KONFIDO Project: a secure infrastructure increasing interoperability on a systemic level among eHealth services across Europe

L. Coppolino, S. D'Antonio, L. Romano, M. Staffa

ITASEC 2017
January 20, 2017, Venice, Italy

Project overview

- Call: H2020-DS-2016-2017 (Digital Security Focus Area)
- Topic: DS-03-2016 - Increasing digital security of health related data on a systemic level
  - *"Proposals would provide a holistic approach to address challenges of secure storage and exchange (including cross-border) of data, protection and control over personal data, and security of health related data gathered by mobile devices combined with the usability of the eHealth solutions."*
- Type of action: RIA (Research and Innovation action)
- Requested contribution: 4.992.077,50 Euro
- Start date: November 1st, 2016
- Duration: 36 months

Partners (1/2)

- EXUS SOFTWARE LTD (UK) – Industry
- ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS – CERTH (GR) – Research Organization
- CONSORZIO INTERUNIVERSITARIO NAZIONALE PER L'INFORMATICA (IT) – Research Organization
- FUNDACIO EURECAT (SP) – Research Organization
- CONSORCI INSTITUT D'INVESTIGACIONS BIOMEDIQUES AUGUST PI I SUNYER (SP) – Research Organization
- COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES – CEA (FR) – Public Body
- MEDCOM (DN) – Public Body

Partners (2/2)

- SUNDHED.DK IS (DN) – Public Body
- IMPERIAL COLLEGE OF SCIENCE TECHNOLOGY AND MEDICINE (UK) – University
- Bit4id srl (IT) – SME
- TELBIOS (IT) – SME
- Fondazione Santobono Pausilipon onlus (IT) – End-user
- AGENCIA DE QUALITAT I AVALUACIO SANITARIES DE CATALUNYA - AQUAS (SP) – End-user
- TIME LEX CVBA (BE) – Law Firm
- EULAMBIA (GR) – Spin-off

Setting up the scene

- The digital era in the in healthcare domain has resulted in the introduction and massive use of tele-monitoring solutions, Electronic Health Records (EHR), genomic information and mobile health (mHealth) applications in combination with the nascent concept of coordinated care.
- These new technologies are leading to an improved user acceptance of e-health applications and to a full exploitation of their advantages.

The other side of the coin

- The constantly increasing digitalization, the digital preservation and use of sensitive data, the introduction of cloud computing and decentralized architectures, as well as the booming market of mobile and wearable devices come along with the cost of proliferation of cyber-crime and the creation of malicious applications.
- Some examples:
  - August 3, 2016, Massive Cyber Attack at Banner Health Affects 3.7M Individuals.
    - Banner Health, one of the largest healthcare systems in the U.S., learned that cyber attackers may have gained unauthorized access to patient information, health plan member and beneficiary information, as well as information about physician and healthcare providers
  - December 21, 2015, Anthem's breach sent a wave of panic through the healthcare industry
    - A cyber-attack against the health insurer Anthem exposed clients' most sensitive and valuable personal information, and revealed just how unprepared the health industry was to threats from increasingly sophisticated cyber criminals

EC initiative on eHealth

- The European Commission (EC) recently developed the Action Plan for eHealth 2012-2020 that provides a roadmap to empower patients and healthcare workers, to link up devices and technologies, and to invest in research towards the personalised medicine of the future.
- This plan focuses its emphasis on providing optimal health services within the European Union (EU), independent of their location, thus supporting and enhancing eHealth application interoperability, security, and privacy issues.
- Given the fast growing uptake of tablets and smartphones, the Action Plan also includes a special focus on mHealth.

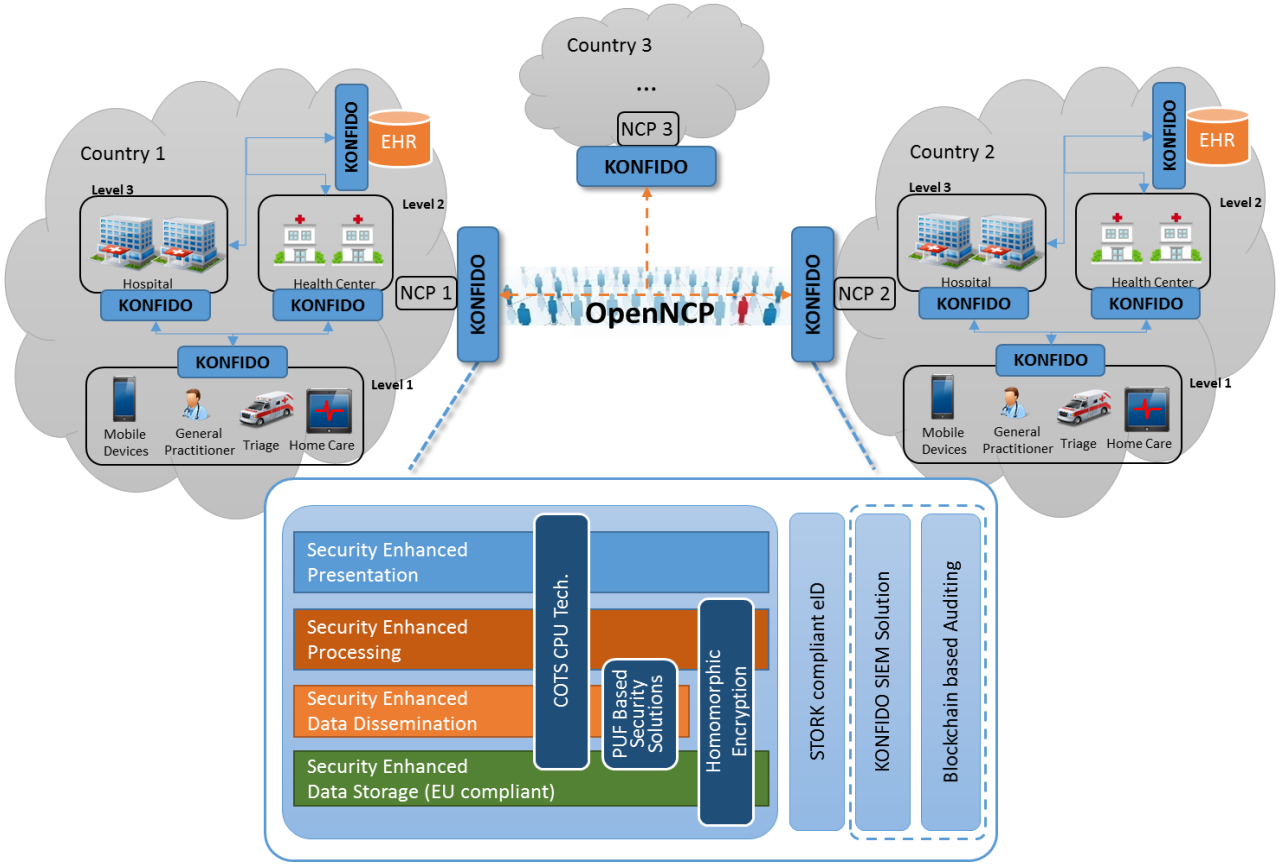
Security challenges in eHealth

- **Data preservation**: ensuring that digital information of continuing value remains accessible and usable.
- **Data access and modification**: storing and retrieving data housed in databases and other repositories. Authentication and authorization are considered as fundamental functions for performing these actions.
- **Data exchange**: the data exchange can be performed both internally (i.e, involving two or more parties belonging to the same healthcare institution) or externally (i.e. involving multiple health care stakeholders belonging to distinct health care systems, possibly of different countries).
- **Interoperability and compliance**, enabling heterogeneous systems and devices to interact and share data by following legal directives and regulations.

The KONFIDO approach

- KONFIDO aims at creating a scalable and holistic paradigm for secure inner and cross-border exchange, storage and overall handling of healthcare data in a legal and ethical way both at national and European level.
- In order to achieve this objective, the following six technological pillars will be exploited:
  - Security Information and Event Management (SIEM)
  - Physical Unclonable Function (PUF)-based cryptography
  - Homomorphic encryption
  - STORK-compliant eID
  - Intel Software Guard Extensions (SGX)
  - Authentication and logging mechanisms *à la* block-chain

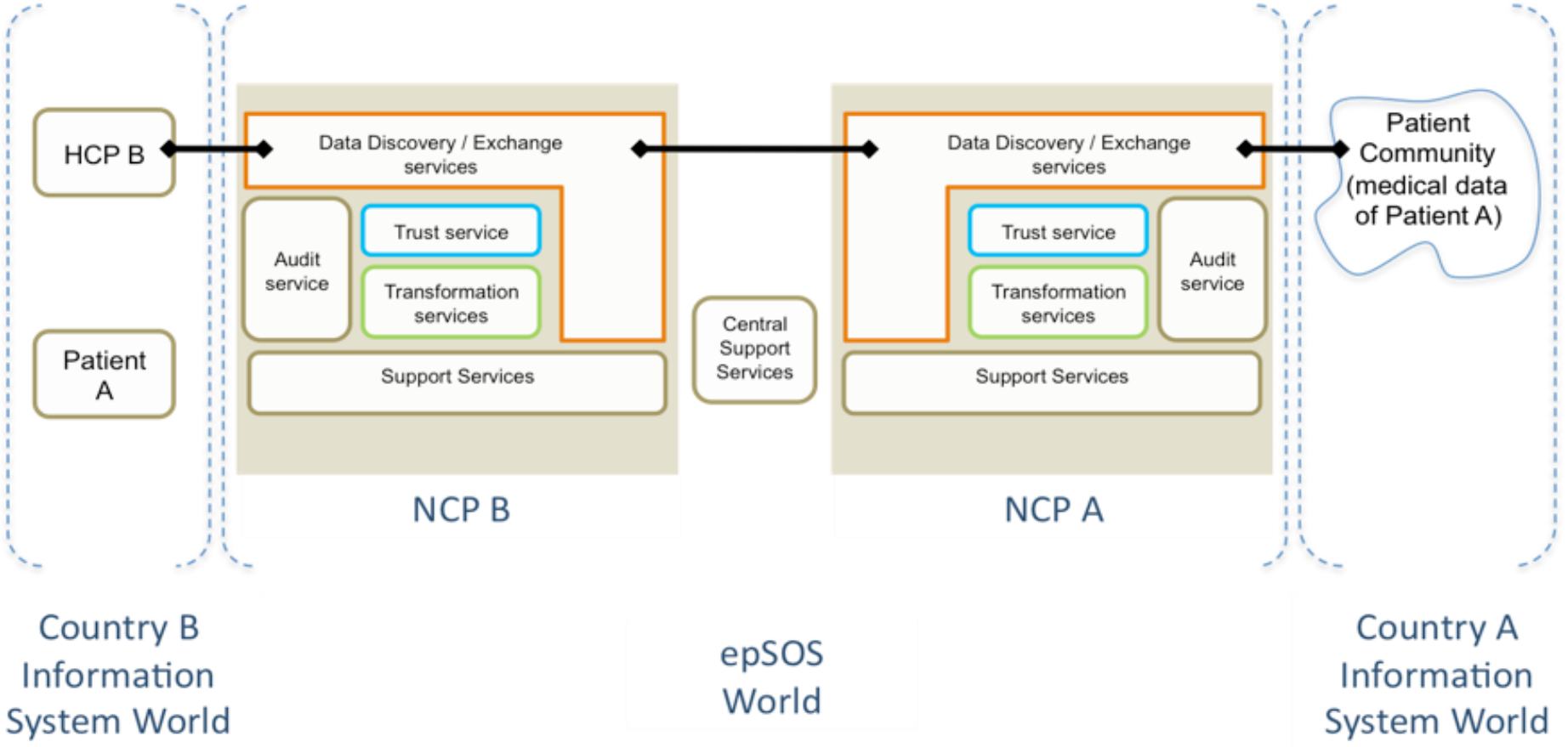
Conceptual view of KONFIDO federated architecture



OpenNCP

- The OpenNCP framework offers a comprehensive set of interoperability services to enable national and regional e-Health platforms to set up cross-border health information networks with minimal adaptation of the existing infrastructure.
- The OpenNCP, available as open source software, has been adopted in 10 Member States, allowing them to interconnect their eHealth infrastructures.
- The National Contact Point (NCP) is the fulcrum of cross border interoperability, exploiting the role of connecting the Participating Nation (PN) to the European Level environment.

NCP concept



HCP= HealthCare Provider

KONFIDO and openNCP (1/2)

- KONFIDO will not extend OpenNCP with additional features. Rather, it will enhance OpenNCP by securely connecting it to the KONFIDO platform.
- By doing so, the information systems of individual countries can interoperate in a secure way.
- KONFIDO will ensure data security at different architectural levels, and in particular: presentation, processing, dissemination, and storage.

KONFIDO and openNCP (2/2)

- Security of data at rest will be provided by means of homomorphic encryption: medical data will be **stored** using the KONFIDO storage support, which will secure sensitive data while guaranteeing compliance to EU regulations.
- When data need to be **exchanged**, KONFIDO will protect their level of security by means of two different technologies, namely: Physical Unclonable Functions and COTS CPU technology.
- Solutions, such as the SGX Intel extensions, enable to create a secure tunnel between the federated domains thus providing additional security during the transferring of the data.
- The OpenNCP reference implementation can thus be enhanced by exploiting the SGX Intel extensions to support both remote attestation of the destination end-point and secure transferring of data which moves encrypted from an end point to the other and finally to the human operator.
- In case the underlying hardware does not support security extensions, KONFIDO will use cryptographic techniques as a fall-back.

Secure data processing in KONFIDO

- Secure **processing** of data can be achieved in KONFIDO in two ways: either data will be in clear, but the processing will be done in a protected execution environment provided by the CPU or data will be encrypted and the processing will be done using homomorphic cryptography.
- The availability of these two options will enable KONFIDO to provide security at a higher performance when the underlying hardware supports security extensions such as ARM TrustZone or Intel SGX.
- At processing time, security enclaves will ensure the decoupling between the sensitive data processing environment and the hosting environment, thus protecting health records even in case of malicious manipulations to the receiving system.
- The creation of security enclaves will guarantee data protection even against processes running with higher privileges and against physical attacks conducted in the hosting environment (e.g. memory inspection).

Further KONFIDO security enhancements

- When data has to be reported to a human operator, it must be decrypted. Security is then guaranteed by using COTS CPU technology for providing a protected presentation environment based on secure enclaves.
- Authentication of human operators will be guaranteed by KONFIDO STORK compliant eID support, which will implement a customized eID solution compliant to STORK specifications.
- Traceability and liability within the KONFIDO domain will be guaranteed by an unforgeable log management system based on block-chain auditing.
- The log management system will be also exploited by a Security Information and Event Management system specifically developed for a federated environment, compliant to the OpenNCP model, and tailored for the healthcare domain.

KONFIDO Use Case

- The effectiveness of the KONFIDO framework will be demonstrated in a realistic scenario dealing with secure cross-region and cross-border mobility for emergency management and patient empowerment.
- The scenario deals with the issues of hospital discharge and follow-up care, which have been found to be the weakest points of cross-border care, primarily because of the deficits in transferring information between hospitals and primary care providers.
- In this scenario a patient is discharged from a hospital in his/her country after an accident occurred out of his/her city and soon after he/she leaves for vacation towards a foreign country.
- In this context the possibility to empower the patients with tele-monitoring devices and to permit the access of their information is fundamental to achieve a secure continuation of the patient follow-up care.

Use case description (1/3)

- The healthcare authorities in the city where the accident takes place, offer a novel telemedicine service enabling to send important data from the ambulance to the emergency care centres, in order to speed-up the triage process and reinforce the preparedness levels.
- Using a tablet application, pictures are taken by the paramedics from the wounds of all family members, which are immediately transmitted through the mobile network to the emergency department on duty.
- Using KONFIDO technologies, encrypted transmission of these data is conducted.

Use case description (2/3)

- In accidents, any information regarding the medical history of the injured can be critical.
- Using the national issued eID technology that KONFIDO recognizes and handles properly, the collection of all the information needed to intervene already in the ambulance (patient identification, clinical details, immunization details, and usual therapy) is made possible.
- On discharge the hospital of the city where the accident took place decided to equip the patient with a tele-monitoring kit for remotely monitoring him/her conditions, in a way to allow him/her to not give up the vacation that he/she and his/her family had already booked some months ago.

Use case description (3/3)

- Data gathered through the kit medical device will be securely transmitted through the KONFIDO network and registered to the patient's medical record in the hospital, where a Health Professional can follow-up the patient's care trend after discharge.
- The kit includes medical devices and a gateway which sends the measured vital signs to the Service Center in the hospital supporting the patients remotely. In case of emergency, he/she will be called back to the hospital for further investigations and exams.
- During this process KONFIDO security mechanisms will ensure data transferring and storage against attempts to data tampering.

Key features of the KONFIDO use case

- **Challenges**: Authentication of different actors at the national level and across different countries, data access policies, secure health data exchange among diverse organizations.
- **Security Threats**: Unauthorized access to sensitive personal healthcare information.
- **Main Actors**: Patients and family members, healthcare professionals from different regions of a country, healthcare organizations from different regions or countries.
- **Infrastructure employed:** eID infrastructure, smart-id technology, encryption mechanisms

Thanks a lot for your attention.

Contact info

- Salvatore D'Antonio
- salvatore.dantonio[at]uniparthenope.it
- Department of Engineering
- University of Naples Parthenope
- Centro Direzionale di Napoli Isola C4
- Ph: +39 081 5476766