encrypt

A scalable and practical privacy-preserving framework

ENCRYPT White Paper

Revolutionizing Data Privacy

The ENCRYPT Project's Innovations and Applications

The ENCRYPT project, an innovative collaborative project under the Horizon Europe Framework Programme, will integrate privacy-preserving technologies (PPTs) across 3 key sectors, aiming to revolutionize the way sensitive data is processed and protected in the digital age. This white paper outlines the project's core methodologies and applications, including the use of Fully Homomorphic Encryption (FHE), Trusted Execution Environments (TEE), Differential Privacy (DP) and advanced Hybrid Protection Services. Through its platform, ENCRYPT seeks to address the combined challenge of ensuring data privacy and utility across federated data spaces within the European Union. This highlights ENCRYPT's compliance with GDPR standards while enabling secure and efficient data processing activities.

ENCRYPT use cases stem from a diverse set of domains such as Fintech, Health and Cybersecurity and through this, the versatility and impact of its results and activities will be presented. Each use case, leverages the project's cutting-edge PPTs to safeguard data while still allowing for data-analytics, enabling decision-making to occur.

From securing financial transactions, achieving data confidentiality and strengthening defenses against cyber threats, ENCRYPT's use cases showcase the project's innovations in privacy preservice technologies. This white paper serves as an essential guide for stakeholders across industries, academia and the ecosystem, offering insights into the project's objectives, methodologies and potential to shape the future of data privacy and security.

Contents

Funded by the European Union

encrypt

A scalable and practical privacy-preserving framework

ENCRYPT White Paper

ENCRYPT Project

Nowadays, a substantial volume of extensive data is available, presenting opportunities to tackle emerging challenges and enhance research and digital services. One instance involves crafting more precise machine learning models through federated learning over massive datasets. However, the primary obstacle in handling such data, often containing sensitive or personal information, lies in the potential threat of cyber-security attacks and the risk of disclosure or misuse. Compliance with data protection regulations and the rigorous standards set by the EU on personal data adds further complexity to the manipulation of such information.

To address these issues, advanced Privacy-Preserving (PP) computation technologies, such as Fully Homomorphic Encryption (FHE), or Differential Privacy (DP), could offer GDPR-compliant solutions once they achieve greater scalability and reliability, making them suitable for real-world scenarios.

Despite the potential, existing PP technologies encounter several limitations before becoming widely adopted security solutions. FHE struggles with scalability when dealing with substantial amounts of data requiring high computational overhead for processing encrypted data. Another common limitation is their lack of integration with existing networking infrastructure and security protocols in ongoing research. In the case of DP as a privacy-preserving technique for machine learning, its effectiveness is notable for low sensitivity queries, making it more challenging for certain query types. Hardware solutions such as Software Guard Extensions (SGX) offer fast and trusted computation but face scalability issues. This is particularly the case for large-scale aggregated computations involving numerous user inputs due to limited paging.

ENCRYPT aims to confront these challenges by providing researchers and service providers dealing with personal and sensitive data a scalable, practical and adaptable privacy-preserving framework. This will facilitate GDPR-compliant processing of data stored in federated cross-border data spaces, going beyond current standards. The project addresses scalability by exploring new multi-key and threshold FHE schemes, considers threats and performance by investigating combinations of various PP methods and tackles slow computation times by offering hardware acceleration. The proposed solutions will undergo development and validation in diverse settings and real-world use cases, including the complex cross-border federated processing of large datasets.

ENCRYPT Platform

The ENCRYPT platform is a pioneering solution within the project, aiming to redefine the landscape of data privacy through its innovative and comprehensive approach to securing sensitive information. Designed to comply with GDPR privacy standards, the platform integrates an array of advanced privacy-preserving technologies (PPTs). Its user-centric design approach aims to empower users of the platform with scalable, efficient and GDPR-compliant data processing capabilities. Although tailored to meet the needs of the project's use cases in healthcare, finance and cybersecurity, the ENCRYPT platform can also facilitate users from other industrial sectors too.

Overview Description of Platform

The ENCRYPT platform provides a comprehensive ecosystem designed to address the multifaceted challenge of handling sensitive data in compliance with GDPR standards. By integrating PPTs such as Fully Homomorphic Encryption (FHE), Trusted Execution Environments (TEE), Differential Privacy (DP), alongside innovative Hybrid Protection Services and Hardware Acceleration techniques, the ENCRYPT platform makes available an array of solutions for secure data processing. The platform's data safeguarding capability will enable researchers, healthcare professionals, and service providers to process personal data without compromising individual privacy.

Funded by the European Union

Central to the ENCRYPT platform is a user-centric, AI-powered recommendation system. This innovation advises users on the optimal PPT to be used for their application - based on their specific data types and user scenarios, thus simplifies the choice of which data privacy technologies to be used - making it more accessible to users with varying levels of expertise.

The ENCRYPT platform also stands out with its robust Hybrid Protection Services which bring together various services, to create a multi-layered defense mechanism against potential data breaches and unauthorized access. Complementing the isolation capabilities of TEE with the encryption power of FHE, the platform offers a comprehensive solution that protects data throughout its lifecycle - during storage, transmission and processing, ensuring that data remains confidential and tamper-proof.

The platform's capabilities are further enhanced by state-of-the-art Hardware Acceleration techniques. Because of the computational demands of PPTs, ENCRYPT integrates specialized hardware to optimize the runtime of cryptographic operations. This improves the platform's efficiency and performance and also scales up its capabilities - enabling the processing of larger datasets.

In summary, the ENCRYPT platform represents an innovation in how sensitive data is processed and protected. Its comprehensive approach, combining cutting-edge privacy-preserving technologies with user-friendly interfaces and AI-driven recommendations, provides a pathway of facing the privacy challenges of the digital age. As the platform evolves, it will enhance GDPR compliant security and privacy of data processing within the EU and the project aims to inspire further innovation in the broader field of data privacy. ENCRYPT, through its development of this platform is leading the way in creating a more secure, privacy-conscious future for digital data processing.

Privacy Preserving Technologies

The ENCRYPT project addresses the increasingly complex challenge of preserving privacy in the digital age where data breaches and privacy concerns are present and rising. As part of its mission, the project is dedicated to developing a scalable, practical and adaptable privacy-preserving framework that enables GDPR-compliant processing of sensitive data which are stored in federated cross-border data spaces. ENCRYPT utilises state-of-the-art privacy-preserving technologies (PPTs), including Fully Homomorphic Encryption (FHE), Trusted Execution Environments (TEE), Differential Privacy (DP) and Hybrid Protection Services, which are also supported by hardware acceleration techniques developed within ENCRYPT activities. Together, these technologies represent ENCRYPT's approach to securing data privacy while allowing for the use of data for computational data analytics to be carried out.

By bringing these technologies together, ENCRYPT aims to bring to real-world practical applications, the theoretical potential of PPTs. The project's implementation of FHE, TEE, DP and hardware acceleration solutions is key to its commitment to advancing the field of data privacy, offering robust protection against unauthorized access and ensuring the integrity and confidentiality of sensitive information. In this way, ENCRYPT will be able to play a role in the setting of new standards for data security and privacy.

Fully Homomorphic Encryption

FHE is an advanced PPT achieving robust data security while maintaining functionality. This cryptographic paradigm enables the execution of complex mathematical operations on encrypted data, which allows any data processing in theory and more kinds of data processing in practice. As data are processed in ciphertext form, confidentiality of sensitive information is retained. This superpower of FHE makes it one of the key technologies of the ENCRYPT project used as a concerted effort to translate cutting-edge cryptographic research into practical applications - especially in private-sensitive industry sectors such as healthcare and finance.

FHE involves complex mathematical operations that can be computationally intensive. ENCRYPT's approach to embedding FHE focuses on optimizing these operations to make them feasible for practical applications. This involves addressing challenges related to noise management in FHE schemes - a fundamental aspect that affects the accuracy of encrypted computations.

Funded by the European Union

Trusted Execution Environment

TEE is an important component in ENCRYPT's set of privacy-preserving technologies. TEE creates an isolated execution space within the processor, ensuring that sensitive data and operations are shielded from the rest of the device's environment and any potential malware. TEE therefore ensures the confidentiality, integrity and security of the data during its processing phase. In this way, GDPR-compliance in the processing of sensitive data can be achieved through this robust solution that safeguards against unauthorized access and manipulation.

Within ENCRYPT, TEE is used alongside FHE, to create a multi-layered defense strategy. For instance, when analysing medical data, TEE enables secure analysis and processing of health information, ensuring that patient privacy is maintained without compromising the use of data for research and clinical purposes. Similarly, in the cyber threat intelligence domain, TEE plays a critical role in securely processing and analyzing data to identify and mitigate threats without exposing sensitive information.

In addition, ENCRYPT also uses unique features of TEE, such as remote attestation - which allows verification of the TEE's integrity from a remote location. This feature establishes and builds trust among participants in federated dataspaces by ensuring that the environment is secure, has not been tampered with and that secure and private data sharing and processing can take place.

Differential Privacy

As a mathematical framework, DP offers a robust mechanism for ensuring the privacy of individual data within a dataset. This makes DP an important tool in ENCRYPT's quest for providing solutions for projects with ethical and technical complexities of handling sensitive information.

The basis of DP lies in adding a controlled amount of random noise to aggregate data queries, thereby masking the contribution of individual data points. This ensures that the privacy of individuals in the dataset is protected, even from those with access to the aggregate data outputs. In this way, data can be utilized for research and development while adhering to GDPR requirements.

Through ENCRYPT's AI-powered recommendation system, whenever DP is recommended for use, algorithmic adjustments will ensure that the noise added is minimal yet sufficient to guarantee privacy – relative to the application setting. While DP provides strong privacy guarantees, its application can affect the accuracy and utility of the processed data. A significant portion of ENCRYPT's research is devoted to exploring and mitigating these trade-offs, ensuring that DP's implementation is both effective and efficient while still providing data utility.

Hybrid Protection Services

Hybrid protection services within ENCRYPT brings together PPTs to enhance data security and privacy across federated data spaces. This approach synergizes FHE and TEE creating a layered defense mechanism which is robust and versatile.

ENCRYPT's hybrid protection services is adaptable, tailoring privacy solutions to the specific needs and contexts of its use cases. By integrating FHE with TEE, ENCRYPT leverages the strength of FHE's encryption and processing capabilities alongside the secure, isolated processing environment provided by TEE.

This combination ensures that data remains encrypted and secure throughout its lifecycle, from storage and transmission to processing – safeguarding privacy across a wide range of potential security threats. This successful merging and use of two technologies also sets a precedent for the broader adoption of hybrid privacy-preserving solutions – incorporating various different tools for the security application of various sectors.

Hardware Acceleration

ENCRYPT also incorporates hardware acceleration as an essential component to enhance the computational performance of PPTs. This is an important step towards deploying real-world applications of complex cryptographic techniques, such as FHE and DP and thus making them more accessible and applicable to a wider range of industrial sectors.

Hardware Acceleration has been specifically designed and developed to migrate the computational intensity of PPTs by offloading certain computationally intensive tasks to Graphics Processing Units (GPUs) - significantly reducing the required processing time. An additional benefit of this work is improved energy efficiency of these operations – which also addresses the energy requirements challenge in the adoption of PPTs.

Funded by the European Union

Functionalities and Modules

ENCRYPT offers a suite of functionalities and modules specifically designed to safeguard sensitive information. These components are not standalone solutions but are interwoven to be part of the ENCRYPT's platform tools and services, prioritizing the user and enabling access of advanced PPTs to users with diverse expertise and requirements.

Pre-processing Tool

ENCRYPT's pre-processing tool is specifically designed to enhance the privacy-preserving capabilities of the platform, preparing data for processing and ensuring that Private Identifiable Information (PII) are identified in a manner which achieves the highest standards of privacy and security – thereby maximizing data utility while minimizing privacy risks.

More specifically, the pre-processing tool performs a variety of data cleansing and transformation operations which prepare data for subsequent processing with PPTs such as FHE and DP. The tool's capabilities include the handling of missing values and the elimination of duplicates. Furthermore, the tool uses advanced techniques for data reduction and feature selection, which are essential for optimizing the performance of privacy-preserving computations. By selecting the most relevant features and reducing the dimensionality of datasets, the tool ensures that computational resources are utilised efficiently, thereby facilitating the processing of large volumes of data without compromising on privacy or speed.

Another key functionality of the pre-processing tool is its ability to perform PIIs detection and extraction. Using Machine Learning (ML) algorithms and Natural Language Processing (NLP) techniques such as Named Entity Recognition (NER), the tool can identify and isolate PIIs within datasets. The extracted PIIs are used by the Recommendation System to propose to the end-user the most appropriate PPT. This capability automates the protection of personal data by decreasing the potential for privacy breaches and enhances the integrity of the data processing pipeline to allow the ENCRYPT platform to support compliance with GDPR and other privacy regulations.

Recommendation System

ENCRYPT's Recommendation System is an innovative tool designed to offer expert advice to users on the most suitable PPT for their specific data processing scenarios. The tool uses a sophisticated algorithm which leverages AI to analyze the characteristics of the user's data, the intended processing activities and the associated privacy requirements. Considering factors such as data sensitivity, processing complexity and compliance requirements, the system makes tailored PPT recommendations that balance data utility with privacy and security.

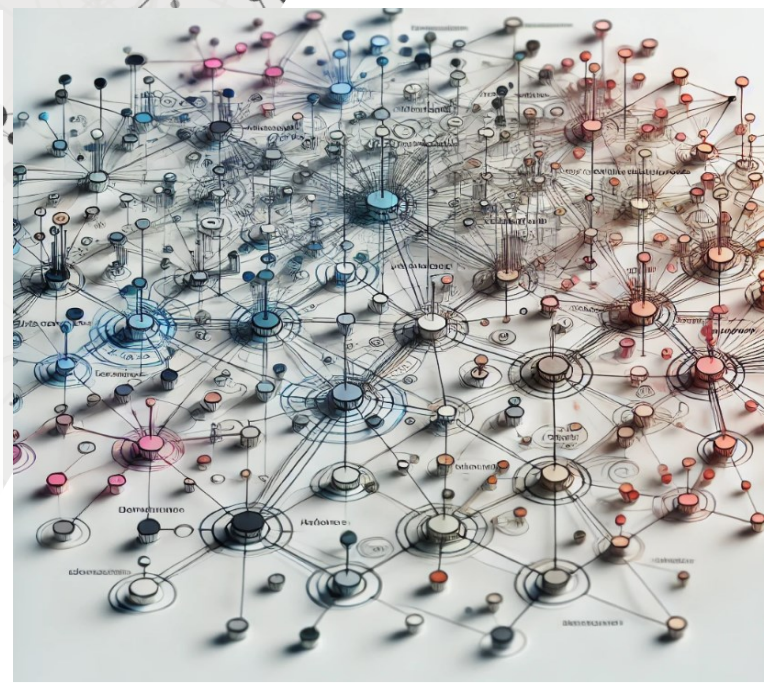
The recommendation system is also designed to continuously update its knowledge base with the latest research findings, technological advancements and regulatory changes. This ensures that the recommendations consider current state of the art but are also forward-looking, anticipating future developments in the privacy domain.

The recommendation system is also designed in a user-centric approach, providing a justification for its recommendation tailored to the knowledge the user, which helps build trust in the system. This makes it more usable for non-experts and facilitates its adoption across diverse sectors, including healthcare, finance, and cybersecurity.

Funded by the European Union

Knowledge Graphs

ENCRYPT also integrates Knowledge Graphs to its set of tools which serve as repositories of interconnected data, but also as dynamic models that enhance the understanding, accessibility and utility of information. This allows the ENCRYPT platform to create a semantically rich, interconnected web of data that can be securely processed and analyzed, which enables a deeper understanding of complex data landscapes without compromising individual privacy.



ENCRYPT's implementation of Knowledge Graphs is designed to map out the relationships between various data points, enabling a more detailed analysis and interpretation of information. This capability is crucial for navigating the complex requirements of GDPR-compliant data processing, as it allows for the seamless integration of data from diverse sources across federated data spaces in the European Union. This fosters a cooperative ecosystem where data can be shared and processed in a manner that is both secure and efficient, opening up the possibility of PPT applications across various sectors.

The use of Knowledge Graphs also plays a crucial role in enhancing the platform's AI-powered recommendation system. Knowledge Graphs provide a semantic layer that facilitates the intelligent analysis of data, enabling the recommendation system to make informed suggestions that are tailored to the unique characteristics and privacy requirements of each dataset and application of users.

Risk Assessment Tool

ENCRYPT's Risk Assessment Tool is an innovative approach to identify, evaluate and mitigate privacy and security risks associated with data processing activities. The tool uses a sophisticated algorithm which carries out both qualitative and quantitative analyses to offer a comprehensive overview of potential privacy and security vulnerabilities coupled with their severity. This enables stakeholders to prioritize mitigation efforts, ensuring that resources are allocated efficiently to safeguard sensitive information.

One of the key functionalities of the risk assessment tool is its ability to provide customized recommendations for risk mitigation by suggesting cybersecurity mitigations that may help in addressing identified risks which are tailored to the specific context of each use case. These mitigations complements those indicated by the recommendation system.

The risk assessment tool is specifically designed with usability in mind, featuring a user friendly interface that allows users to easily navigate through the risk assessment process. This user-centric approach ensures that the tool is accessible to a wide range of stakeholders, from data protection officers and IT security professionals to project managers, junior researchers and policy makers. This empowers stakeholders to actively participate in the privacy and security management of their data processing activities.

Funded by the European Union

Use Cases

The ENCRYPT project presents three use cases which illustrate the practical application and impact of these PPTs across the sectors of Fintech, Health, and Cyber Threats. Each use case has been designed to address the unique challenges and requirements of its respective domain, showcasing the adaptability and effectiveness of the ENCRYPT platform in safeguarding sensitive information while facilitating essential data processing activities.

Fintech

The Fintech use case is a real-world example application of privacy-preserving technologies in the financial sector. It shows how the ENCRYPT platform can facilitate secure and compliant data analysis and data processing within the highly regulated, GDPR compliant and privacy-sensitive environment of financial services.

The main objective of the Fintech use case is to demonstrate the ability of the ENCRYPT platform to enable financial institutions to share and process their data in a manner that protects sensitive customer information and proprietary financial models. This is achieved through PPTs such as FHE, DP and TEE, which allow these institutions to derive valuable insights without exposing the underlying data – which includes transaction histories, customer profiles and financial records. This not only enhances operational efficiency and service delivery but also builds trust with customers by demonstrating a commitment to protecting their personal and financial information.

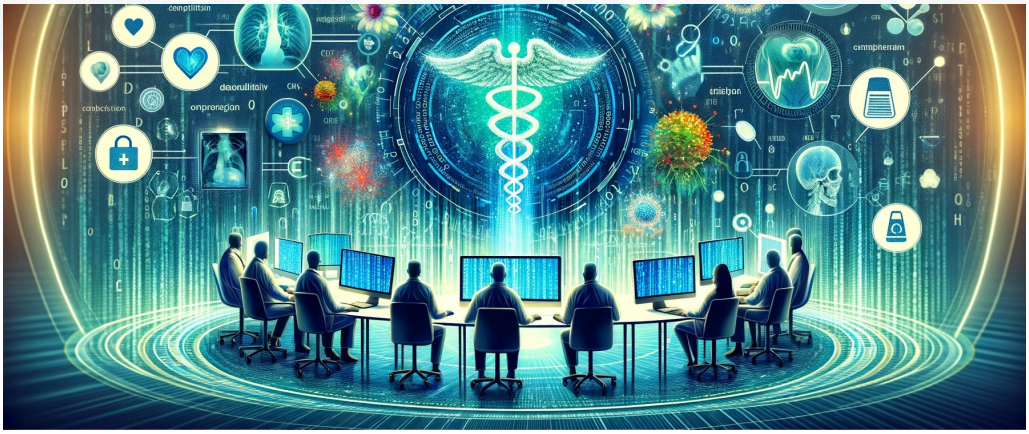
Furthermore, this use case explores the deployment of the ENCRYPT platform's Recommendation System and Risk Assessment Tool. This proactive approach to risk management is invaluable in the Fintech domain, where the rapid pace of innovation and the complexity of financial products necessitate a dynamic and adaptive privacy strategy.

Health

The ENCRYPT use case for Health is a landmark application of PPTs in healthcare, a sector where the confidentiality of patient information is paramount. This use case is specifically designed to address the unique challenges of handling sensitive health data, showcasing how the ENCRYPT platform enables medical institutions to process and analyze health data securely, thereby enhancing patient care while also complying with GDPR and other privacy regulations.

An important aspect of the Health use case is effort on enhancing the interoperability and accessibility of health data across different healthcare institutions and research entities. The ENCRYPT platform facilitates a secure and efficient exchange of health information, fostering collaboration and innovation in medical research and patient care. By thus allowing secure access to anonymized patient datasets, the platform supports the development of predictive models for disease progression and treatment outcomes, contributing to the advancement of personalized medicine.

The Health use case also illustrates the practical application of ENCRYPT's recommendation system and risk assessment tool. These modules guide healthcare institutions in selecting the most appropriate PPTs for their specific data processing needs and provide a comprehensive evaluation of potential privacy and security risks. This approach will help streamline the adoption of privacy technologies in healthcare settings and will also ensure that risk mitigation strategies are aligned with the sector's regulatory and operational requirements.



Funded by the European Union

Cyber Threats

The ENCRYPT Cyber Threats use case highlights the important role PPTs can have in strengthening cybersecurity measures against increasingly sophisticated cyber threats. The use case also demonstrates how the ENCRYPT platform employs advanced cryptographic and privacy-enabling technologies to enable secure and private sharing of Cyber Threat Intelligence (CTI) across organizations. Specifically, for this use case, fully homomorphic encryption and trusted execution environment will be used. These technologies enhance collective defense mechanisms while ensuring that sensitive information remains protected.

The challenge of this use case is the balance between the need for open sharing of threat intelligence and the necessity to protect the confidentiality of the shared data. Cybersecurity teams require access to timely and relevant threat data to effectively prevent, detect and respond to cyber-attacks. However, the sharing of this data often involves sensitive information that could reveal vulnerabilities, proprietary security measures, or even personal data, thereby posing privacy risks. The ENCRYPT project addresses this challenge using PPTs. These technologies ensure that data can be analyzed, correlated and exchanged without exposing the actual content, thus maintaining the privacy of the data subjects and the security of the organizations involved.

Data pre-processing is used in the Cyber Threats use case. The Cybersecurity domain data holders use the tool in their premises to clear their data (e.g. remove duplicates) and identify PIIs in the dataset. The Cyber Threats use case also explores the use of ENCRYPT's recommendation system and the risk assessment tool, which is tailored for the cybersecurity domain. The recommendation system assists organizations in selecting the most suitable PPTs based on the specific context of shared threat intelligence, considering factors such as the sensitivity of the data and the required level of data utility. In parallel, the risk assessment tool enables organizations to identify and evaluate the potential privacy and security risks associated with sharing CTI, providing actionable insights for risk mitigation.

The use case also highlights the importance of collaboration and interoperability in combating cyber-threats. By facilitating secure and privacy-preserving sharing of CTI, the ENCRYPT platform enhances the collective cybersecurity posture of participating organizations. It enables a more coordinated response to cyber threats, reducing duplication of efforts and accelerating the countering of threats and dissemination of critical threat intelligence.

Conclusion

As this white paper has presented, ENCRYPT is a novel project with innovations in the application of privacy-preserving technologies. It also paves the way for future secure and private data processing across the European Union. Through its integration of state-of-the-art technologies such as fully homomorphic encryption, trusted execution environments, differential privacy, coupled with advanced hybrid protection services and hardware acceleration techniques, ENCRYPT has laid down the groundwork for overcoming some of the most pressing challenges in data privacy today. The project's approach to combine technical expertise with regulatory and ethical compliance, sets a new paradigm in the quest to balance data utility with privacy.

The practical applications of ENCRYPT, illustrated through its use cases in Fintech, Health, and Cyber Threats, highlights the project's potential to catalyze change across various sectors. By providing a secure and compliant framework for data processing, ENCRYPT protects sensitive information and also provides the opportunity for new innovations and improved services. The project's emphasis on user-centric tools further enhances its accessibility and applicability, ensuring that the benefits of privacy-preserving technologies can be widely adopted and adapted to meet the needs of a diverse set of users across various sectors and technical expertise.

The insights, methodologies and lessons learned during ENCRYPT are expected to influence future research, policy-making and technological development, enabling a more secure, privacy-conscious digital future. As we move forward, ENCRYPT results have the potential to play a critical role in shaping the landscape of data privacy and security, ensuring that the digital society of tomorrow is built on the principles of trust, confidentiality and respect for individual privacy.

Funded by the European Union

encrypt

A scalable and practical privacy-preserving framework

ENCRYPT project in a nutshell

Project Title	A scalable and practical privacy-preserving framework
Acronym	ENCRYPT
GA No	101070670
Start	01 July 2022
End	30 June 2025
Budget	4.392.540 €
EU Funding	4.392.540 €
Call	HORIZON-CL3-2021-CS-01
Funding	RIA - Research and Innovation action
Topic	HORIZON-CL3-2021-CS-01-04

Consortium

EXUS · ENGINEERING THE DIGITAL TRANSFORMATION COMPANY · CERTH CENTRE FOR RESEARCH & TECHNOLOGY HELLAS · EIGHTBELLS Independent Research & Consultancy · cea

TrustUP A PARTHENOPE UNIVERSITY SPIN-OFF · ARISTOTLE UNIVERSITY OF THESSALONIKI · DBC EUROPE S.A. · TILBURG UNIVERSITY Understanding Society · UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

BANK OF EPIRUS COOPERATIVE YOUR LOCAL BANK · GOETHE UNIVERSITÄT FRANKFURT AM MAIN · JG|U UNIVERSITÄTSmedizin. MAINZ · MANCHESTER 1824 The University of Manchester

Stay in touch!

https://encrypt-project.eu · encrypt-project · @encrypt_project

encrypt

A scalable and practical privacy-preserving framework

Funded by the European Union