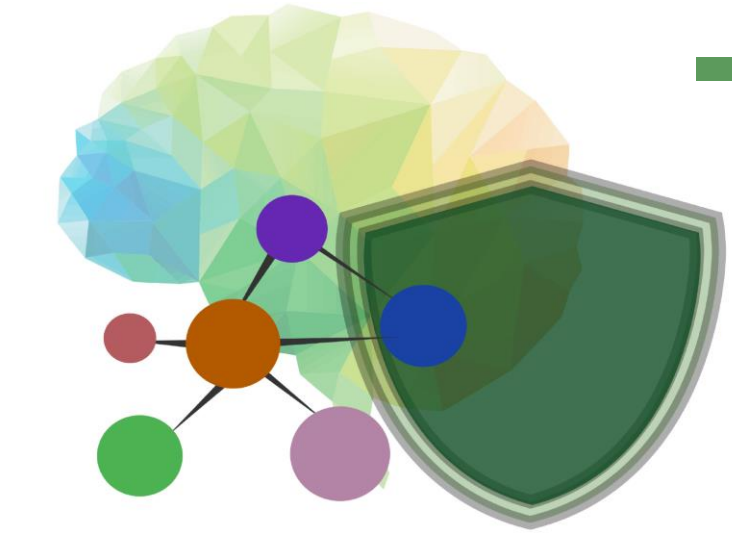
SECURED NEWSLETTER

ISSUE #2 | MARCH 2024



WELCOME

Welcome to the second newsletter of the SCALING UP SECURE PROCESSING, ANONYMIZATION AND GENERATION OF HEALTH DATA FOR EU CROSS BORDER COLLABORATIVE RESEARCH AND INNOVATION EU project, formally named also as SECURED.

In this newsletter we present the current version of the architecture as defined by the SECURED consortium members, events where the SECURED project was highlighted as well as recent scientific publications developed in the context of the project.

SECURED ARCHITECTURE

Pages 2-3 describe the preliminary SECURED architecture and its components.

EVENTS & NEWS

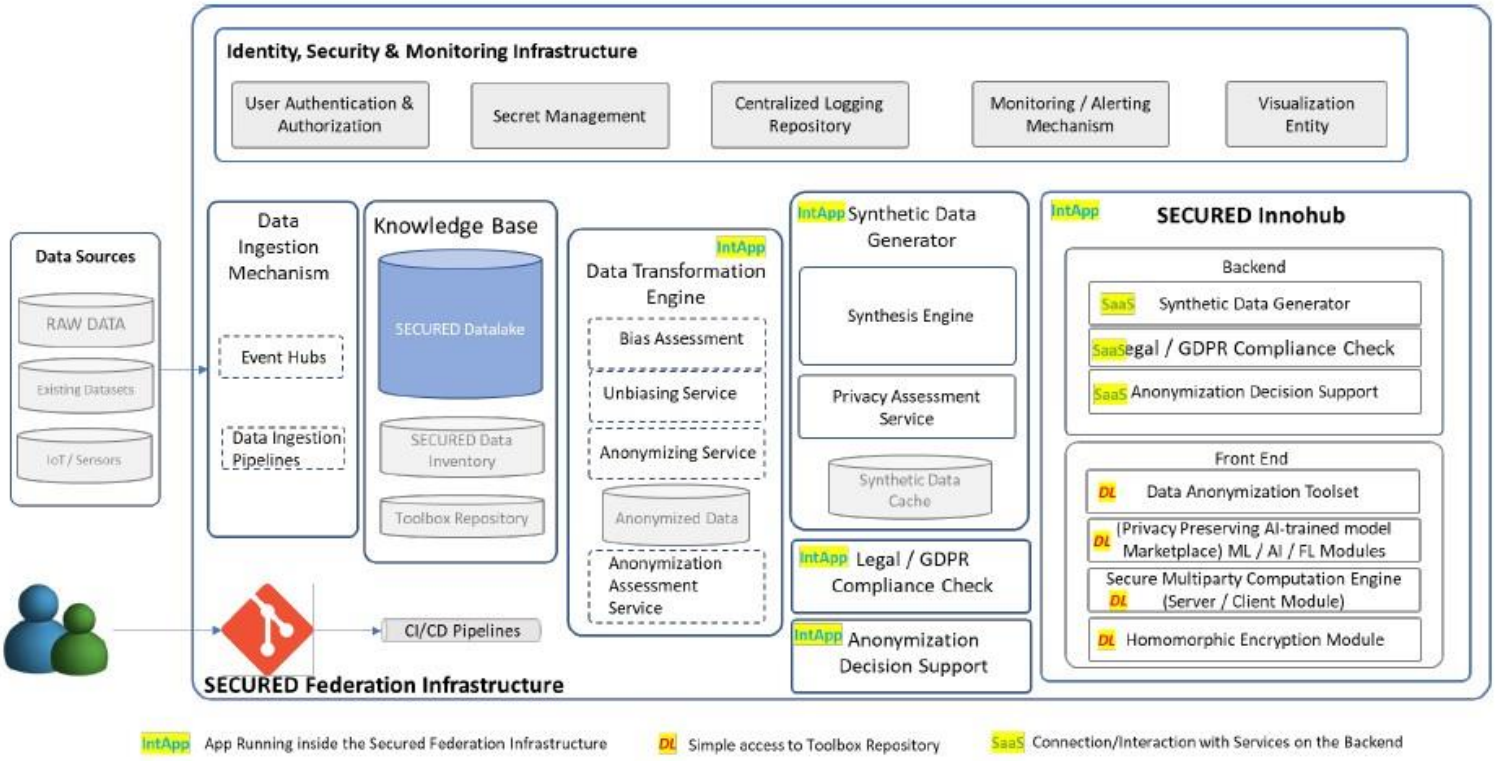
Pages 4-5 provide the current update of the project from the end of the first semester until February 2024.

BASIC INFO

Page 6 provides initial information regarding the project, including the members of the Consortium, basic facts of the project and social media platforms.

SECURED ARCHITECTURE

In **SECURED**, our intention is to offer a one stop collaboration hub able to provide a secure and trusted environment for decentralized, cooperative processing of health data through SMPC techniques as well as generation of new, synthetic data and anonymization assessment to health data providers and users. Our vision is to facilitate the broad adoption of health datasets across Europe by making the interconnection between EU health data hubs, the health data analytics research community, health application innovators (like Healthcare SMEs) as well as end users.



The broader **SECURED** architecture contains several interconnected services which cooperate to provide the overall platform functionality. Purely from an architectural standpoint, these services are contained inside the **SECURED Federation Infrastructure**, more or less an umbrella-entity that allows us to define the boundaries of the provided solution as well as to properly identify the necessary communication interfaces and flows that need to be implemented.

The function of each component is described below.

Funded by the European Union (Grant Agreement Nr. 101095717, SECURED Project). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Health and Digital Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Identity, Security and Monitoring Infrastructure

The Identity, Security and Monitoring Infrastructure is the architectural node responsible for federated user authentication, delegated fine-grained authorization ensuring role-based access to corresponding services, user management and communication channel encryption. The node incorporates the centralized logging repository, a dedicated monitoring/alerting mechanism and a visualization entity for transforming system-oriented information into a more user-friendly format.

Data Ingestion Mechanism

The Data Ingestion Mechanism is responsible for accurate, timely and error-free data transfer from all external data sources to the data repositories and/or data transformation functions of the SECURED Federation Infrastructure.

SECURED Knowledge Base

The SECURED Knowledge Base will act as the major data storage module of the broader SECURED Federation Infrastructure. Due to the vastly heterogeneous data that the specific module needs to handle, it must integrate several data storage solutions, each with a predefined scope and functionality.

Data Transformation Engine

The Data Transformation Engine operates as a Platform-as-a-Service within the SECURED Federated Infrastructure and utilizes the Data Anonymization Toolbox as a service for the SECURED Innohub users.

SECURED Innohub

The SECURED Innohub will act as the user entry-point to further exploit the SECURED Federation Infrastructure functionality. The module will allow access to authorized users only.

Synthetic Data Generator

The Synthetic Data Generator is the component that will be in charge of producing new data when required. This component is data-driven, therefore it will require an external preparation, e.g. machine learning training.

Anonymization Decision Support

The Anonymization Decision Support is a platform-as-a-service (an application running inside the SECURED Federation Infrastructure) where a registered SECURED Innohub user provides as an input information related to a specific dataset and the service suggests the optimal techniques to be used for anonymizing the dataset and/or for performing anonymization assessment.

Legal Compliance Check

The Legal Compliance Check component is offered as a service of the SECURED Innohub and is providing support on the legal aspects related to a privacy sensitive dataset.

Funded by the European Union (Grant Agreement Nr. 101095717, SECURED Project). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Health and Digital Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

EVENTS & NEWS

SECURED Privacy Preservation Tutorial in 5th CPS Summer School at Sardinia, Italy

SECURED participated in the 5th Cyber Physical Systems (CPS) Summer School in Sardinia Italy (18-22 September 2023) with a specialized Tutorial on Privacy Preservation. **SECURED** partners demonstrated how secure computation techniques including homomorphic encryption can be adopted in constrained settings, and applied to CPSs and medical devices.

SECURED Project at hiPEAC Conference 2024

The work done in **SECURED** project regarding Fully Homomorphic Encryption was presented by prof. Paolo Palmieri (UCC partner) in hiPEAC conference 2024 on the tutorial entitled "Open Source Libraries and Components for Security" that took place in Munich on the 18th of January 2024. Prof. Palmieri's presentation was greeted very favorably by the hiPEAC audience and very interesting discussions followed the presentation.

SECURED Project at DATE Conference 2024

The **SECURED** concept and the latest developments in the project have been presented in the DATE 2024 Conference by the Project Coordinator prof. Francesco Regazzoni (UvA) at Valencia, Spain, 27 March 2024. Prof. Regazzoni's presentation provided a lot of insight on the **SECURED** activities, followed by a discussion on the Privacy Preserving Technologies adopted in the project. The open call was also introduced to the DATE'24 audience and although the SECURED open call hasn't aired yet, several companies already expressed interest to get involved.

Funded by the European Union (Grant Agreement Nr. 101095717, SECURED Project). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Health and Digital Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

SECURED Project Second Plenary Meeting

The 2nd Plenary meeting of SECURED was held in Athens on January 14th-15th 2024. The progress on the project's research activities was presented but most importantly through the partners' collaborative effort the project's use cases where revised and updated! The partners convened for a focused workshop on key project activities: Secure Multiparty Computation/FHE, anonymization/deanonymization, Federated Learning, and synthetic data generation. As a consortium we harmonically and collectively established our next research and development goals to provide beyond the state of the art privacy preserving technologies.

Blog posts

Learn about the legal considerations surrounding the management of sensitive personal data for medical purposes, and their protection by innovative data anonymization tools developed by the SECURED Project.

- SECURED: Project updates and legal insights for the beginning of its second year, *by Maja Nisević and Daniela Spajić, CiTiP Blog* **Part 1** **Part 2**

Latest Publications

- Olar, A., Tyler, T., Hoppa, P. *et al.* "Annotated dataset for training deep learning models to detect astrocytes in human brain tissue." *Sci Data* 11, 96 (2024). https://doi.org/10.1038/s41597-024-02908-x
- J. L. F. Betting, C. I. De Zeeuw and C. Strydis, "Oikonomos-II: A Reinforcement-Learning, Resource-Recommendation System for Cloud HPC," 2023 IEEE 30th International Conference on High Performance Computing, Data, and Analytics (HiPC), Goa, India, December 18-21, 2023, pp. 266-276, doi: 10.1109/HiPC58850.2023.00044
- Pol G. Recasens, Jordi Torres, Josep Berral, Søren Hauberg, Pablo Moreno-Muñoz, "Beyond Parameter Averaging in Model Aggregation," NeurIPS 2023, New Orleans, Luisiana, USA, December 10-16, 2023
- Alexander Islam El-Kady, Apostolos P. Fournaris, Vassilis Paliuras, "Dilithium Hardware-Accelerated Application using OpenCL-based High-Level Synthesis," 42nd IEEE/ACM International Conference on Computer-Aided Design (ICCAD) 2023, San Francisco, California, USA, October 29 - November 2, 2023

Funded by the European Union (Grant Agreement Nr. 101095717, SECURED Project). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Health and Digital Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

CONSORTIUM

The SECURED project is bringing together 17 partners from 9 different European countries highlighting the expertise to successfully accomplish the neds and goals of the project.

More info on the consortium here.

PROJECT BASIC INFORMATION

Title: SCALING UP SECURE PROCESSING, ANONYMIZATION AND GENERATION OF HEALTH DATA FOR EU CROSS BORDER COLLABORATIVE RESEARCH AND INNOVATION

Acronym: SECURED

GA No: 101095717

Start: 01 January 2023

End: 31 December 2025

Topic: HORIZON-HLTH-2022-IND-13-02

Type of action: HORIZON-RIA

Project Coordinator: Francesco Regazzoni

Project Coordinator Institute: University of Amsterdam

STAY CONNECTED

https://secured-project.eu/

YouTube @securedeuproject

@SecuredEU

securedeuproject

secured-project

Funded by the European Union (Grant Agreement Nr. 101095717, SECURED Project). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Health and Digital Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.