Security Conference

Achieving Data Privacy Without Sacrificing Data Usability: The ENCRYPT Solution

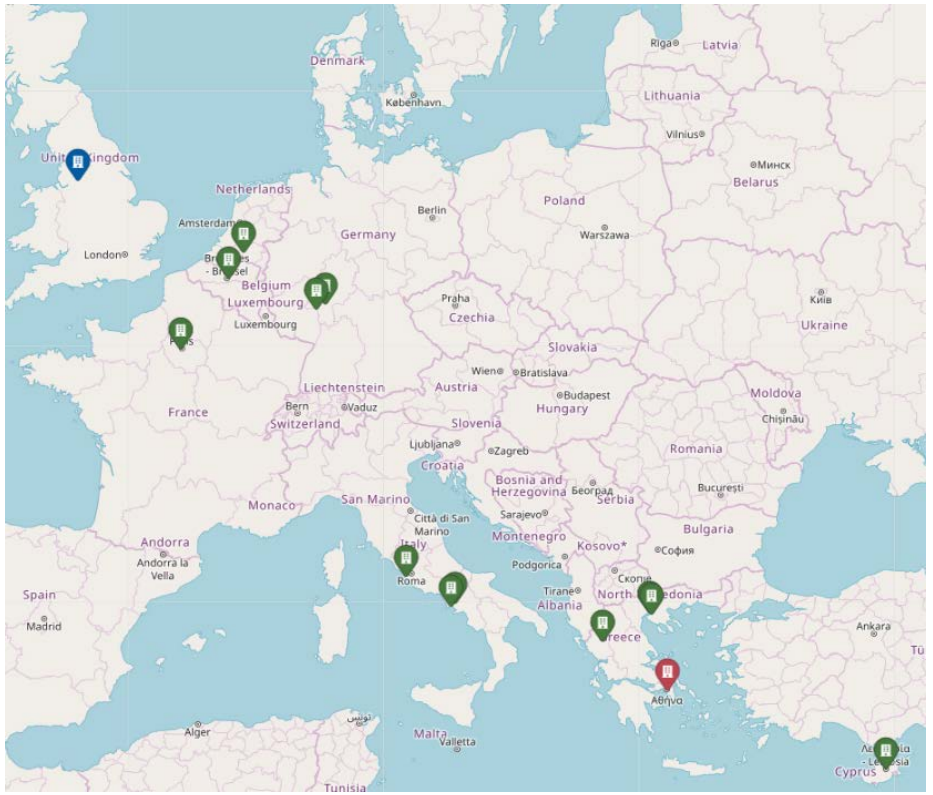
Presented by: Salvatore D'Antonio - University of Naples Parthenope

16/10/2023

ENCRYPT Facts and Figures

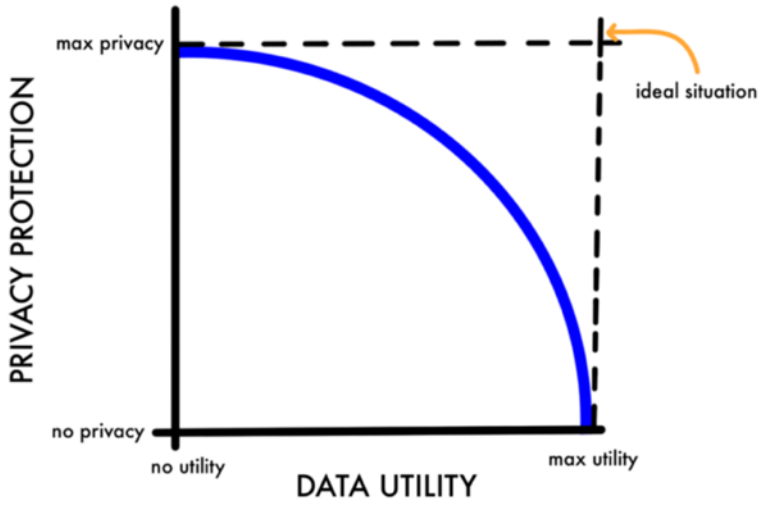
- **Project Short Name:** ENCRYPT (A SCALABLE AND PRACTICAL PRIVACY-PRESERVING FRAMEWORK)
- **Grand Agreement ID**: 101070670
- **HORIZON-CL3-2021-CS-01-04** - Scalable privacy-preserving technologies for cross-border federated computation in EU involving personal data
- **Funding Scheme:** Research 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
- **Website**: https://encrypt-project.eu/



Challenges and ENCRYPT Vision

- Huge amounts of data in new fields related to Industry 4.0, Health, Finance, and Research
  - ✓ Sensitive data are present
  - ✓ Researchers and service providers working with personal data need to process them in a privacy-preserving fashion
  - ✓ State-of the-art Privacy-Preserving technologies, such as Homomorphic Encryption, Differential Privacy, suffer from scalability issues
  - ✓ Trade-off between privacy protection and data efficiency



- ENCRYPT will deliver a scalable, practical, adaptable privacy-preserving framework facilitating the GDPR-compliant processing of data stored in federated cross-border data spaces by exploiting
  - Privacy-preserving computation technologies
  - Supporting technologies, including a recommendations system and a methodological framework to assess the level of privacy risk and impact to the organization
  - Validation in 3 real-world use cases

encrypt

ENCRYPT High Level Objectives

1. To **improve the applicability** and **performance** of Privacy-Preserving technologies towards GDPR compliant, cross-border federated processing of sensitive data, developing an integrated service platform

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

3. To foster, and inherently support **interoperability of** Privacy-Preserving **processing of similar data types** across different organisations, and across different sectors

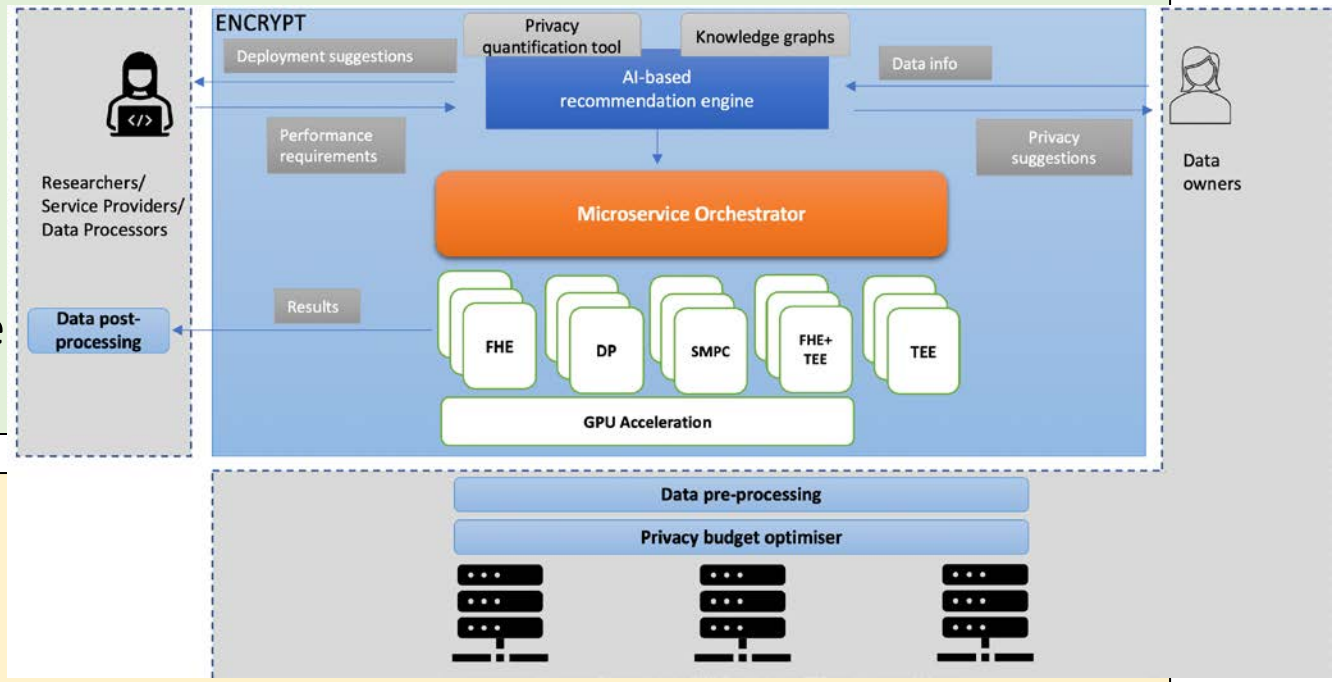
4. To promote GDPR-compliant common **European Data Spaces** and facilitate the **exchange of Cyber Threat Intelligence information**, liaising with relevant initiatives and projects

5. To ensure the **applicability** of the developed solutions, by **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 by disseminating and exploiting open-source project results

ENCRYPT Key Technologies and results

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



- **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

Use cases and cyber risk differentiation

Health domain: Cooperative Oncology	Cybersecurity domain: Cyber Threat Intelligence information sharing	Fintech domain: Data Analytics
Cybersecurity risk: security-induced safety implications	Cybersecurity risk: data breaches and illegal use of CTI information	Cybersecurity risk: data subject reidentification

ENCRYPT Use Case 1 – Medical Domain: Cooperative oncology

Description

- Cancer management is very challenging
- Different medical specialists from various medical disciplines need to cooperate in order to evaluate and analyze the same patient from different perspectives
- In case of radiotherapy treatment, continuous exchange of information between different actors as well as between technological equipment is necessary
- Health care professionals (HCP) need to process and share large amounts of medical data, often in real time and across different hospitals or units
- Data integrity is an essential requirement

ENCRYPT Use Case 2 – Fintech Domain

- **Need 1:** Need of the financial institutions to be sure about the **security and privacy levels** required to **ensure the anonymity of their clients not only internally** to their organization, but also when they **share their data to potential 3rd parties** to perform data analysis and/or to deliver tailored software solutions for the bank's activities.
  - ✓ **Pseudonymization is not enough**.
  - ✓ **Advanced Privacy-Preserving** techniques are required.

- **Need 2:** 3rd party/entity receives these data from the financial institutions and perform AI-driven data analysis in order to deliver tailored software solutions serving the strategies and policies of the bank in specific business portfolios.
  - ✓ **Efficiency and accuracy of the AI models during training** has to be ensured when Privacy-Preserving techniques are applied

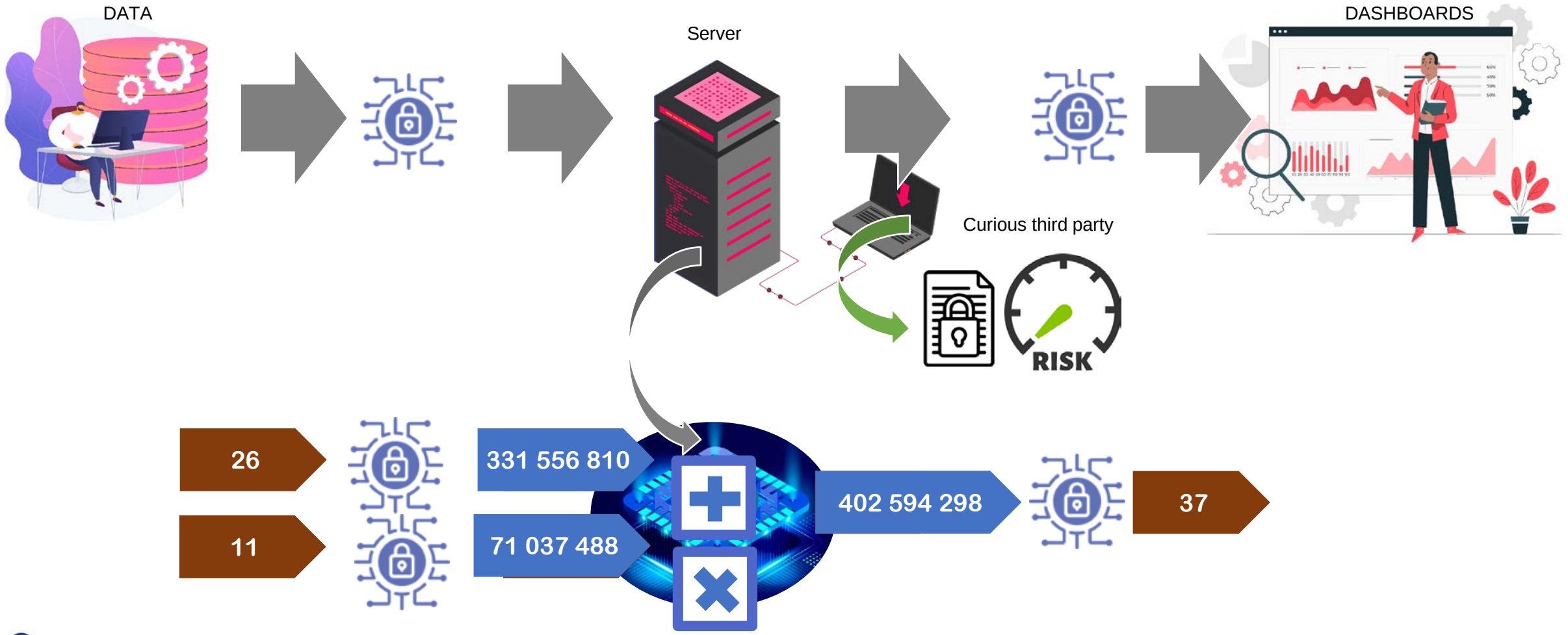
ENCRYPT Use Case 3 – CTI Domain

- Cyber Threat Intelligence (CTI) extracts knowledge about cyberattacks
- Sharing CTI allows for enhancing cyber situational awareness and defense strategies
- Organizations are often hesitant or reluctant to share information due to concerns about sensitive data
- Implementing effective Privacy-Preserving data processing technologies can help data owners to share and exchange CTI information
- Connection with MISP platform and correlation of CTI collected information with Indicators of Compromise of targeted attacks, vulnerability information and even terrorism information stored in the MISP platform using privacy-preserving data analytics

ENCRYPT Privacy-preserving Technologies - TEE

- While standard secure protocols and technologies already exist to protect data in transit, ENCRYPT is focusing on security of data in use and confidential computing
  - ✓ Use of Trusted Execution Environment Technologies (Intel SGX, ARM TrustZone, AMD SEV)
  - ✓ wrt Intel SGX, an extension to CPU ISA allows user-level code to allocate private regions of memory, called Secure Enclaves
  - ✓ The trust model foresees that everything outside the secure enclave is untrusted, including the OS, Hypervisor, and firmware
    - This implies that system call are not allowed in the enclave
  - ✓ Limitation: enclave page cache (EPC) size
- Critical functions of medical image processing and segmentation software are executed inside TEE
  - ✓ Code and data are protected even from cyberattacks launched by high-privilege users

ENCRYPT Privacy-preserving Technologies - FHE



encrypt

FHE strengths

- All data is encrypted - Data remains encrypted at all times.
- No secrets stored on the computation server - The computation server holds no secret information.
- Monolithic computation (small attack surface) - Streamlined computation minimizes vulnerabilities.
- Trusted third party = cryptography (decryption key) - Trust is anchored in cryptography, specifically the decryption key, rather than external third parties.
- The data is not altered - Data integrity is maintained; it remains unaltered.
- No theoretical limit in applications - Unbounded potential across diverse applications.
- No security hardware required (data confidentiality) - Ensures data confidentiality without the need for specialized security hardware.
- Security proofs - Supported by proven security mechanisms.
- Resistance to ransomware (Cloud) - Built to withstand ransomware attacks, especially in cloud environments.
- Resistance to quantum computer attacks - Designed to be resilient against potential quantum computing threats.

FHE is one of the 5 Impactful Emerging Technologies for 2022 (GARTNER)

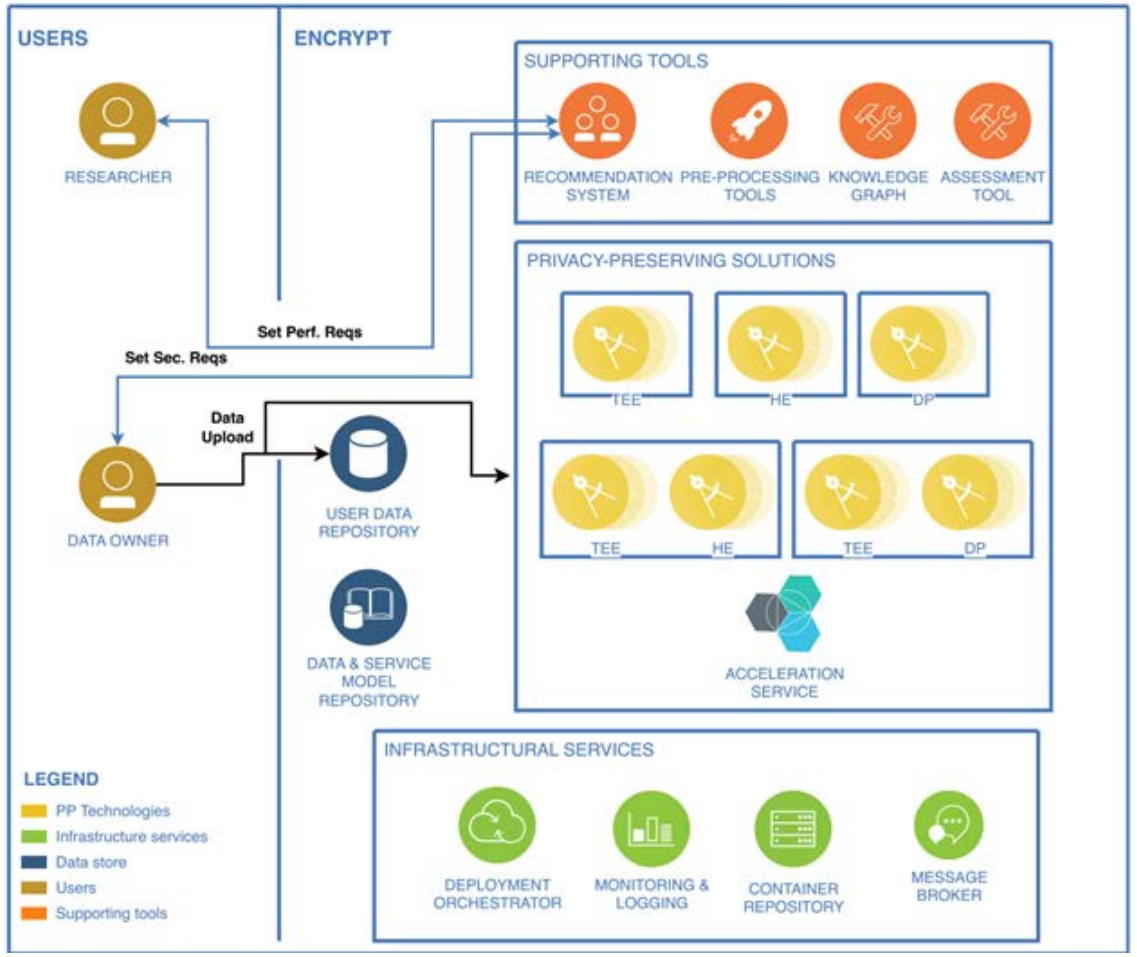
encrypt

User and system requirements

- Collection of users' needs and specification of ENCRYPT system requirements have been performed following ENISA "Guidelines for SMEs on the security of personal data processing "
- Assessing and managing security risks for personal data
  - ✓ Definition of processing operation and its context
    - What is the personal data processing operation?
    - What are the types of personal data processed?
    - What is the purpose of the processing?
    - What are the means used for the processing of personal data?
    - Where does the processing of personal data take place?
    - Which are the categories of data subjects?
    - Which are the recipients of the data?
  - ✓ Understanding and evaluating impact
    - Type of personal data
    - Criticality of the processing operation
    - Special characteristics of the data subjects
  - ✓ Definition of possible threats and evaluation of their likelihood
  - ✓ Evaluation of risk

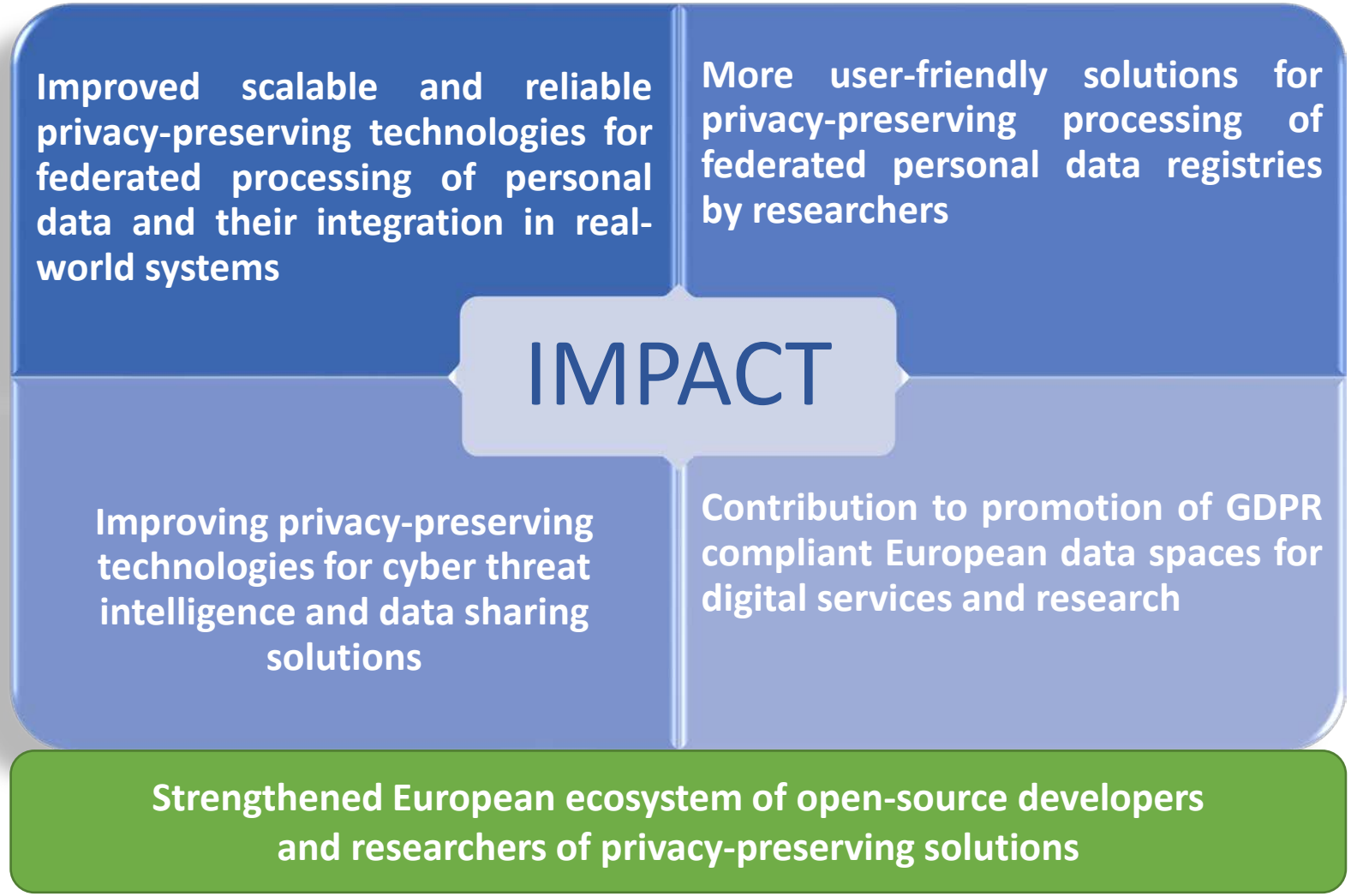
ENCRYPT architecture design

- Adoption of the RM-ODP (Reference Model of Open Distributed Processing) architectural standard
  - ✓ The Enterprise viewpoint includes a definition of ENCRYPT objectives, services, and users
  - ✓ The Computation viewpoint overviews the different components and their organization
  - ✓ The Information viewpoint defines different service information flows at all interfaces within the ENCRYPT architecture
  - ✓ The Engineering viewpoint describes the interaction across the entire distributed ENCRYPT architecture
  - ✓ The Technology viewpoint includes the identification of ENCRYPT technologies, used for the implementation, e.g., hardware and software platforms, networks, storage devices



encrypt

ENCRYPT Contribution To Call Impacts



encrypt

Thanks a lot for your attention !

Contact info: salvatore.dantonio@uniparthenope.it