LICORICE

reLIable and sCalable tOols foR self-sovereIgn identity and data protection framEwork

Funded by the European Union

The Role of Crypto-Biometrics in the LICORICE Project

EAB Research Projects Conference
September 2026

Rosario Arjona (marjona@us.es)
Associate Professor, University of Seville

Contents

1. LICORICE Partners
2. LICORICE Project
3. LICORICE Toolsets for Self-Sovereign Identity
4. LICORICE Crypto-Biometrics as a Service (CBaaS) Approach
5. CBaaS in LICORICE Pilots
6. Demo based on the EUDI Wallet Reference Implementation

LICORICE Partners

13 partners from 8 EU Member States:

1. TRIALOG
2. ATOS*
3. AIT
4. TU GRAZ
5. UNIVERSIDAD DE MURCIA
6. INTERNATIONAL DATA SPACES ASSOCIATION (IDSA)
7. UNIVERSIDAD DE SEVILLA
8. UvA
9. FBK
10. NEC LABORATORIES EUROPE
11. FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS (FORTH)
12. UBITECH
13. BULL*



* ATOS R&D team for SSI transferred to Advanced Computing Spain S.L. under the Bull brand from 1 February 2026

LICORICE Project

- LICORICE is a **European Innovation Action** aimed at reinforcing **digital trust**, **data sovereignty**, and **secure identity management** in the context of digital transformation. It started in October 2024.
- It delivers advanced **self-sovereign identity** and **privacy-preserving** toolsets for **user-centric identity** management and **verifiable federated data** sharing and computing.
- Fully aligned with the EU Digital Identity and Data Strategy and contributing to the Digital Decade goals, LICORICE supports:
  - The **EUDI Wallet ecosystem**,
  - The development of **secure EU data spaces**,
  - And the fight **against cyber threats and identity-related crimes**.
- Its results will be validated in **two operational pilots**:
  - **Cyber Threat Intelligence AI-based assistance and sharing.**
  - **eHealth and biomedical research services.**
- The project focuses on **interoperability, standardization, scalability, usability**, and **open-source** adoption.

LICORICE Toolsets for Self-Sovereign Identity

- **Decentralised Identity Management** with issuer and verifier of selective-disclosure credentials:
  - **Privacy-Preserving Identifier Derivation (PPID)**: with unlinkable and auditable pseudonym credentials.
  - **Privacy-Preserving Attribute-Based Credentials (P-ABC)**: with ZKP-based credentials.
  - **Attribute-Based Direct Anonymous Attestation (DAA-A)**: with hardware roots of trust.

- **High Level of Assurance** with:
  - **Device binding**: credentials should be univocally associated with their true wallet.
  - **User (holder) binding**: a wallet should be univocally associated with its true user.

Crypto-Biometrics as a Service (CBaaS): offering two-factor authentication (biometrics with possession/knowledge), verifiability (external evidence), protection (irreversibility, unlinkability and revocability), long-term security (post-quantum) and remote hardware-based security (cloud trusted execution environment)

LICORICE Crypto-Biometrics as a Service (CBaaS) Approach

- **Two authentication factors**: Facial biometrics and user-device secret or PIN/password ((EU) 2015/1502)
- Biometric data protected at communications, processing and rest (GDPR)

End-to-end encryption with ephemeral keys

Cloud-based Trusted Execution Environment (TEE) for crypto-biometrics techniques offering:

- Hardware-based security (eIDAS, EUDI ARF)
- Verifiability (external evidences by signing a challenge after authentication)
- Scalability and usability (non-device centric)
- Open to developers (European digital sovereignty)

Biometric template protection offering:

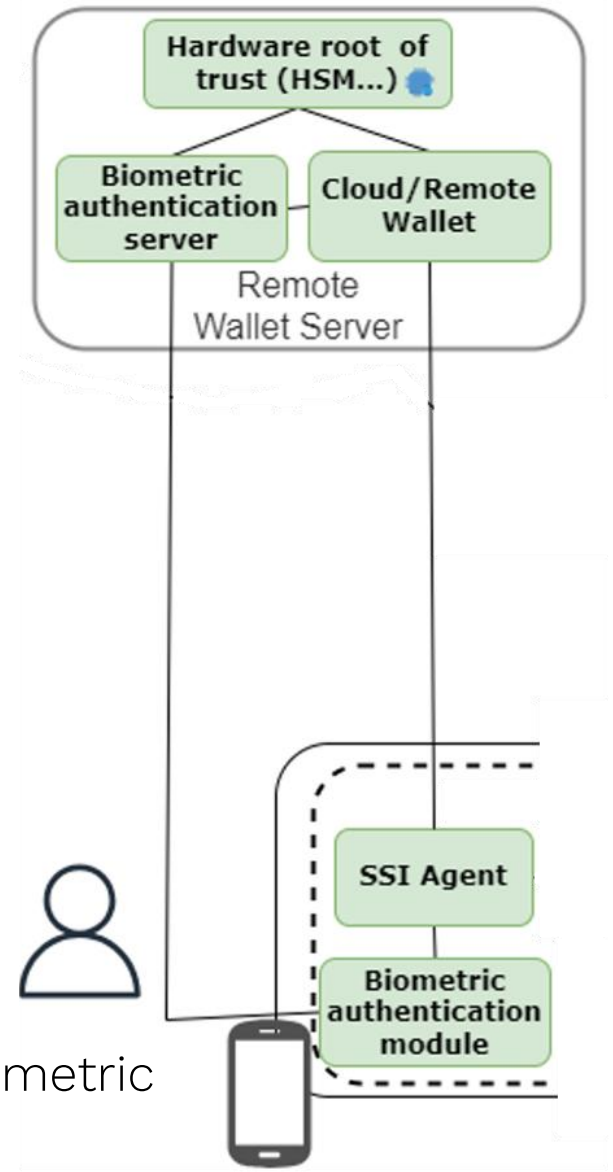
- Irreversibility, unlinkability and revocability (ISO/IES 24745)
- Preserving recognition accuracy of unprotected system
- Post-quantum security, with efficient computational and communication/storage costs

LICORICE Crypto-Biometrics as a Service (CBaaS) Approach

2. **Feature extraction** (combining factors), **template protection** (fuzzy extractor), **matching** (recovering a secret key) and **challenge signature** (with the secret key recovered) are performed in the TEE of the Hardware root of trust.

   Storage of the protected template (during enrollment) and **challenge generation** (during authentication) are performed in the Biometric authentication server.

3. After authentication, an **access token** (following Open ID Connect) is generated to issue and verify credentials through the SSI Agent and the Cloud/Remote Wallet.



1. **Acquisition** is performed in the Biometric authentication module.

LICORICE Tools in Cyber Threat Intelligence (CTI) Pilot

CTI pilot objective: Validate LICORICE toolsets and strengthen cybersecurity operations using AI while upholding data privacy.

Solution:

- **AI-Driven Assistant**: Processes Cyber Threat Intelligence (CTI) data in compliance with data protection regulations.
- **Privacy Integration**: Utilizes Privacy-Enhancing Technologies (PETs) to anonymize sensitive data.

Outcome:

- **Privacy-respecting** security environment.
- **Secure Collaboration**: Enables safe data sharing between organizations.

CBaaS is required for the authentication of their users (experts and external users) previously to use the wallet

Challenges

- **Automated Privacy-Preserving Anonymization.**
- **Compliance with Data Protection Regulations.**
- **Integration of Privacy-Enhancing Technologies (PETs)** without compromising confidentiality.
- **Scalability and Performance optimization** handle high volumes of CTI data in real-time.
- **Secure Collaboration Framework**: secure information-sharing protocols.

LICORICE Tools in eHealth Pilots

ehealth pilot objective: Validate LICORICE toolsets for user-centric authentication and secure health data control.

Solution:

- **Privacy-Preserving AI** for Chronic Disease Management and early detection.
- **Federated Learning (FL)** for decentralized model training across diverse sources (hospital devices, wearables).
- **Self-Sovereign Identity (SSI)** to empower user control over health data.
- **Privacy-Preserving Technologies** like secure multi-party computation to ensure confidentiality.

Outcome :

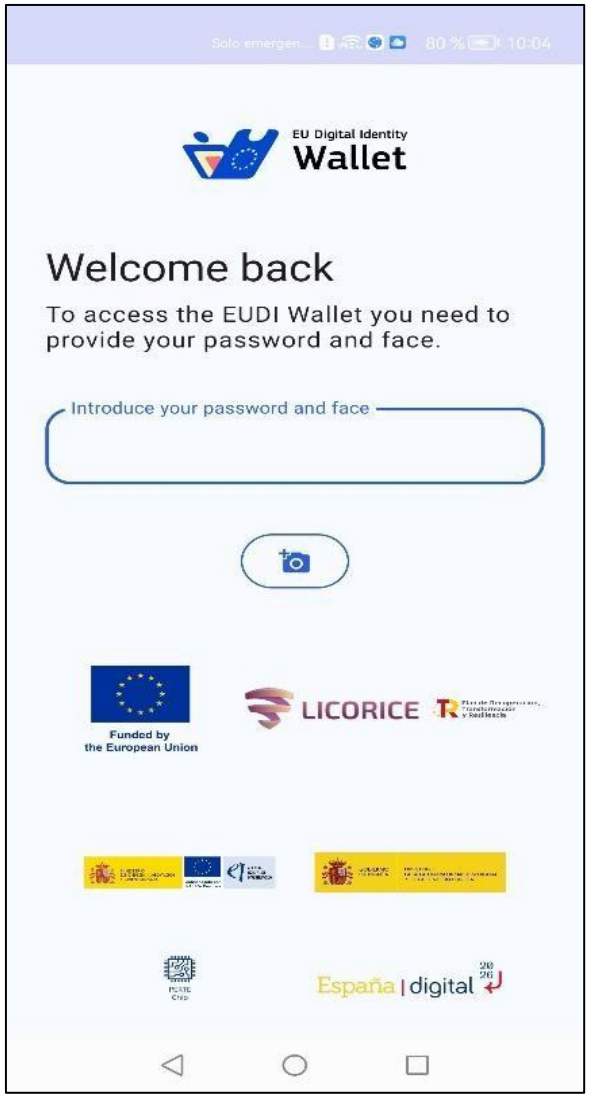
- **Support secure data sharing for research and public health**, aligned with the European Health Data Space.
- **Secure medical data exchange**, **remote monitoring**, and **privacy-aware telemedicine**.

CBaaS is required for the authentication of their users (patients and doctors) previously to use the wallet

Challenges:

- **Data and privacy regulations** (e.g., GDPR or AI Act) limit data sharing and AI-driven healthcare innovation.
- **Enhance Patient Trust and Data Protection.**
- **Mitigate Risk and Protect Reputation.**
- **Expand Telemedicine Opportunities.**
- **Ensure Long-Term Sustainability**, safeguards against evolving cyber threats.

Demo based on the EUDI Wallet Reference Implementation



- We have modified the **reference implementation** of the EUDI Wallet to include face recognition (in addition to PIN/password).
- Active liveness detection (with user interaction) for face acquisition and avoiding facial presentation attacks.
- A **smartphone** can act as user device.
- A **cloud hardware enclave** can act as remote trusted execution environment.

LICORICE

- Website

- LinkedIn

Thank you for your attention



LICORICE

reLIable and sCalable tOols foR self-sovereIgn identity and data protection framEwork

Rosario Arjona (marjona@us.es)

LICORICE Project with Grant Agreement No. 101168311 under EU Horizon Europe