“Blockchain-based auditing for securing eHealth data exchange integrity”

Presented by Dimitris Kanakidis/ Head of Innovation

Who we are

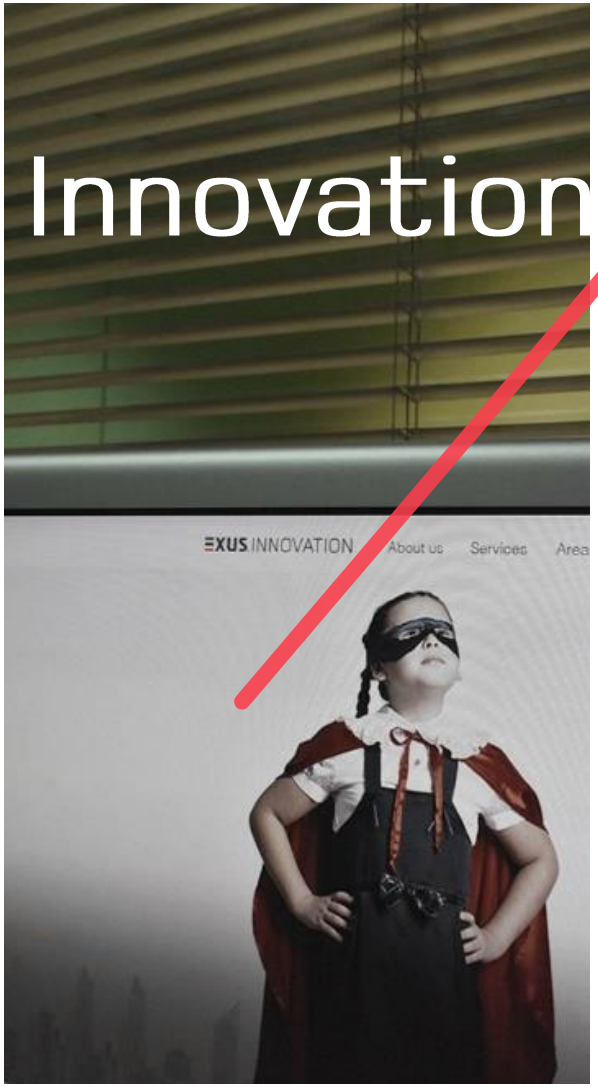
29 years in the business

156 employees

Customers in 26 countries

London Athens

INFOCOM MOBILE CONNECTED World

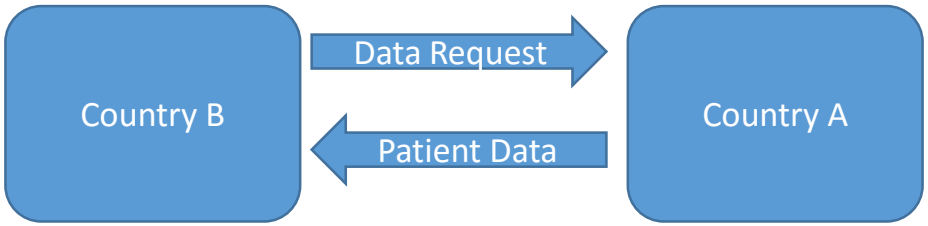


Our Innovation department is working on numerous large-scale Research and Innovation Projects in various sectors such as Security (Physical and Digital), Health and Creativity with our core competence being around data analytics, complex event processing and large scale cloud implementations

Technical Skills

We have participated in more than 50 European and National Research Programs leading to widespread recognition of our Research/ Innovation department in the IT field.

Challenge: Cross-Border eHealth Data Retrieval



Country B should be aware of:

- Data formats and protocols of every country A
- The national infrastructure of every country A
- Regulations of every country A

The European Framework for Cross-border eHealth Data Exchange

- **OpenNCP** is the technical outcome of the epSOS project
- **OpenNCP** is a part of the eHealth Digital Service Infrastructure (eHDSI), under the Connecting Europe Facility (CEF) and allows for the exchange of eHealth Data in Europe

PS: Patient Summary
eP: ePrescription

epsos
EUROPEAN PATIENTS SMART OPEN SERVICES

CEF programme

INFOCOM MOBILE CONNECTED World

Pillars for eHealth Interoperability in EU

- Existing national healthcare infrastructures/legislation remain unchanged
  - Member States are reluctant to accept impositions on their own legislation
- Trust among Member State (MS) is based on contracts and agreed policies
  - The National Infrastructure (NI) of a MS never checks for security messages from the NI of another MS
- Information is exchanged but not shared.
  - Any OpenNCP user MAY NOT modify an original document from abroad.
    The user retrieves a "read-only" document.

Security Assessment of epSOS

- Security of communications is ensured by employment of cryptography and secure protocols
- Security of communicating parties is not enforced by technical means; it is instead assumed by legally binding agreement
- No protection is offered against propagation of cyberattacks; instead, attacks which success in compromising a NI can exploit NCP to propagate to other countries

…These security aspects were out of scope of epSOS

The KONFIDO* Use case

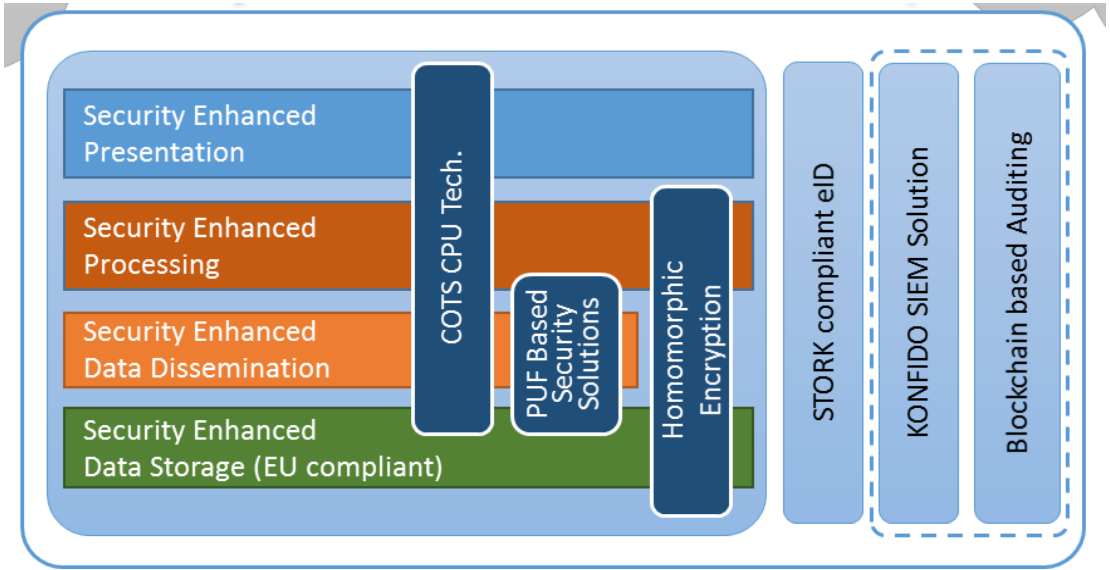
Co-funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement nº 727528.

www.konfido-project.eu

* KONFIDO means “Trust” in Esperanto

Six state-of-the-art Technologies

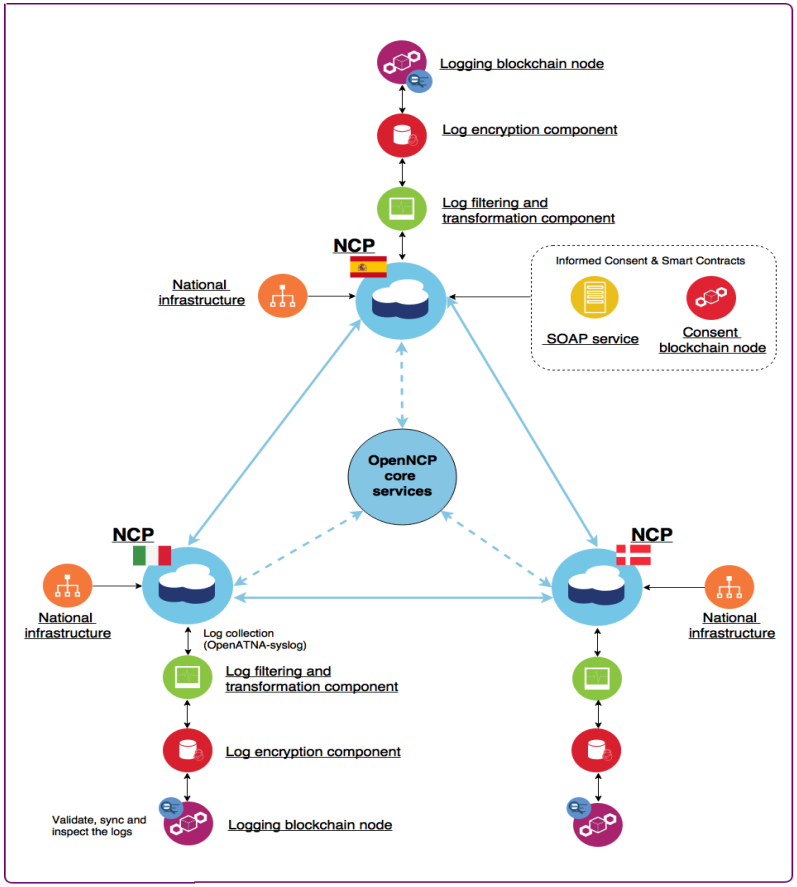
- Exploit the new security extensions of COTS CPUs for creating protected execution environments for eHealth applications
- Develop novel photonic encryption key generation technologies
- Build an efficient homomorphic encryption mechanism supporting secured health data storage, processing and exchange
- Develop customized SIEM solutions for real-time monitoring of the security of eHealth applications
- **Implement disruptive logging and auditing mechanisms**
- Design and implement a eIDAS compliant eID infrastructure



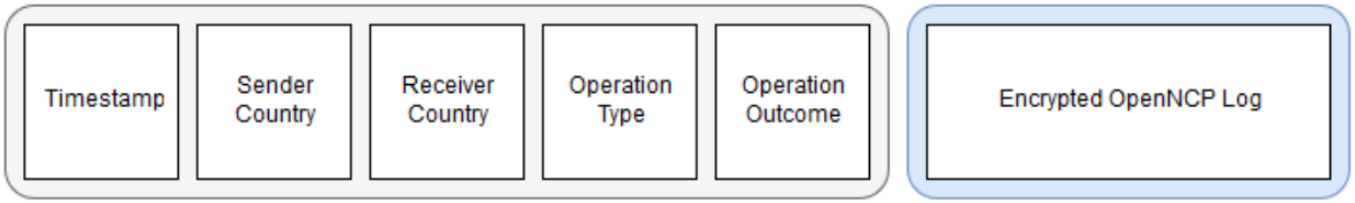
KONFIDO auditing blockchain-based mechanism

- Distributed, federated, tamper-proof log management system
  - Collects relevant logs generated by OpenNCP operations
  - Based on industrial standards such as ATNA
- Informed consent management system
  - Collects any consent provided through OpenNCP
  - Permanent record on when this consent was provided and its duration

No health data is stored on the blockchain!



OpenNCP log storage scheme:



- Each KONFIDO log contains a set of exchange related metadata and the actual log
- Metadata do not contain any personal identifiers and they are accessible to all countries
- A combination of symmetric and asymmetric encryption is applied on the OpenNCP log

Only auditors from the countries participating in the original eHealth exchange request are able to successfully decrypt the log

Why blockchain?

- Creates a **secure**, **unforgeable registry** for log files regarding the exchange of eHealth data among MSs
- Enables **automated permission handling** based on patient informed consent through smart contracts
- Provides **traceability** and **liability** support

A legally binding system based on **blockchain** auditing that allows to prove that specific eHealth data:

- Have been requested by a legitimate entity
- Have been provided (or not)

What is the future of Blockchain in Healthcare?

- 40 percent of health execs see blockchain as top 5 priorities. (https://www2.deloitte.com/insights/us/en/topics/understanding-blockchain-potential/global-blockchain-survey.html)
- Furthermore, the global healthcare market spend on blockchain is expected to hit $5.61 billion by 2025, according to a report by BIS Research.
- The adoption of the blockchain technology could save the healthcare industry up to $100-$150 billion per year by 2025 in data breach-related costs, IT costs, operations costs, support function costs and personnel costs, and through a reduction in frauds and counterfeit products. (https://bisresearch.com/industry-report/global-blockchain-in-healthcare-market-2025.html)

EXUS INNOVATION

THANK YOU