



Konfido

Secure and Trusted Paradigm for
Interoperable eHealth Services

Paolo Campegiani
Bit4id
pca@bit4id.com



This project has received funding from the European Union's Horizon 2020
Framework Programme for Research and Innovation under grant
agreement no 727528.

Cross-border exchange of eHealth data in Europe

2

KONFIDO is an Horizon 2020 project that wants to facilitate the cross-border exchange of eHealth data in Europe

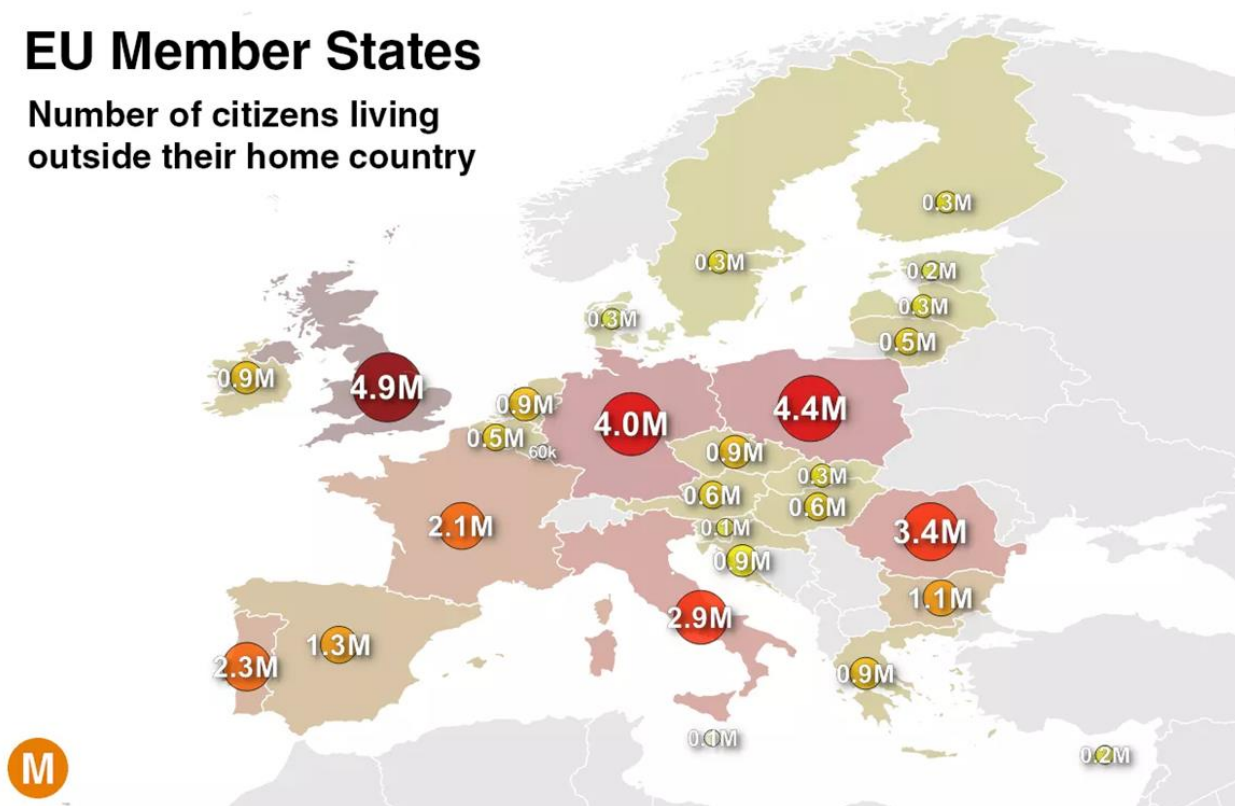
Cross-border exchange happens when an EU citizen that is abroad needs to access his/her eHealth data, stored in his/her country of origin.

How relevant is this *for you*?

Relevance of cross-border exchange of eHealth data

EU Member States

Number of citizens living outside their home country



(Source: U.N. Population division)

- There are around 40 M of Europeans living abroad (in the world)
- A significant number of them is living in Europe
- There are around 0.9M of British people living in Europe (source: Brexit data)
- Reasonable to say that there are at least 10M of Europeans living in an European country different the one of origin
- Plus, people temporarily abroad (tourists, conference attendees...)

Cross-border exchange of eHealth data as an European priority

- Affordable and universal healthcare in Europe is a fundamental right of every European citizen
- Making this possible for people abroad is a way to support citizens' mobility in Europe (and citizens' mobility in Europe leads to a better Union, a more functioning and productive labor market, a stronger economy)
- Cross-border interoperability between Electronic Health Record in Europe was the focus of the epSOS project (2008-2014) and e-SENS project
- epSOS developed the OpenNCP (Open National Contact Point) system
- Directive 2011/24/EU on patients' rights in cross-border healthcare
- Development of OpenNCP is funded by the Connecting European Facility (CEF) vehicle
- The «Joint Action to Support the eHealth Network» (JASeHN) is defining the guidelines for electronic exchange of eHealth data, including the Legal Agreement on the exchange of health data, to be signed by the Member States

Connecting Europe Facility and Digital Service Infrastructure

Connecting Europe Facility (CEF) is a regulation that defines how the Commission can finance support for the establishment of trans-European networks to reinforce an interconnected Europe. It's defined for three different areas:

CEF Transport: 24,05 BN €

CEF Energy: 5,53 BN €

CEF Telecom: 1,04 BN €

A Digital Service Infrastructure describes solutions that support the implementation of EU-wide projects, providing trans-european interoperable services. It is founded by CEF

Building Block DSI: basic digital service infrastructures (key enabler, like eDelivery)

Sector Specific DSI: DSI for specific domains (eHealth, Cybersecurity, e-Justice, ...)

OpenNCP, the DSI for eHealth

OpenNCP is a Sector Specific DSI service that allows for the exchange of eHealth Data in Europe (Patient Summary and ePrescription)

Each Member State has a single OpenNCP that acts as a gateway for all the cross-border requests of eHealth data

OpenNCP security model is Web of Trust: each OpenNCP instance trusts the others and processes requests for eHealth data on their behalf.

eHealth DSI Countries Deploying Services

	PS	eP
Austria	♥	♥
Croatia	♥	♥
Cyprus	♥	♥
Czech Republic	♥	
Estonia	♥	♥
Finland		♥
France	♥	
Germany	♥	
Greece	♥	♥
Hungary	♥	♥
Ireland	♥	♥
Italy	♥	♥
Luxembourg	♥	
Malta	♥	
Portugal	♥	♥
Sweden		♥
Switzerland	♥	♥

Konfido and OpenNCP

- Horizon 2020 project to advance state-of-the-art eHealth technology and specifically OpenNCP along these dimensions:
 - Digital security
 - Data preservation
 - Data access and modification
 - Data exchange
 - Interoperability
 - Compliance
- Holistic approach:
 - **User centric**
 - Targeting all the levels of an IT infrastructure
 - Taking into account legal, organizational and operational contexts

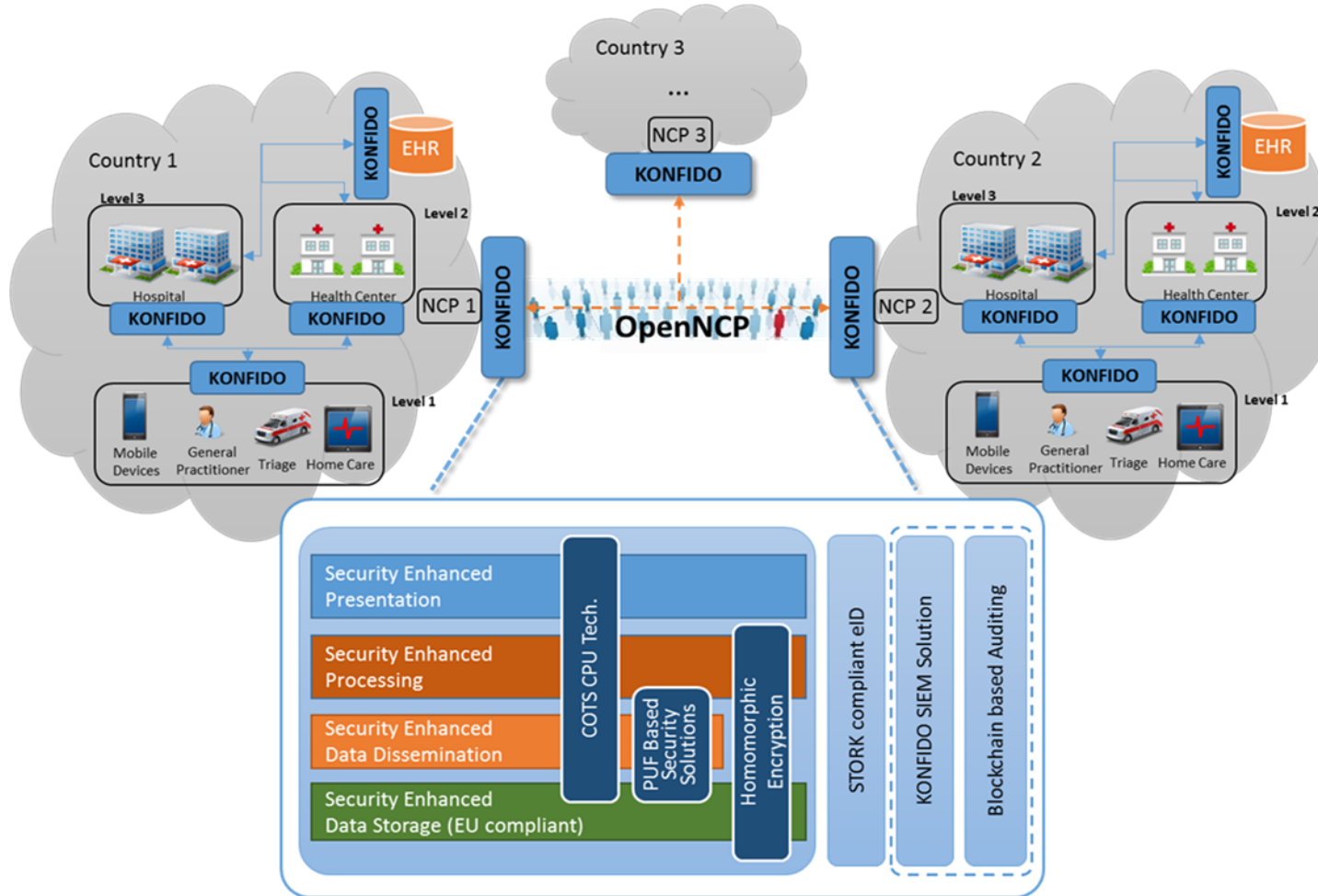
Konfido partners



Pilots in: Italy, Spain, Denmark



Konfido deployment view



Konfido works alongside OpenNCP providing security related services:

- eIDAS Authentication
- Intel Safeguard Extension
- Photonic Physically Unclonable Functions (pFUP)
- System Information and Event Monitoring
- Homomorphic Encryption
- Blockchain based logging

eIDAS Authentication

10

Using an eIDAS eID for eHealth brings in a clear legal framework for interoperability and security (assurance)

We are not considering the general solution for the problem, only what is needed to support eIDAS eIDs in the three participating countries

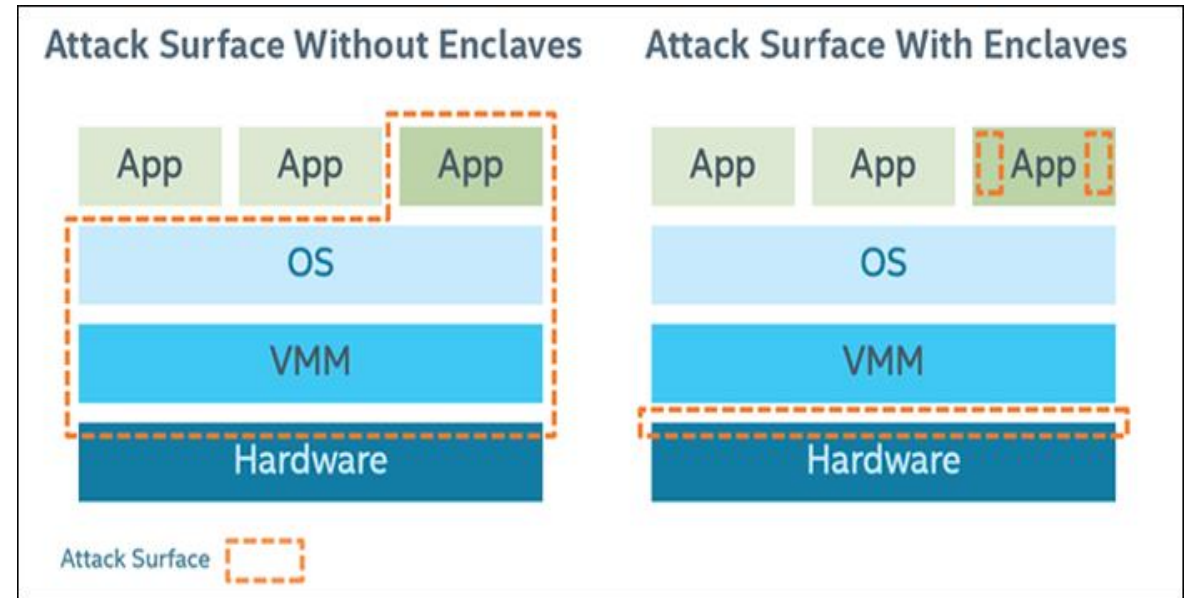


Intel SafeGuard Extensions

Intel Software Guard Extension protects some memory areas making them accessible only to a specific program function

- The OS cannot access them
- The hypervisor cannot access them

In Konfido SGX could be applied to protect keys, credentials and authenticated sessions

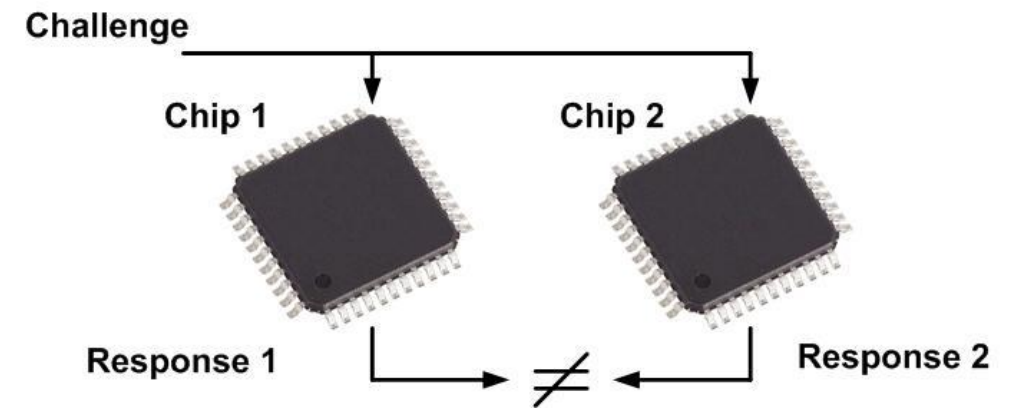


Photonic Physically Unclonable Functions

12

- Each chip has some physical defects
- These defects does not prevent the chip from working
- These defects are unique and not reproducible, even by the chip manufacturer

These defects could act as a unique identification for the chip as a base for an encryption mechanism or as a source of entropy



System Information and Event Monitoring

13

OpenNCP does not have a system to collect and analyse system logs

OpenNCP is a distributed system working with a «Circle of Trust» deployment principle

A System Information and Event Monitoring should collect logs from the different OpenNCP instances to consolidate a view on the systems' performance and behaviour



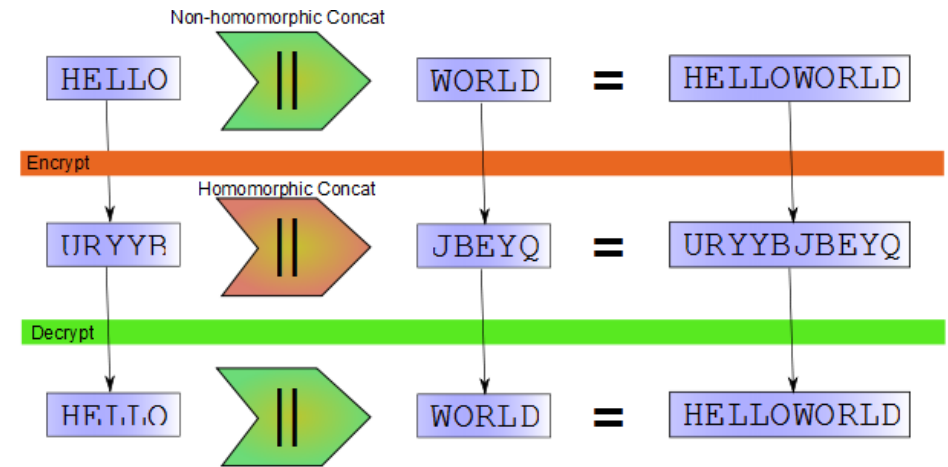
Homomorphic Encryption

An Homomorphic encryption scheme is a way to encrypt data that:

- Allows to perform computations on the encrypted data
- The result of the computation on encrypted data is the encrypted result of the computation on cleartext data

Homomorphic encryption allows to let your data encrypted on cloud provider's premises, letting it perform computations on these encrypted data and then making it possible only for you to decrypt the result of the computation.

In Konfido, homomorphic encryption will be used to manage the ePrescription Summary (ePS).



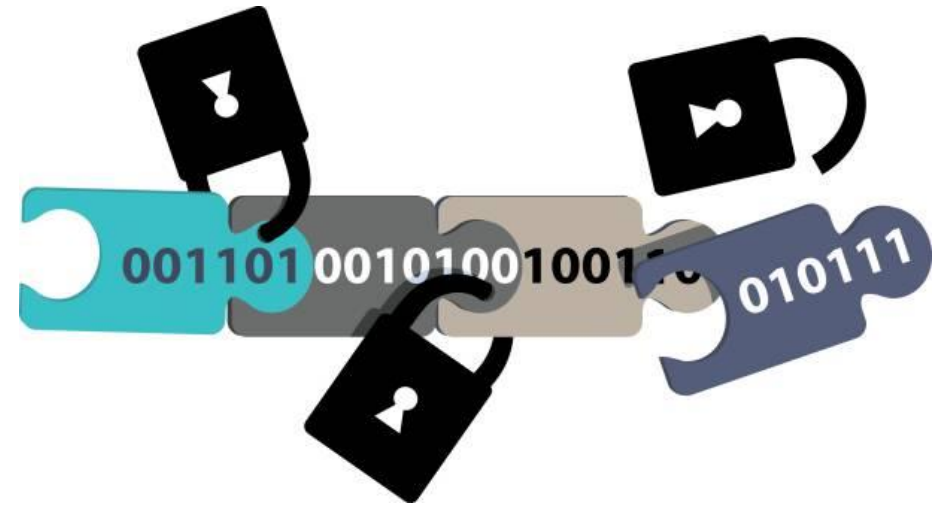
Blockchain based logging

First class actors in OpenNCP are Member States

A Member State requires or provide eHealth data

These two (now) cooperating parties must reach an agreement that the actual request or provision of data has happened

This kind of information will be stored on a permissioned distributed ledger





Konfido status and links

Konfido started on **1st November, 2016**

Now we are entering the design phase, after the domain analysis and the user requirements gathering

Web site: www.konfido-project.eu

[@konfidoproject](https://twitter.com/konfidoproject)

Contact me: **Paolo Campegiani** | pca@bit4id.com



This project has received funding from the European Union's Horizon 2020 Framework Programme for Research and Innovation under grant agreement no 727528.