ENCRYPT - A scalable and practical privacy-preserving framework

Clustering Meeting – 10/02/2023

Giovanni Mazzeo

Trust Up srl

Project Summary

- ENCRYPT - A scalable and practical privacy-preserving framework
- Grant Agreement No: 101070670

- Start Date: 01/07/2022
- Duration: 36 Months

- Total Budget: 4,392,540.00€

The ENCRYPT Consortium

- **14 Partners:**
  - ✓ **8 Countries**
  - ✓ **3 Pilots**

BANK OF EPIRUS COOPERATIVE
YOUR LOCAL BANK

CERTH
CENTRE FOR RESEARCH & TECHNOLOGY HELLAS

ENGINEERING
THE DIGITAL TRANSFORMATION COMPANY

cea

MANCHESTER 1824
The University of Manchester

ARISTOTLE UNIVERSITY OF THESSALONIKI

UNIVERSITÄTSmedizin. MAINZ

TrustUP
A PARTHENOPE UNIVERSITY SPIN-OFF

EXUS

EIGHTBELLS
Independent Research & Consultancy

TILBURG UNIVERSITY
Understanding Society

DBC EUROPE S.A.

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

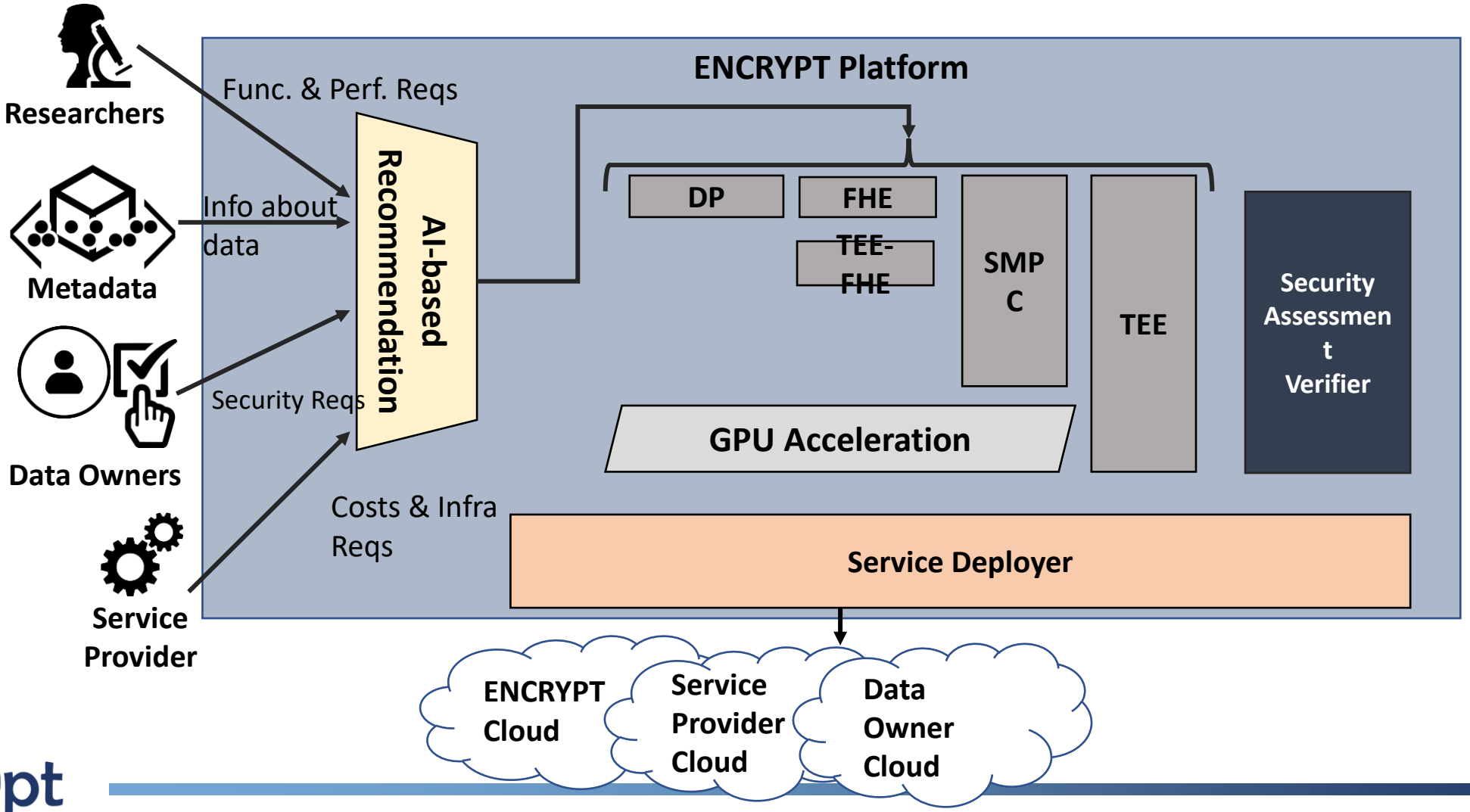
encrypt

ENCRYPT - A scalable and practical privacy-preserving framework

- ENCRYPT provides a platform for secure interoperability among:
  - ✓ **data owners**,
  - ✓ **researchers**,
  - ✓ **and service providers**
- through **confidential processing of privacy-sensitive data.**
- It does so via configurable, optimizable, and verifiable privacy preserving techniques, specifically:
  - ✓ *Fully Homomorphic Encryption* (FHE)
  - ✓ *Secure Multi-Party Computation* (SMPC)
  - ✓ *Differential Privacy* (DP)
  - ✓ *Trusted Execution Environment* (TEE)

encrypt

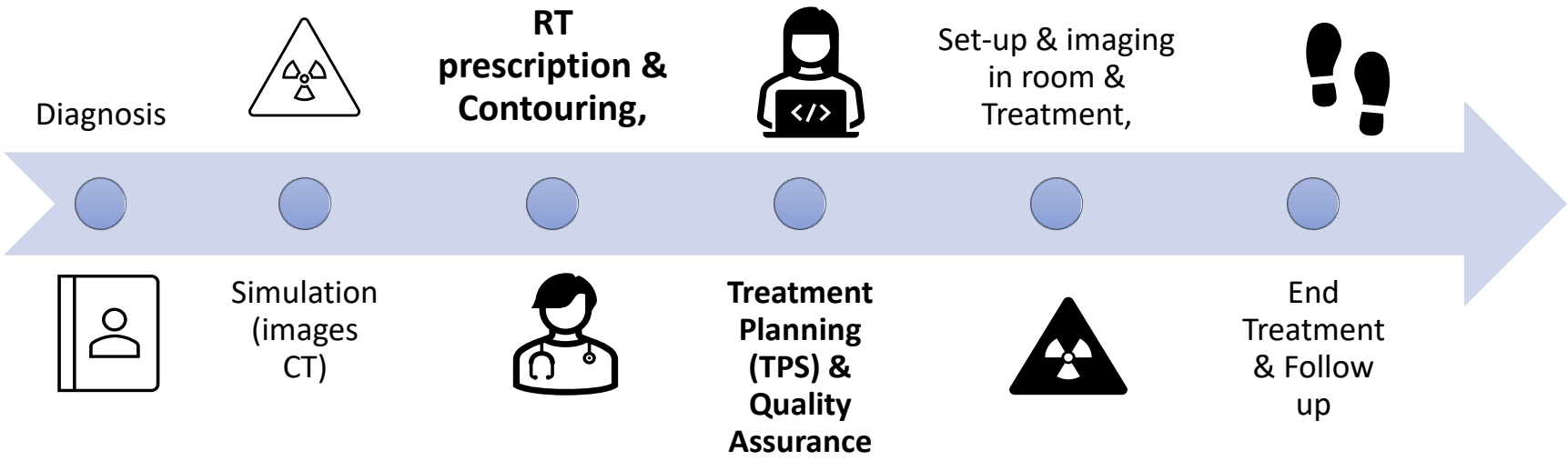
The ENCRYPT Architecture



The Innovation brought by ENCRYPT

- ENCRYPT combines privacy-preserving technologies to overcome their limitations
  - ✓Privacy-preserving technologies used in ENCRYPT present drawbacks when used alone in specific use cases and under certain conditions
  - ✓As an example: HE + TEE
- ENCRYPT provides a contribution in the field of accelerated privacy-preserving technologies
- ENCRYPT implements an approach to ease the identification of PP solutions based on a number of metrics
  - ✓Privacy-level
  - ✓Data to protect
  - ✓Sensitive processing
  - ✓Performance requirements
  - ✓Cost requirements
  - ✓Deployment location

The Health Domain Use Case – Cooperative Oncology



- **Risks**
  - ✓ While anonymization is already adopted to protect confidentiality of users, no security measures are taken to protect the integrity of prescription, contouring, and treatment planning phases. Their tampering could threaten patients' life.
- **The ENCRYPT Solution**
  - ✓ The generation of treatment planning and related metadata are performed in a TEE-secured Container. Data is shielded and verified via the hw-sealed key accessible from inside the enclave

The Financial Domain Use Case

- Bank of Epirus is a financial institution gathering a vast trove of data related to their customers to extract valuable information and score their creditworthiness
- Customer interactions with the bank hold the promise for better services, tailored to customers and more profitable to the institutions.

- **Risks**
  - ✓ Analytics made on customers' financial data of customers could lead to an exposure of sensitive information

- **The ENCRYPT Solution**
  - ✓ In ENCRYPT, homomorphic encryption combined with TEE is used to protect the computation and at the same time overcome limitations of HE

Thank you!

Stay in touch

https://encrypt-project.eu/

encrypt-project

@encrypt_project