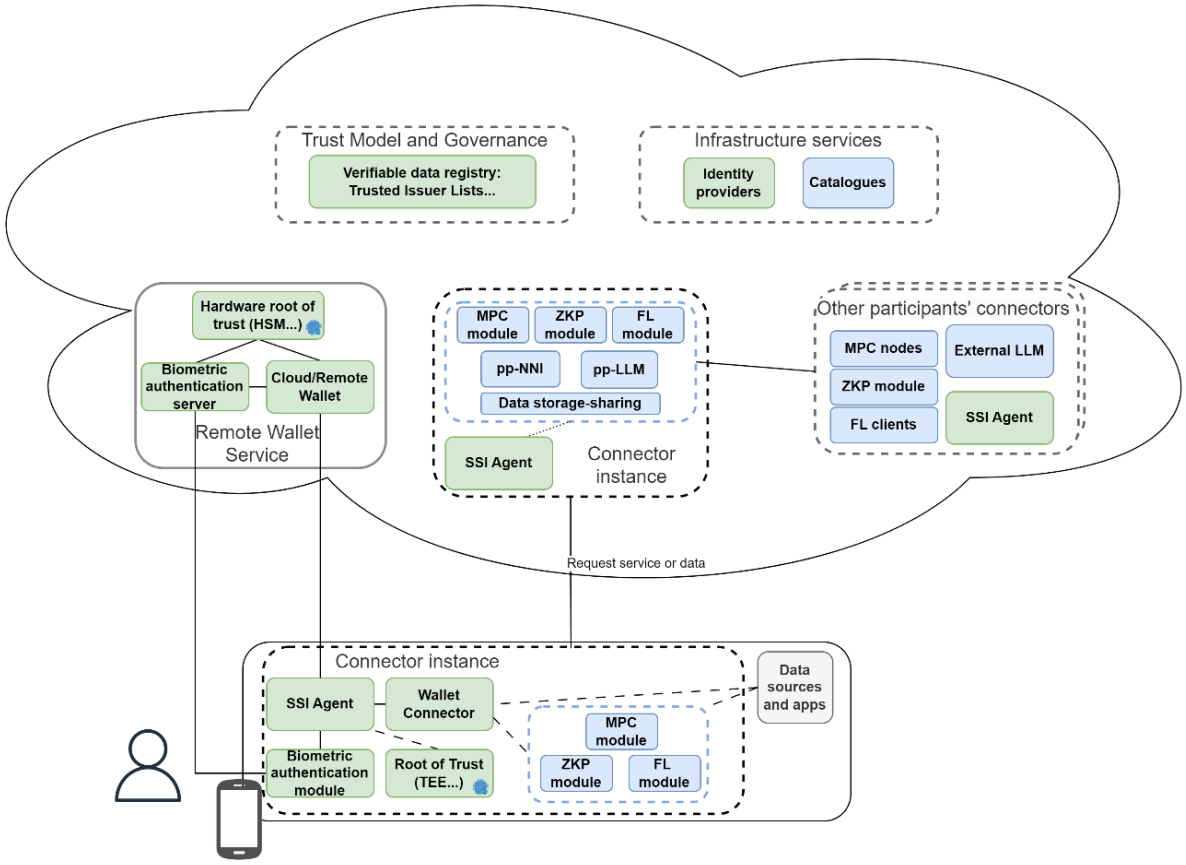
Jesus Garcia Rodriguez from University of Murcia (UMU)

The LICORICE Framework Blueprints

The LICORICE framework does not aim to create a single monolithic architecture. Instead, the project proposes a modular ecosystem of tools that can be combined depending on the needs of different participants.



The core LICORICE toolset blueprint is composed of several components that can be grouped into two main domains: tools related to self-sovereign identity management and tools designed for privacy-preserving data processing. The toolset, as showcased in the figure, is designed to synergistically leverage common concepts and technical approaches, protocols and best practices in two domains: the ecosystem of European Digital Identity and the initiatives within the EU's Data Strategy on Data for the development of data spaces.

Identity management tools

LICORICE is aligned and complements eIDAS Toolbox specifications, extending with highly secure approaches the security and privacy guarantees of the identity management solution. In this sense, the toolset includes:

SSI Agents allow the management of Verifiable Credentials aligned with the standards and specifications that are relevant in the eIDAS ecosystem European Digital Identity ecosystem, including OID4VCI and

OIDC4VP. These agents support the traditional roles present in self-sovereign identity systems: issuer, verifier and holder.

LICORICE considers the remote wallet configuration, where **cryptographic wallet services** (i.e., Wallet Secure Cryptographic Applications) are deployed remotely. That is, the functional management of the sensitive cryptographic material, such as the user secret keys, will occur in a backend server of the Remote Wallet Service provider, using advanced technologies for protecting secret material through a **Hardware Root of Trust,** such as Hardware Security Modules or secure computing techniques.

To strengthen the security of the wallet, the framework incorporates **Biometric Authentication**. This mechanism allows authentication processes to rely on biometric data to bind the wallet to its legitimate holder.

Lastly, the **Wallet Connector** acts as a bridge between external data sources and the wallet ecosystem. It enables generic data coming from sensors or mobile applications to be converted into interoperable formats based on Verifiable Credentials. As a result, this data can be shared securely through the identity ecosystem when required.

Privacy-preserving data processing

Following current trends for data spaces, the toolset is intended to be deployed on-demand by each participant in the data ecosystem depending on their needs for data processing. Thus, the tools will be aligned with the concept of "Personal Data Spaces". To achieve this goal, the tools cover different functionalities:

The toolset includes modules for verifiable computing on sensitive data, such as Multi-Party Computation (MPC) approaches and Federated Learning (FL) approaches. The main goal of these tools is performing privacy-preserving data processing for data distributed among different participants, while introducing as the main innovation the verifiability of the correctness of the computations carried out.

The framework also includes tools for enabling enable the use of AI-as a service while ensuring the privacy of the sensitive input data. Privacy-preserving Neural Network Inference (PP-NNI) deals with privacy-enhancing cryptographic mechanisms for avoiding sensitive data leakage during Neural Network Inference processes. Additionally, the pp-LLM module enables the anonymization of queries to Large-Language Models to provide insights over processed data without disclosing sensitive information.

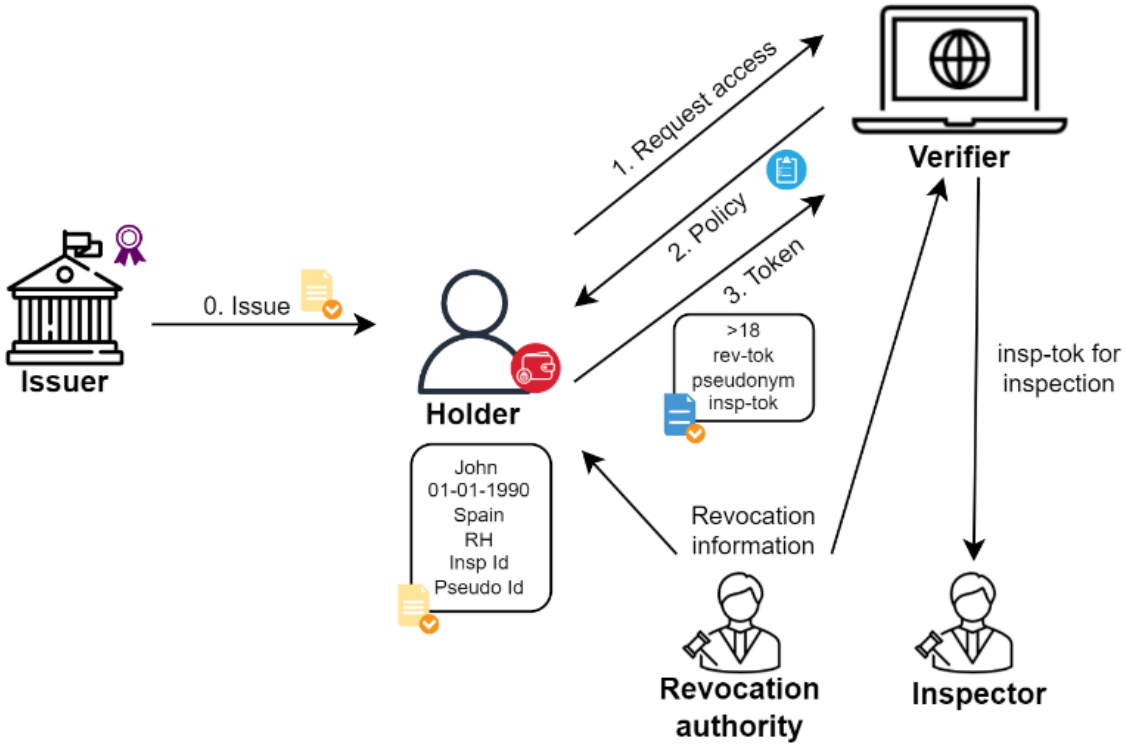
Finally, it is sometimes necessary to directly share data. In this case, tools for applying (pseudo)-anonymization techniques can help provide privacy-respecting data sharing, balancing data usefulness with the protection of potentially sensitive data.

Privacy-preserving Attribute-Based Credentials (p-ABC)

Key Features: Selective Disclosure and Unlikability

Privacy-preserving Attribute-Based Credentials (p-ABCs), also known as anonymous credentials, are systems that use advanced cryptography, often based on zero-knowledge proofs, to allow a user to derive a presentation proof from a digitally signed credential. This enables minimal disclosure, where only specific, required attributes or statements over their values are revealed, and unlikability, preventing different presentations of the same credential from being linked together.

The schemes are built to satisfy two primary high-level security properties: unforgeability, ensuring an adversary cannot falsely claim possession of attributes, and privacy, guaranteeing no extra information is leaked beyond what the user intentionally discloses.



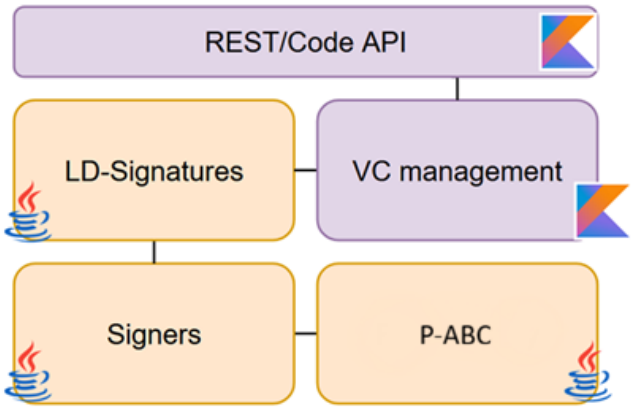
Extensions to these core components include revocation mechanisms for invalidating credentials, inspection for trusted identification in cases of abuse, range proofs for verifying numeric attributes against predicates without revealing exact values, and pseudonyms for controlled likability.

Integration within the LICORICE Ecosystem

The P-ABC security module developed in LICORICE provides the functionality of p-ABCs integrated into key specifications and flows of the EUDIW ecosystem, enabling the improvement of the privacy characteristics of a wallet instance over the baseline instantiation.

This approach is realised through a crypto core backend designed to mediate all interactions with the underlying zero-knowledge mechanisms. Its purpose is to make p-ABC functionality consistently accessible to issuers, holders, and verifiers, ensuring that selective disclosure, unlikability, and predicate-based proofs can be applied within standard verifiable credential flows.

Particularly, the pABC component provides the functionality required to generate, present and verify Verifiable Credentials using the p-ABC scheme. The functionality, following the overall LICORICE approach, is provided “as-a-service” in a REST-based remote security module for Issuers, Wallet holders and Verifiers, although it could also be integrated locally in each wallet instance if appropriate secure hardware/software stack (e.g. Trusted Execution Environments) are present.



Thus, the p-ABC cryptographic engine is abstracted by introducing a dedicated management layer that adapts these capabilities to standard Verifiable Credentials. This layer bridges the gap between low-level cryptographic operations and high-level identity workflows, ensuring that issuance, storage, and presentation processes can leverage p-ABC privacy features while remaining interoperable with existing SSI components. This is achieved through the definition of Signature Suites for the original signature and for the zero-knowledge proof over a signature.

Privacy-preserving Cyber-Threat Intelligence (ppCTI)

Addressing Privacy Concerns in CTI Sharing

The privacy preserving Cyber-Threat Intelligence (ppCTI) component fits into LICORICE as a privacy-respecting data sharing tool focused on CTI Sharing capabilities. It provides policy-based application of privacy preserving techniques to obfuscate sensitive CTI attributes prior to sharing with external actors.

The goal is to bridge the gap between effective sharing of key cybersecurity resources such as threat indicators and indicators of compromise, and the need to protect sensitive operational information that could expose vulnerabilities if shared without appropriate safeguards.

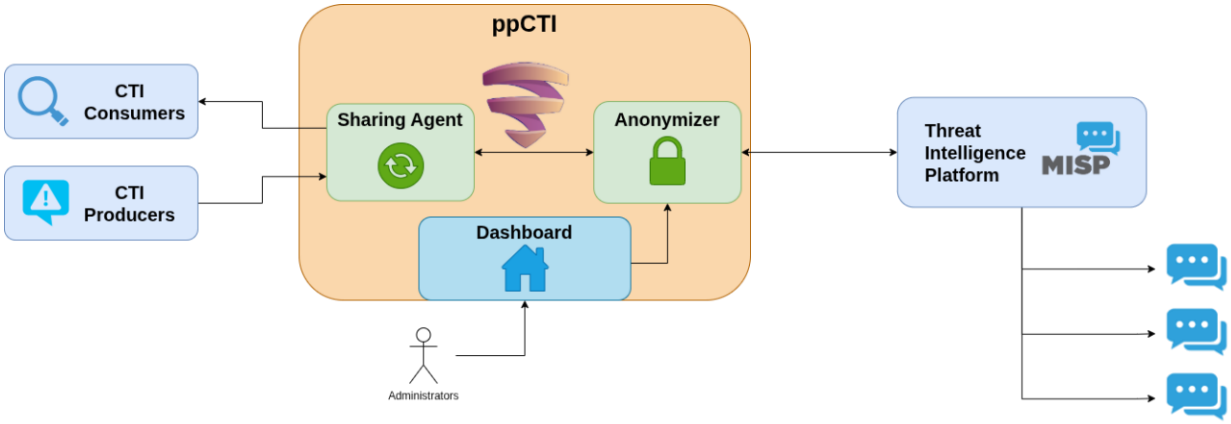
The ppCTI component acts as a middleware between CTI sources and consumers, preprocessing data in standard formats like STIX or MISP data model, using fine-grained privacy policies, generating obfuscated events suitable for CTI Sharing through the threat intelligence platform, and likewise collecting incoming events for processing and forwarding to LICORICE CTI consumers. This functionality relies on several services

Sharing Agent: The primary entry point to the ppCTI service for both CTI producers and consumers, this subcomponent exposes APIs to share CTI payloads and to receive periodic updates on the latest received CTI.

Anonymizer: This subcomponent handles manipulation of CTI data in order to conform to the established privacy policy.

Dashboard: Acts as a frontend for administrators to configure the behaviour of the ppCTI component. Within the dashboard there are tools to generate and modify privacy policies, as well as to establish the active policy and a list of all previously created policies.

MISP: Our component utilizes MISP as the Threat Intelligence Platform of choice for CTI Sharing purposes, although any other source/destination can be plugged in as part of the processing pipeline.



Addressing Privacy Concerns in CTI Sharing

The ppCTI component has been designed with the objective of supporting the information-sharing goals highlighted in several European cybersecurity initiatives, including the NIS2 Directive and the Cyber-Resilience Act.

These initiatives emphasise that effective detection and mitigation of cyber-threats depend on the ability of organisations to exchange information about incidents and vulnerabilities. However, sharing such information can introduce risks if sensitive operational or personal data is exposed, which has led to organisations' reluctance to participate in such systems in the past and concerns about the new landscape.

The tool provides a platform *for sharing of CTI and threat data across domains and with the whole ecosystem,* including CSIRTs. By integrating privacy-enhancing technologies such as anonymization and pseudonymization directly into the sharing pipeline, ppCTI aims to address these concerns, while keeping data usefulness.

The platform therefore enables the exchange of cyber-threat intelligence across domains while ensuring that privacy and confidentiality requirements are respected. This approach allows organisations to contribute to a stronger collective cybersecurity posture without increasing their exposure to additional risks.

Conclusion

The LICORICE framework demonstrates how digital identity technologies and privacy-enhancing cryptographic tools can be combined to support secure digital ecosystems.

Through components such as privacy-preserving attribute-based credentials and privacy-preserving cyber-threat intelligence sharing, UMU explores in the project practical ways of improving privacy, interoperability and trust within emerging European digital infrastructures.

As the project continues to evolve, these tools will contribute to building a more secure and privacy-respecting environment for identity management, data sharing and cybersecurity collaboration across Europe