
Prover Avg. Execution Time	3432.12 ms	306.48 ms
Prover Min/Max Execution Time	3073.00 / 3673.00 ms	252.00 / 367.00 ms
Verifier Avg. Execution Time	3332.17 ms	5.30 ms
Verifier Min/Max Execution Time	2978.00 / 3553.00 ms	3.00 / 11.00 ms

Execution time comparison between ZK-SecreC and zk-SNARK implementations

Metric	ZK-SecreC	zk-SNARK
Prover Avg. CPU usage	33.11%	7.13%
Verifier Avg. CPU usage	29.68%	1.02%
Prover Avg. Memory usage	1231.55 MB	1608.27 MB
Verifier Avg. Memory usage	1545.53 MB	962.24 MB

Figure 2: Resource usage comparison between ZK-SecreC and zk-SNARK implementations

Advocate and TNS/Federation Smart Contracts

Advocate

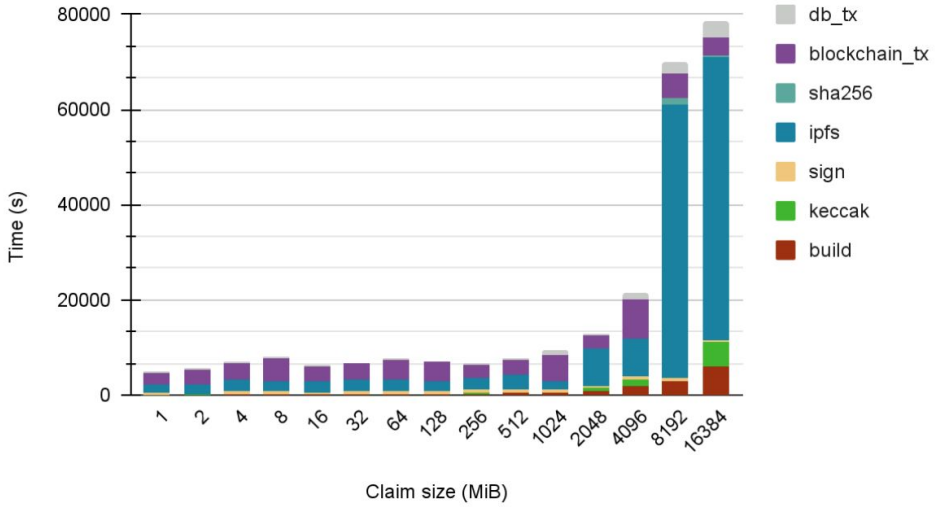
- Verifiable, tamper-proof evidence collection (supports a diverse range of evidence sources and types, e.g., Jaeger or an Istio Gateway).
- Enables auditability of collected verifiable evidence.
- Enables aggregation and policy-driven transformations.
- Installed in three pilots: Evidence-based Medicine, Smart Viticulture, Industry 4.0.
- Paper: “Advocate - Trustworthy Evidence in Cloud Systems” [2]

TEADAL Name Service (TNS)

- Allow human-readable names to be associated with blockchain addresses and resources.

Federation Smart Contracts

- Manage the governance and operations of the federation.

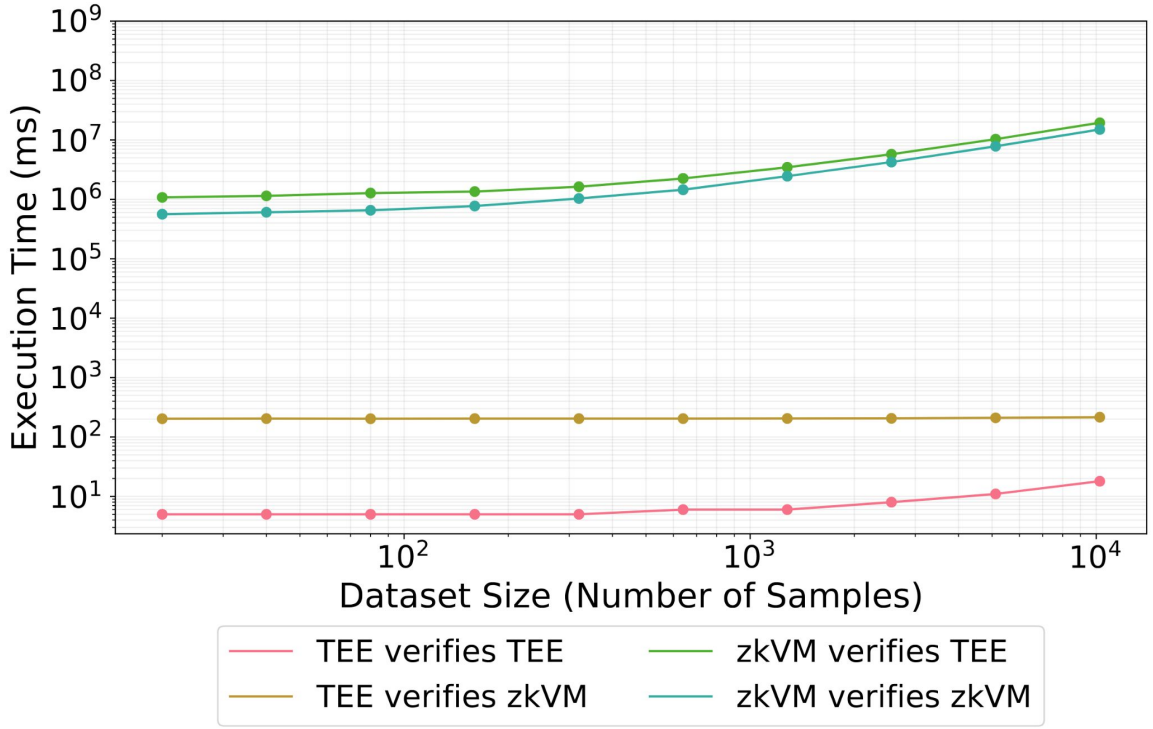


Advocate claim creation performance

[2] S. Werner, S. Masoudi, F. Castillo, F. Piper, J. Heiss. “Advocate - Trustworthy Evidence in Cloud Systems,” in 6th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 2024.

TrustOps

- Set of practices and a methodology, designed to embed evidence-driven trust throughout the software life cycle.
- Integration of evidence-driven practices into TEADAL's data exchange, federated service operations, and the development of software components.
- Paper: "TrustOps: Continuously Building Trustworthy Software" [3].
- Paper: "Trusted Compute Units: A Framework for Chained Verifiable Computations" [4].



Training time comparison of zkVM and TEEs with zkVM or TEE as previous phase.

[3] E. Brito, F. Castillo, P. Pullonen-Raudvere and S. Werner, "TrustOps: Continuously Building Trustworthy Software," in 28th International Conference on Enterprise Design, Operations and Computing, 2024.
[4] F. Castillo, J. Heiss, S. Werner, and S. Tai, "Trusted Compute Units: A Framework for Chained Verifiable Computations," in IEEE International Conference on Blockchain and Cryptocurrency, 2025.

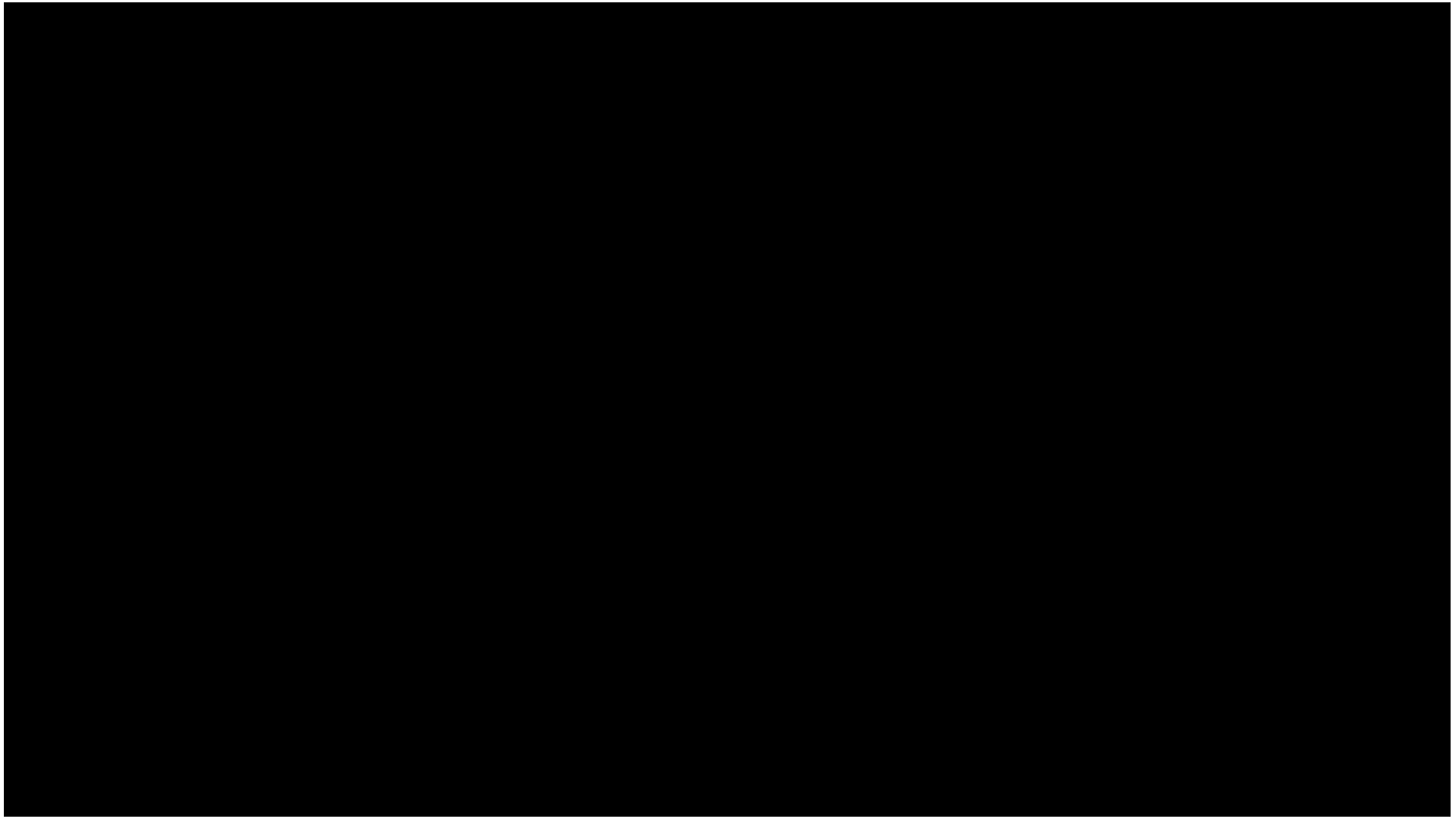
Catalog Transaction Observer

- Catalogue can be configured to execute BPMN processes as a response to two main interactions:
  - Lifecycle events (publishing, editing, deleting) related to assets descriptions
  - Requests that a user can trigger related to a specific asset, like requesting access to an FDP or requesting to advertise an asset through a dataspace connector
- Inserting BPMN activities in the right parts of such processes allow immutability logging events to Advocate

(Some) Evidence sources

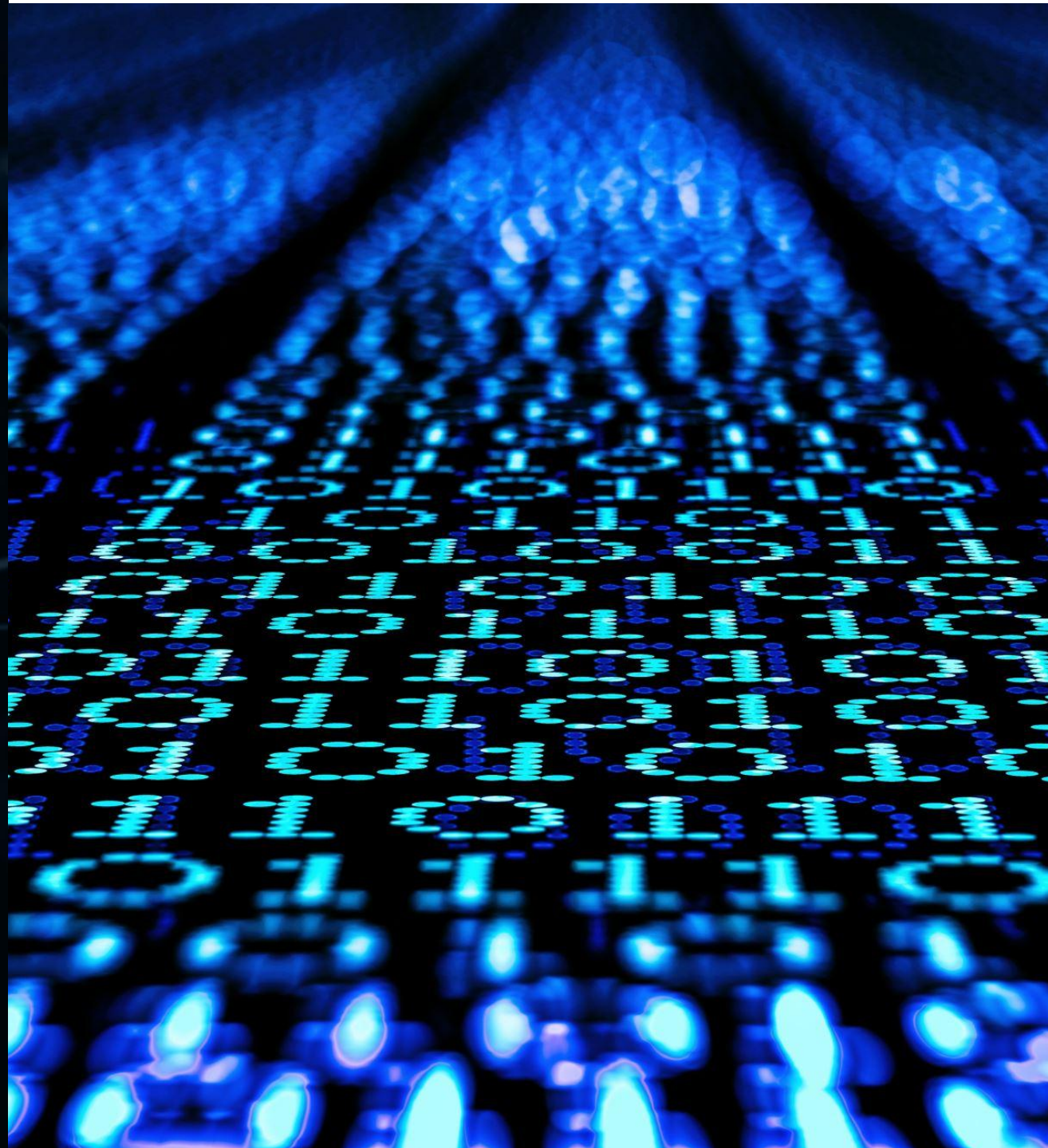
- Identity Management Actions.
- FDP/sFDP Access.
- FDP/sFDP Initialization.
- Data Pipeline Deployment.
- Resource Consumption Metrics.

DEMO (Claim Generation)

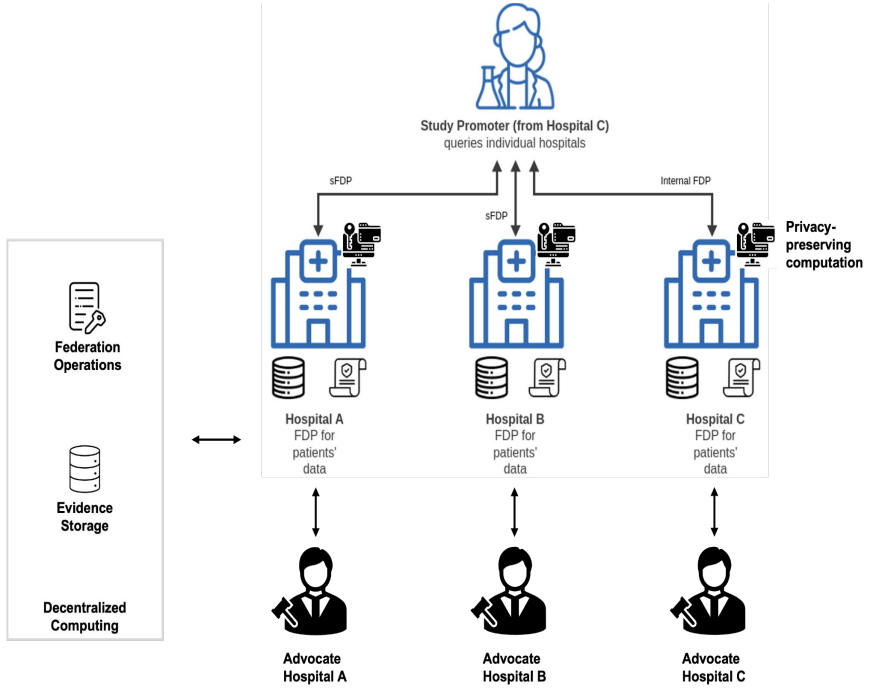


TEADAL

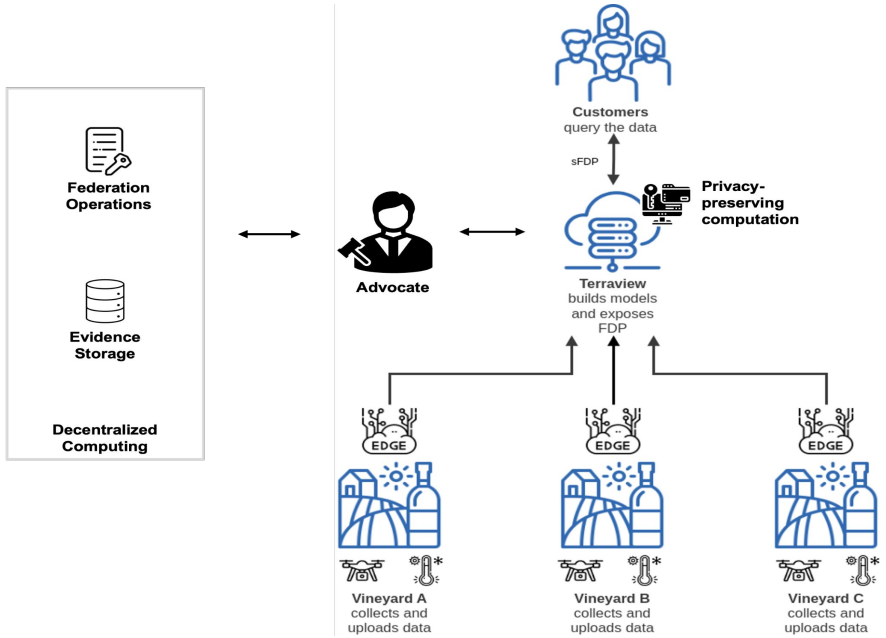
Integration of Pilot Cases and Privacy Tracking Scenarios



Pilot Cases

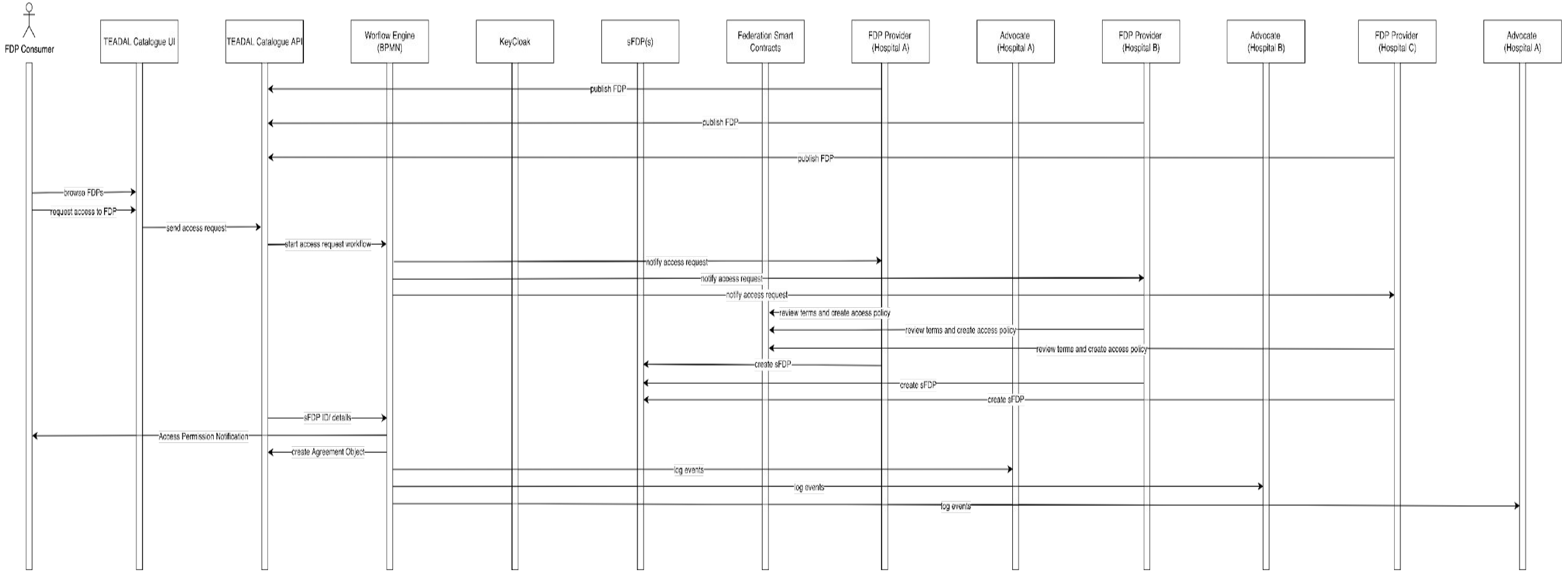


Evidence-based Medicine



Smart Viticulture

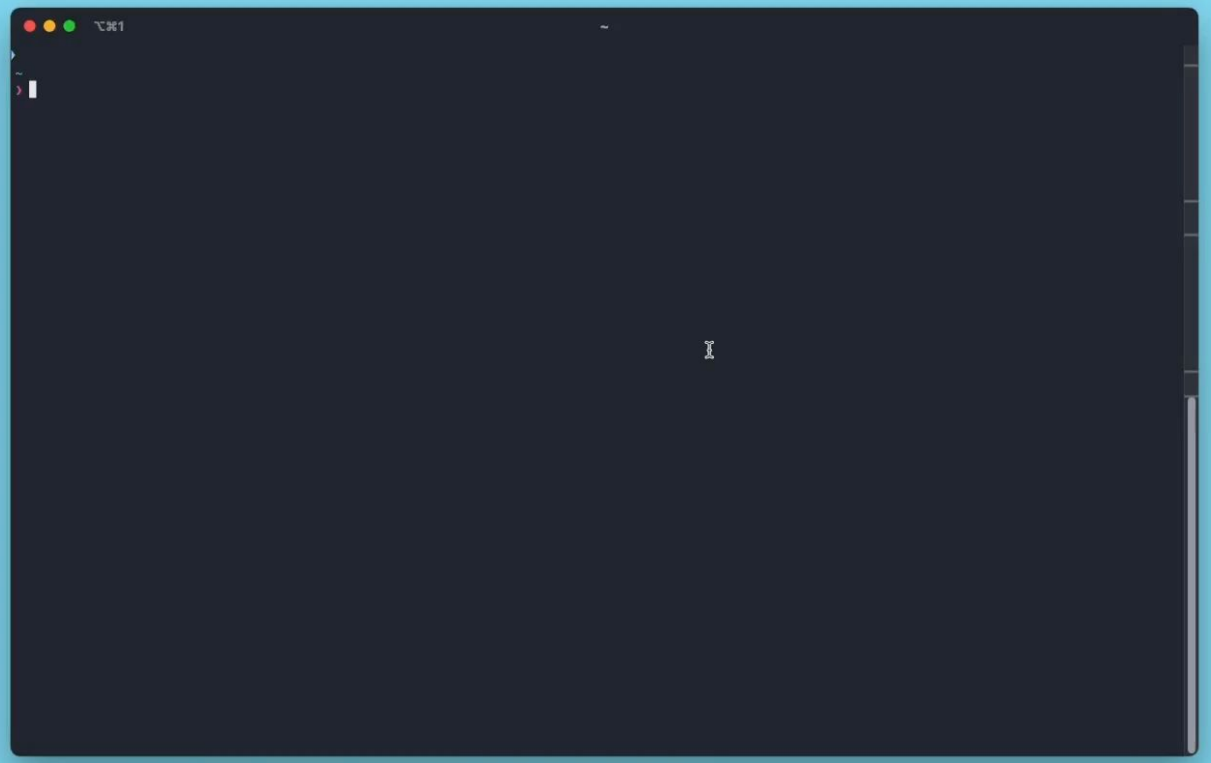
Integration of Evidence-based Medicine



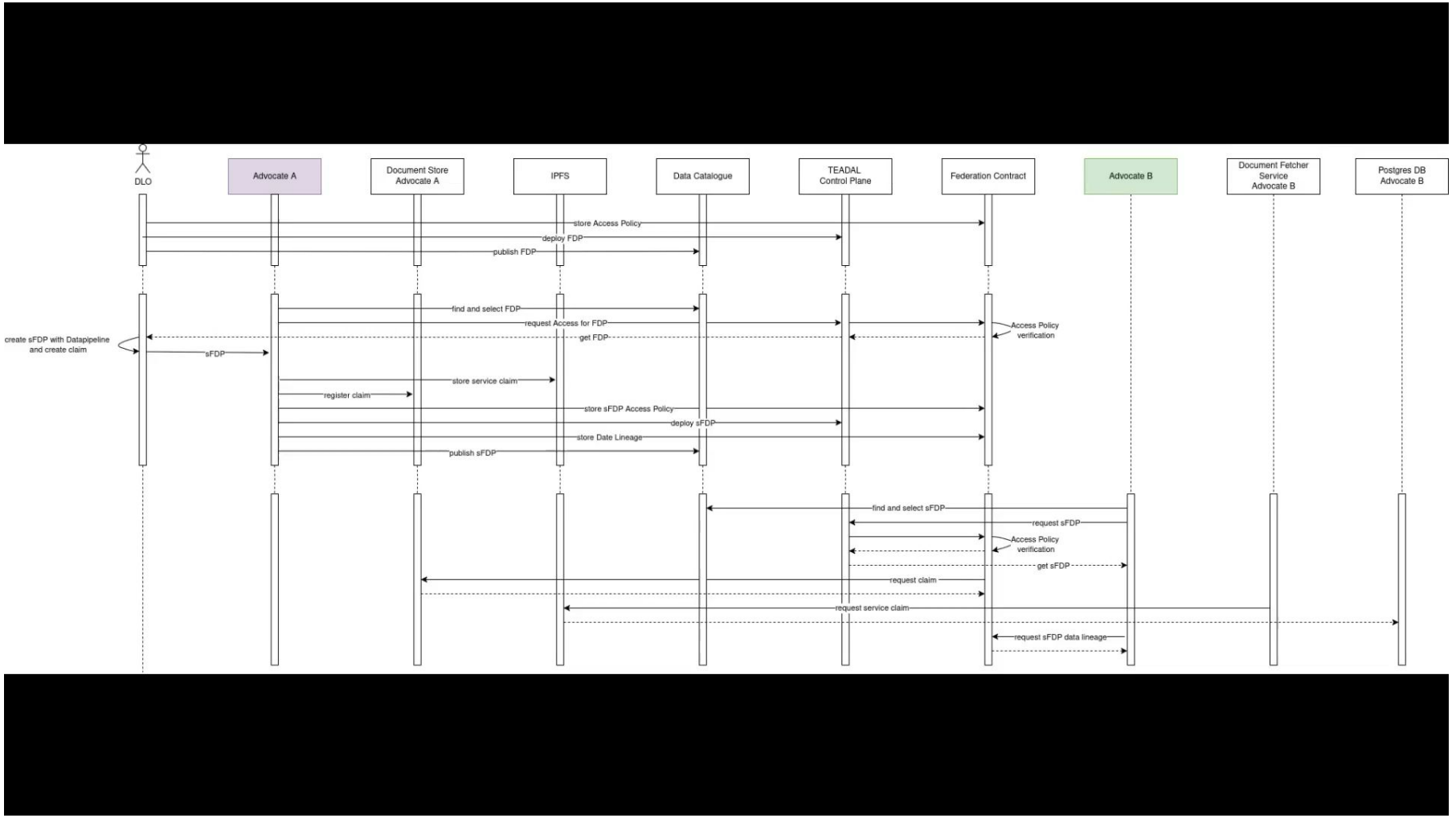
Integration of Privacy Tracking Scenarios

1. **Policy tracking**
2. **Cross-organization data usage**
3. **Data lineage tracking**
4. **Consent management**
5. **Data erasure**

Aggregation demonstration



Cross Organizational Use



Publications

- TrustOps: Continuously Building Trustworthy Software

  (29th Enterprise Design, Operations, and Computing. EDOC 2024 Vision)

- Advocate - Trustworthy Evidence in Cloud Systems

  (6th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS 2024))

- Building Trustworthy AI Systems: AI Inference Verification with Blockchain and Zero-Knowledge Proofs

  (6th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS 2024))

- Trusted Compute Units: A Framework for Chained Verifiable Computations

  (7th International Conference on Blockchain and Cryptocurrency (ICBC 2025))

- Towards Trusted Service Monitoring: Verifiable Service Level Agreements

  (TBP 23rd International Conference on Service-Oriented Computing (ICSOC 2025))

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).**