Project Overview



PRIVIDEMA

Erkay Savaş
Sabanci University

PRIVIDEMA Consortium

17/09/2026

Agenda

- PRIVIDEMA overview
- Objectives, consortium & progress
- Expected results, work plan & timeline
- Use Case 1 – Privacy-Preserving Digital Identity Wallet
- Use Case 2 – Privacy-Preserving Cyber Threat Intelligence
- Technology building blocks: FHE library, hardware acceleration, differential privacy
- Main challenges, risks & roadmap
- Discussion

About PRIVIDEMA

- PRIvacy-Preserving IDEntity MAnagement for Digital Wallet and Secure Processing of Cyber Threat Intelligence Data

Keyfacts

Reference

Reference Number:
101167964
Programme type:
HORIZON-IA
Programme acronym:
HORIZON-CL3-2023-CS-01-02

Duration

Project Start: 01.11.2024



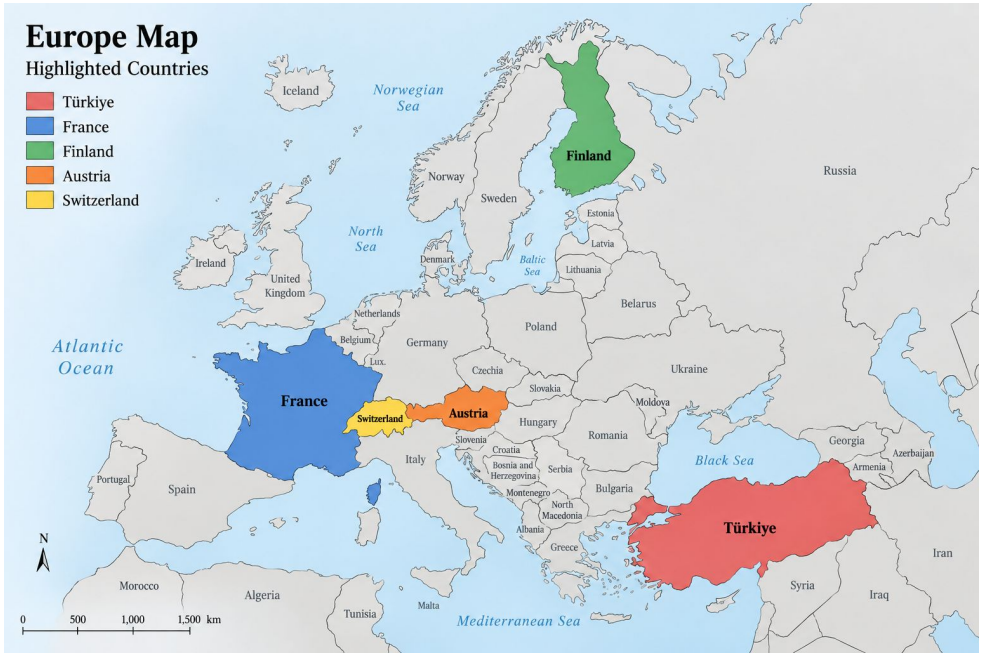
Cost and Funding

Costs:
€ 5.311.339,36
Funding:
€ 3.133.964,75

[European Digital Identity Regulation](https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation)
https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation

Consortium & Partners

- **Project team:**
  - Technikon Forschungs-Und Planungsgesellschaft Mbh (TEC) (Coordinator)
  - Tune Insight (Technical Lead)
  - Commissariat à l'Énergie Atomique et aux Énergies Alternatives (CEA)
  - Sabanci University (SU)
  - Thales Dis France Sas (THALES / TCS)
  - Turun yliopisto (UTU)
  - Idakto (iDAKTO)





PRIVIDEMA: Use Cases

- **Privacy-Preserving Identity Management**: Develop advanced tools for digital identity wallets that enable individuals to securely manage and share their personal information without compromising their privacy.
  - **Use case 1**: *Identity management for enhanced privacy preserving Digital Wallet*
- **Cyber Threat Intelligence Data Processing**: Create and demonstrate a privacy-preserving cyber threat data processing system to enhance cybersecurity across borders while protecting sensitive information from exposure.
  - **Use case 2**: *Secure data sharing and analytics for Cyber Threat Intelligence.*

Our Objectives - Progress So Far

1

Grow the community

Build a network of European cybersecurity experts through open tools, events, and shared knowledge.

✓ Presented at EAB & EICC, and contributor to ISO standards

2

Make encryption faster

Accelerate encrypted computation, in software and hardware, so privacy tech becomes practical to use

✓ Prividema-lib v0.1 released, open source

3

Protect digital identity

Give people real control over their identity, matching faces without ever exposing the raw biometric data.

✓ Wallet prototype built

Our Objectives - Progress So Far

4

Share threat data safely

Let organizations collaborate on cybersecurity threats and vulnerabilities without exposing their own systems or software to one another.

✓ Prototype in place

5

Bring smaller companies on board

Help SMEs access, adopt, and benefit from cutting-edge privacy-preserving and identity technologies.

✓ 2 SME partners piloting

Expected Results & Status

1 Open-source FHE library

A software toolkit for computing directly on encrypted data; the core engine behind every use case in the project.

✓ v0.1 released

2 Hardware-accelerated toolkit

The same library, accelerated using GPUs, to make encrypted computation fast enough for real-world use.

✓ CUDA library released

3 Privacy-safe machine learning library

Tools to analyze data and spot patterns while mathematically guaranteeing individuals' privacy.

◑ Core algorithm built

Expected Results & Status

4

Digital identity wallet demo

A working prototype that lets people prove who they are without ever exposing their raw biometric data.

◑ Prototype running

5

Secure threat-sharing tool

A system that lets organizations share cybersecurity alerts and vulnerability data without revealing their own weak spots to one another.

◑ Baseline prototype

How the Project is Organized

1

Foundations

Setting up the project and defining *requirements for both use cases*.

WP1 – WP3

2

Core Technology

Building the ***encryption library***, ***hardware acceleration***, and ***privacy-preserving ML*** *tools*.

WP4 – WP8

3

Validation

Testing everything in ***two real-world demonstrators***.

WP9

4

Sharing & Impact

Open-source **releases**, *publications*, and *outreach to standards bodies and SMEs*.

WP10 – WP11

11 work packages in total — grouped here into 4 phases for clarity

Project Timeline

▲ We are here — M18



M1 – Start

M36 – Project ends

✓ Mostly complete

Phase 1 (M1–M18)

Requirements defined, architecture designed, and first open-source libraries and prototypes delivered.

◑ Upcoming

Phase 2 (M18–M36)

Integrating privacy technologies into both use cases and delivering the final, validated demonstrators.

Use Case 1: Proving Who You Are, Privately

⚠️ The problem

Face recognition today means your data either stays locked on your phone, or gets sent somewhere you cannot fully verify. And unlike a password, a stolen face can never be changed.

✓ Our approach

We use Fully Homomorphic Encryption (the CKKS scheme) to *encrypt facial embeddings on-device* before anything is sent. The match is computed as a *cosine similarity directly on the encrypted data*. Biometric data is never exposed, including to us.

Embeddings are extracted with **InsightFace**, an established open-source model. We perform *1:1 verification* by matching face data only against an enrolled template. *Not identification*

Use Case 1: How It Works

1

Scan

EU Digital Identity Wallet is run and an on-device InsightFace model extracts facial embedding

2

Encrypt

Device instantly encrypts the scan, always keeping the original data unreadable

3

Match

Homomorphic cosine similarity is computed directly on the ciphertext (WSCA)

4

Unlock

Only secure hardware (WSCD) decrypts the similarity score and unlocks

In progress

Where we are today

The wallet app and secure backend are up and running, supporting user onboarding, credential issuance (OID4VCI), and credential presentation (OID4VP). Biometric matching is currently server-side; a proof of concept *combining InsightFace with CKKS-based FHE* has already been demonstrated, and the overall architecture has been fully specified. The next milestone focuses on integrating FHE-based biometric matching, enabling the encrypted face-matching step (Step 3) to operate in a privacy-preserving manner as designed in the project architecture.

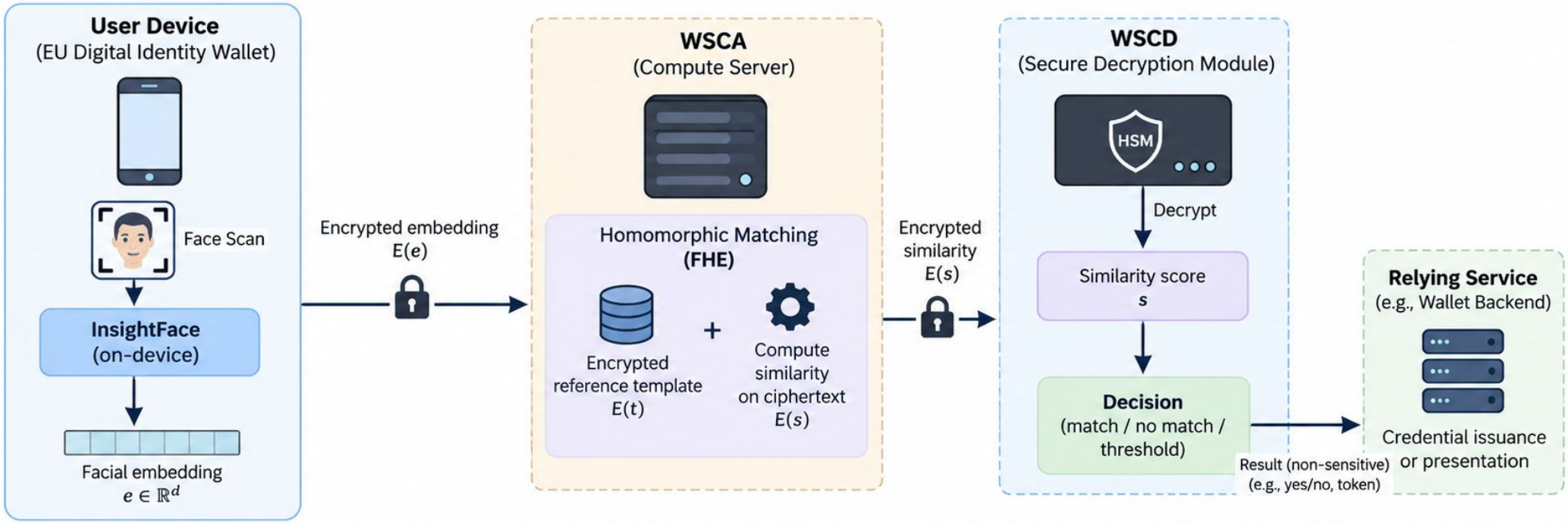
Use Case 1: How It Works

1 Scan
On-device InsightFace extracts facial embedding

2 Encrypt
Device encrypts the embedding and keeps raw data unreadable

3 Match
WSCA computes homomorphic cosine similarity directly on the ciphertext (FHE)

4 Unlock
Only secure hardware (WSCD) decrypts the similarity score and releases the result



Key Properties

- Raw biometric data never leaves the device
- Matching is performed on encrypted data using FHE at WSCA
- Only WSCD (HSM) decrypts the similarity score
- The relying service receives only a non-sensitive result

Abbreviations

- **WSCA**: Wallet Service for Computation and Analytics (server, performs homomorphic computation)
- **WSCD**: Wallet Service for Cryptographic Devices (secure hardware, e.g., HSM)
- **FHE**: Fully Homomorphic Encryption
- **E(·)**: Encrypted data

prividema.eu

Use Case 2: Spotting Cyber Threats Safely

⚠️ The problem

To check for known cybersecurity vulnerabilities, one would normally need to reveal exactly which software is being used. However, this information is itself sensitive, as an attacker could exploit knowledge of the software stack to identify potential attack vectors.

✓ Our approach

PRIVIDEMA lets an organization check for vulnerabilities relevant to it without ever revealing its software inventory, not even to the service doing the checking.

Use Case 2: How It Works

1 — Collect
Gather threat data from public feeds; currently ~350,000 known vulnerabilities

2 — Prepare
Clean and organize the data so it is ready to query

3 — Analyze
Check for relevant threats using encrypted, privacy-preserving queries

4 — Warn
Send an early warning only to those affected

◑ In progress

Where we are today

A working server and client already enable organizations to query an up-to-date CVE database using CycloneDX SBOMs. The next step is adding user accounts and integrating OnionPIR and MHE to ensure queries and aggregate statistics remain privacy-preserving across Scenarios 2–4.

Use Case 2 – The Four Scenarios

1 Single Vulnerability Check

A user checks whether their own software has known vulnerabilities, without revealing their software list to the provider.

Private Information Retrieval (PIR)

Assumes an honest-but-curious provider

2 Ongoing Monitoring

Extends Scenario 1 with persistent user accounts, enabling continuous checks instead of one-off queries.

PIR + user accounts

Assumes an honest-but-curious provider

3 Secure Aggregate Statistics

Multiple users combine data to compute shared statistics, without exposing any individual's answer.

Multiparty HE (MHE) + Differential Privacy

Assumes an honest-but-curious provider

4 Anomaly Detection

Users privately pool their interaction history to detect if the provider itself deviates from protocol.

Federated Learning + Differential Privacy

Protects against a compromised provider

Building Block: A Toolkit for Computing on Encrypted Data

🎯 The Goal

What It Is

A unified low-level foundation for FHE, supporting BFV, CKKS and TFHE/CGGI interoperability with scheme switching, while reducing the computational cost of privacy-enhancing technologies

✓ Delivered

What We Have Built

The first open-source version of this toolkit (prividema-lib v0.1) is already released and freely available, providing the common engine powering both use cases.

- *Open source:* github.com/Prividema/prividema-fhe

WP4/5 — Library for Efficient FHE · Led by Tune Insight · Months 1–36

Building Block: Making Encrypted Computing Fast

🎯 The Goal

What It Is

Computing on encrypted data is naturally much slower than working with normal data. This building block provides GPU/FPGA-accelerated middleware for FHE primitives, with a unified interface across FHE frameworks, significantly speeding up encrypted computation.

✓ Delivered

What We Have Built

A GPU-accelerated port of libSpqlios enables CUDA-based FFT/NTT acceleration, with reported speedups of 16× to 40×. The work also establishes unified interfaces, memory and runtime management, with around 15 functions identified for further GPU acceleration:
https://github.com/Alisah-Ozcan/HEonGPU

WP6/7 — Hardware Acceleration for FHE · Led by SU · Months 1–36

prividema.eu

Building Block: Protecting People, Not Just Data

🎯 The Goal

What It Is

Even anonymized statistics can accidentally reveal information about individuals. This building block provides mathematically guaranteed privacy for data sharing, statistics, and ML, applied to secure aggregate statistics and anomaly detection.

◑ In progress

What We Have Built

A practitioner-oriented differential privacy survey, a novel InexactLMBM optimization algorithm, and a baseline output-DP clustering prototype are already available, with benchmarking underway for integration into the anomaly detection use case. They feed two of Use Case 2's four scenarios: protecting secure **aggregate statistics** (**Scenario 3**), and **anomaly detection** (**Scenario 4**), spotting a misbehaving service provider without exposing anyone's data.

WP8 — Differential Privacy · Led by UTU · Months 3–34

Challenges We are Tackling

1

Winning Trust

New privacy technology can feel unfamiliar. We align with EU regulations such as eIDAS and proving ourselves through real pilots.

2

Encryption Maturity

Fully homomorphic encryption (FHE) is still a young field. We are contributing to ISO standards and open-source tools to help it mature.

3

Scaling Up

Encrypted computation must run fast enough for real use. We're improving this through both smarter software and hardware acceleration.

4

Real-World Data

Testing needs real data, not just samples. We are partnering directly with SMEs and other organizations to access it.

Roadmap - What Comes Next

1

Use Case 1

Switch on encrypted face-matching and run the final demo.

2

Use Case 2

Add the remaining privacy layers and expand to more scenarios.

3

Encryption Library

Finish supporting all encryption schemes and stabilize the toolkit.

4

Hardware Acceleration

Accelerate more of the toolkit using GPUs.

5

Privacy Guarantees

Extend differential privacy into full anomaly detection.

6

Sharing Our Work

Newsletter, conferences, and continued standards contributions.

PRIVIDEMA Grant Agreement No. 101167964

If you need further information, please contact the coordinator:

TECHNIKON Forschungs- und Planungsgesellschaft mbH

Burgplatz 3a, 9500 Villach, AUSTRIA

Tel: +43 4242 233 55 Fax: +43 4242 233 55 77
E-Mail: coordination@prividema.eu

Funded by the European Union

Funded by the European Union under grant agreement no. 101167964. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.