A scalable and practical privacy-preserving framework

4 Dec 2024

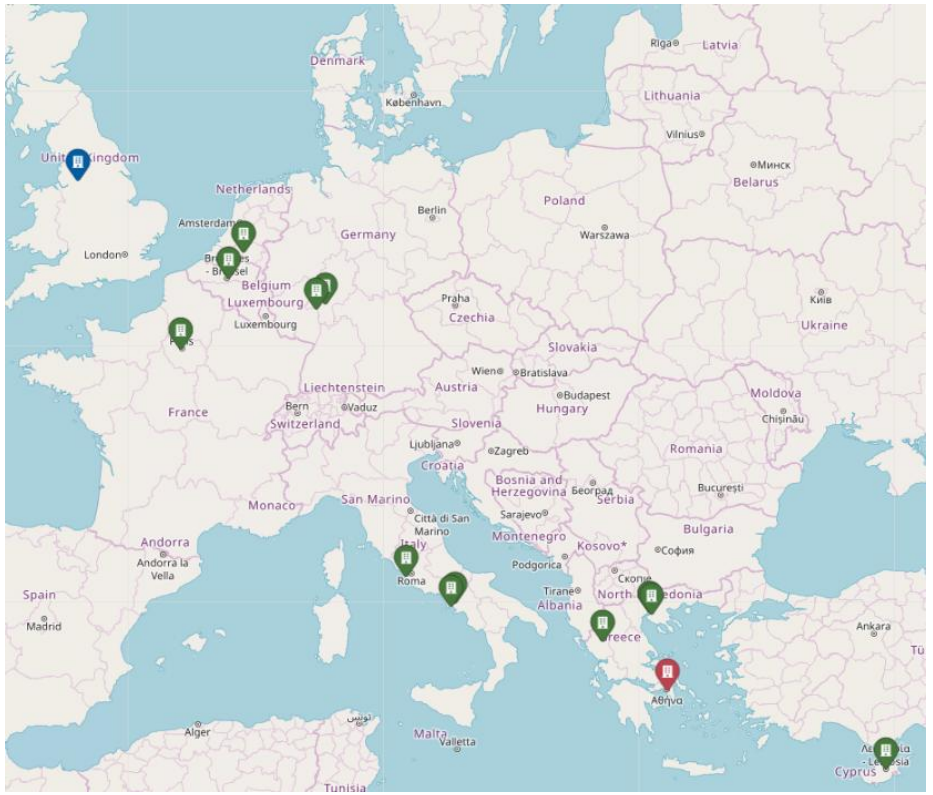
encrypt

Funded by the Horizon Europe Framework Programme of the European Union under Grant Agreement nº 101070670.

ENCRYPT Facts and Figures

- **Project Short Name:** ENCRYPT
- **Grand Agreement ID**: 101070670
- **HORIZON-CL3-2021-CS-01-04** - Scalable privacy-preserving technologies for cross-border federated computation in EU involving personal data
- **Funding Scheme:** Research and Innovation Action (RIA)
- **Total Funding:** 4,392,540 €
- **Duration:** 36 Months (July 2022 – June 2025)
- **Consortium:** 14 partners, 8 countries
  - ✓ 1 start-up (TRUSTUP)
  - ✓ 3 x SMEs (EXUS, 8BELLS, DBC)
  - ✓ 2 x Enterprises (ENG, EPIBANK)
  - ✓ 8 Research Institutes (CERTH, AUTH, UNIMAN, TIU, CEA, UNINA, GUF, UMC-Mainz)

- **Coordinator:** EXUS SOFTWARE MONOPROSOPI ETAIRIA PERIORISMENIS EVTHINIS (EXUS) - Greece



ENCRYPT Consortium

Consortium Partners	Short Name	Country
1. EXUS SOFTWARE MONOPROSOPI ETAIRIA PERIORISMENIS EVTHINIS	EXUS	Greece
2. ENGINEERING - INGEGNERIA INFORMATICA SPA	ENG	Italy
3. ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	CERTH	Greece
4. EIGHT BELLS LTD	8BELLS	Cyprus
5. COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES	CEA	France
6. TRUST UP SRL	TRUSTUP	Italy
7. ARISTOTELIO PANEPISTIMIO THESSALONIKIS	AUTH	Greece
8. DBC EUROPE	DBC	Belgium
9. TILBURG UNIVERSITY- UNIVERSITEIT VAN TILBURG	TiU	Netherlands
10. UNIVERSITA DEGLI STUDI DI NAPOLI FEDERICO II	UNINA	Italy
11. SYNETAIRISTIKI TRAPEZA IPEIROU SYN.P.E.	EPIBANK	Greece
12. JOHANN WOLFGANG GOETHE-UNIVERSITAET FRANKFURT AM MAIN	GUF	Germany
13. UNIVERSITAETSMEDIZIN DER JOHANNES GUTENBERG-UNIVERSITAET MAINZ	UMC-Mainz	Germany
14. THE UNIVERSITY OF MANCHESTER	UNIMAN	United Kingdom

1 x Start up

8 x Research Institutes & Universities

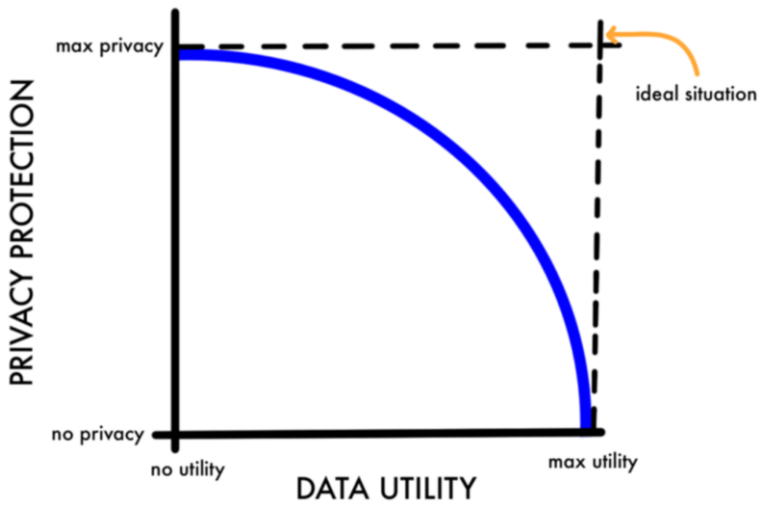
3 x SMEs

2 x Enterprises

encrypt

Challenges and ENCRYPT Vision

- Vast amounts of data in new fields related to Industry, Health and research
  - ✓ Sensitive data are present
  - ✓ researchers and service providers working with personal data need process them in a privacy-preserving way,
  - ✓ Existing PP technologies (HE, MPC, TEE or DP) suitable for small-scale level
  - ✓ Trade-offs between max privacy and efficiency



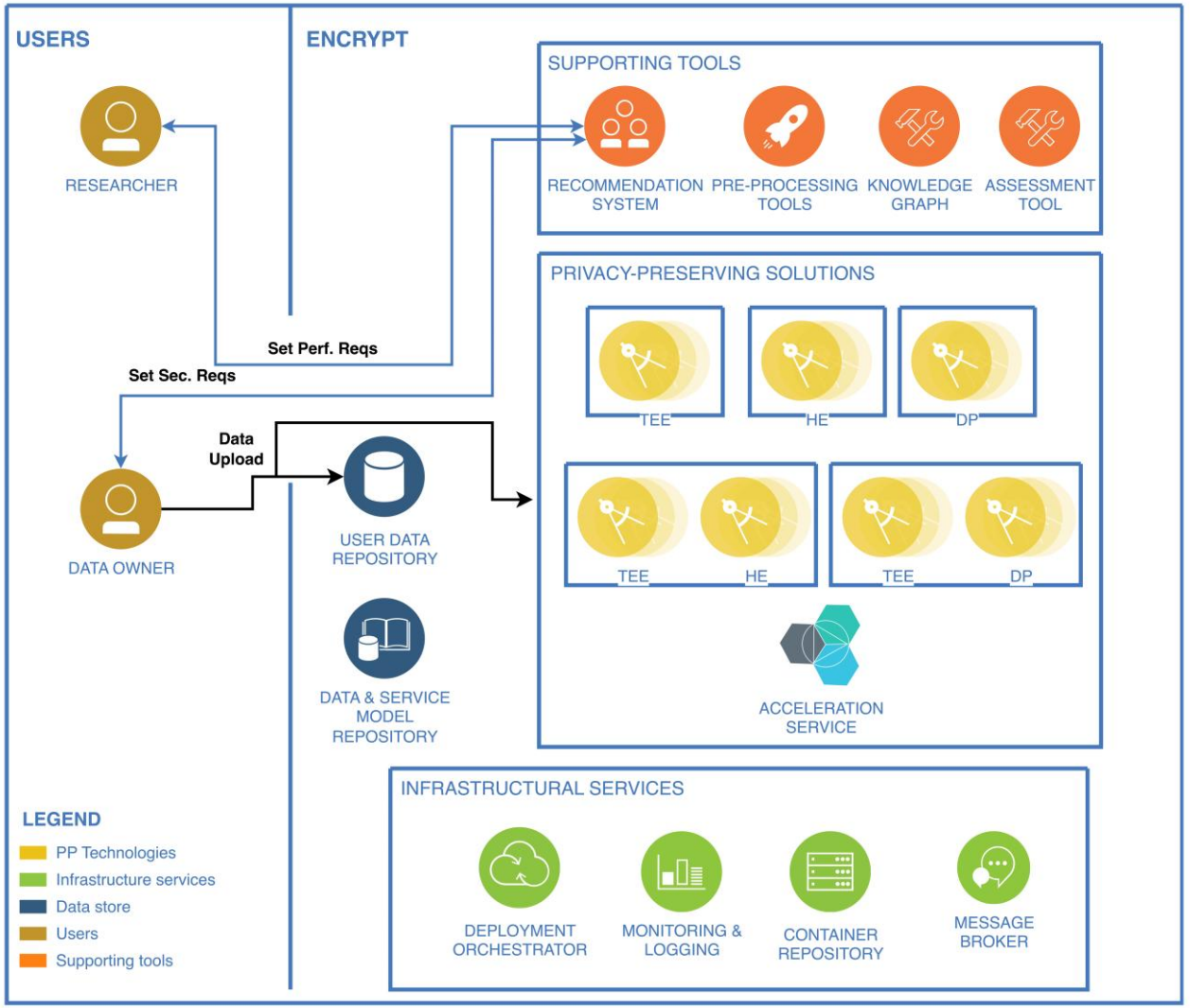
- ENCRYPT will deliver a scalable, practical, adaptable privacy-preserving framework facilitating the GDPR-compliant processing of such data stored in federated cross-border data spaces by exploiting
  - State-of-art PP computations technologies
  - State-of-art supportive technologies, including a recommendations system and a methodological framework to assess the level of privacy and impact to the organization
  - Validation in internal and external Use cases in real-world systems

encrypt

ENCRYPT Key Technologies and results

- **Privacy –Preserving Computation Solutions**
  - ✓ Fully Homomorphic Encryption (FHE)
  - ✓ Trusted Execution Environment (TEE)
  - ✓ Differential Privacy (DP)
  - ✓ Combined HE+TEE, HE+DP
  - ✓ Acceleration Service

- **Privacy –Supporting Tools**
  - ✓ Advanced data-preprocessing
  - ✓ Knowledge Graphs
  - ✓ Methodological Framework for privacy risk assessment
  - ✓ AI–powered Recommendation system
  - ✓ Front-end and back-end services



encrypt

ENCRYPT High Level Objectives

1. To **improve the applicability** and **performance** of PP technologies towards GDPR compliant, cross-border federated processing of personal and other sensitive data, developing a **toolset of scalable, practical, and reliable PP technologies**

2. To **improve the user-friendliness** of PP technologies facilitating the identification, understanding, selection, and adoption of PP technologies **by all actors**

3. To foster, and inherently support **interoperability for PP processing of similar data** types across organisations, and across sectors.

4. To promote GDPR-compliant common **European Data Spaces** and facilitate the **exchange of CTI**, liaising with relevant initiatives and projects with a focus on standardization

5. To ensure the **applicability** of the developed solutions, **co-designing them with end-users**, and validating them in **realistic use cases** including federated data infrastructures with personal data

6. To **strengthen the ecosystem** of open-source developers and researchers of privacy-preserving solutions disseminating, and exploiting open-source project results, as well as upskilling researchers.

ENCRYPT Use Cases

- **Health Domain**: supported by the Hospital Clinic of UNINA validating PP technologies on Patients Data in different use case scenarios
- **Cyber Threat Intelligence (CTI) Domain**: supported by CERTH as service provider/data processor, and EXUS, DBC, 8BELLS as data owners and end-users
- **Fintech Domain**: supported by EXUS as the service provider/data processor, EPIBANK as the data steward, and their customers as the data owners
- **External 1:** MIRACUM federated health data infrastructure. Sharing healthcare data from different university hospitals and joint research. GUF and AMC-MAINZ, participating in the MIRACUM consortium, are also participating in ENCRYPT

ENCRYPT Validation Phases

1st phase: In Lab Validations

2nd phase: Encrypt 3 x Use cases

3d phase: External Validation

4rd phase: External Validation

1 **[M17-M27]**

2 **[M24-M32]**

3 **[M24-M32]**

4 **[M24-M32]**

FINTECH

miracum

EU projects

Milestone No	Milestone Name	Due Date
M1	1st version of user requirements, technological specifications, architecture and integration plan	M07
M2	Final version of user requirements, and technological specifications	M12
M3	ENCRYPT components v1	M16
M4	Integrated ENCRYPT prototype v1 and final architecture	M18
M5	Integrated ENCRYPT prototype v2, validated in-lab	M27
M6	Final ENCRYPT prototype and final components versions	M32
M7	Final ENCRYPT prototype validated in use cases	M36

M32: Feb. 2025
M35: May. 2025

encrypt

Contacts

https://encrypt-project.eu/

encrypt-project

@encrypt_project

encrypt