

Konfido: Secure and Trusted Paradigm for Interoperable eHealth Services

Paolo Campegiani, Bit4id



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

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

CEF Transport: 24,05 BN €

CEF Energy: 5,53 BN €

CEF Telecom: 1,04 BN €

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

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	♥	♥

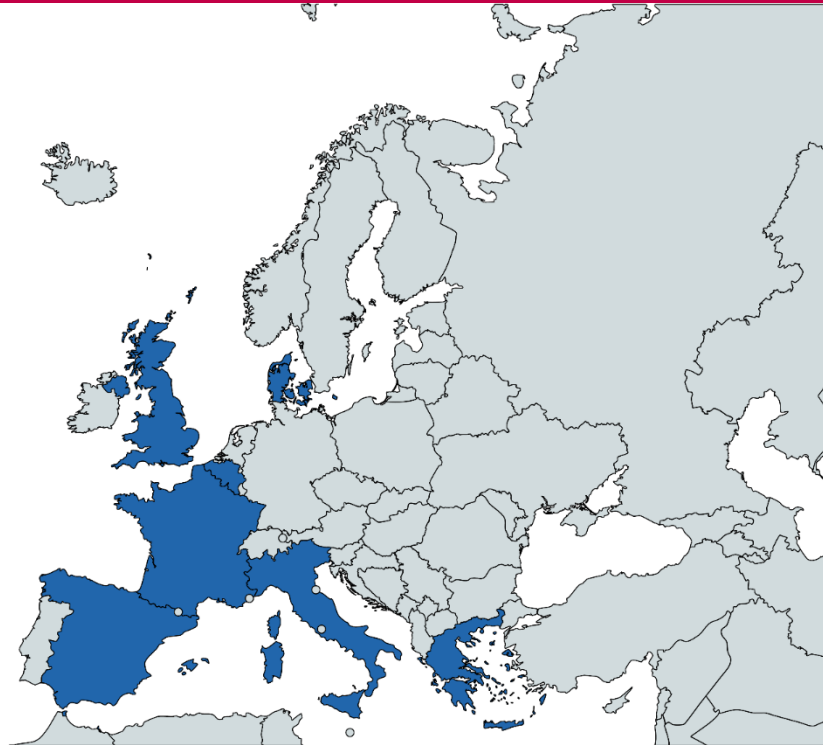
- Horizon 2020 project to advance state-of-the-art eHealth technology and specifically OpenNCP along these dimensions:
 - Digital security
 - Data preservation
 - Data access and modification
 - Data exchange
 - Interoperability
 - Compliance
- Holistic approach:
 - **User centric**
 - Targeting all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

- eHealth users have strong, legitimate views on how they want to do their difficult job
- You have to gain their trust, otherwise they simply don't use the system
- In Konfido users participate from the design phase
- There are three pilots to test the system and raise awareness on OpenNCP

Konfido Partners and Countries

19 **PORVOO GROUP**

25-26 May 2017 Rome, Italy



sundhed.dk



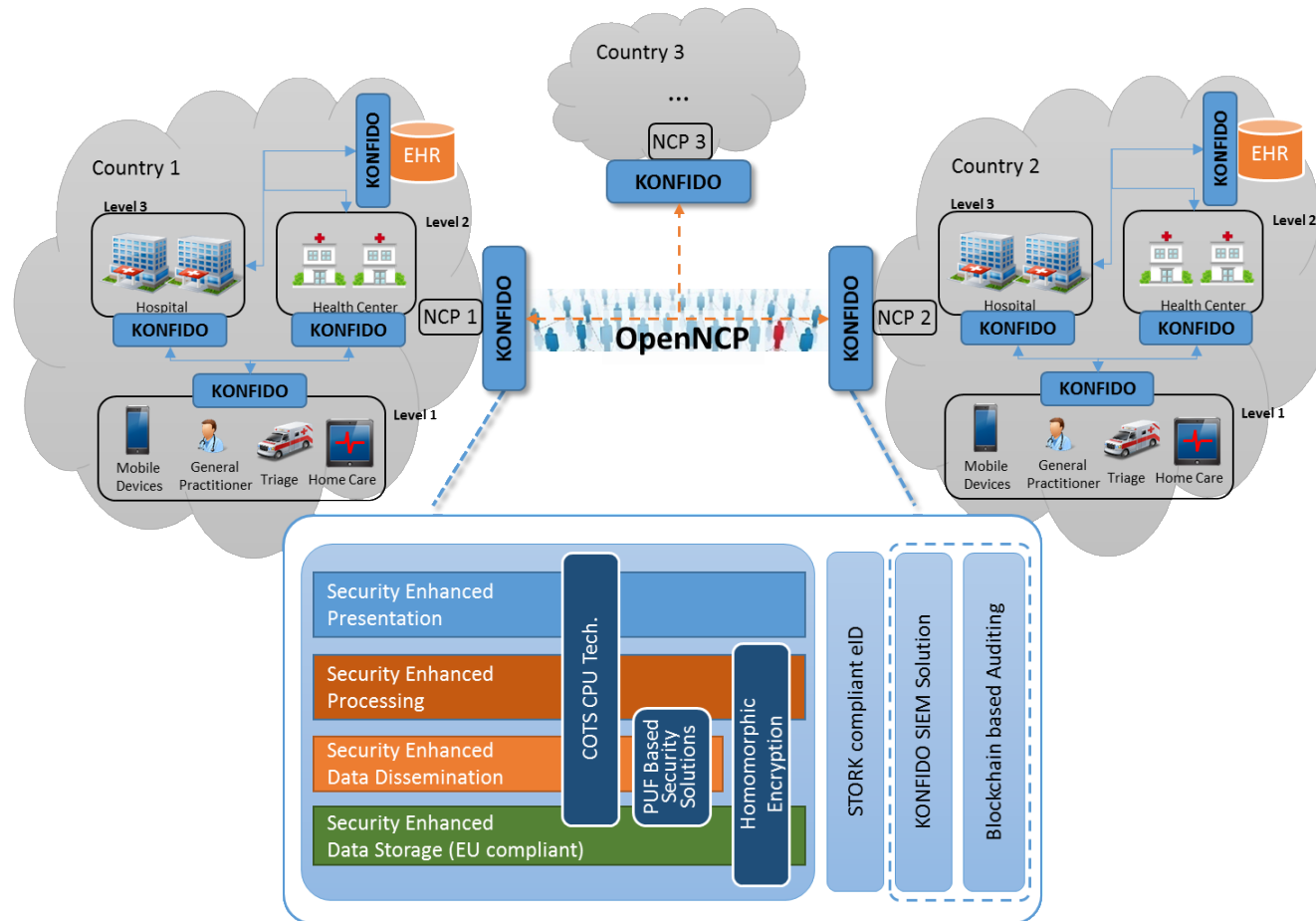
EXUS.INNOVATION



CERTH
CENTRE FOR
RESEARCH &
TECHNOLOGY-HELLAS



Konfido deployment view



Italy

Denmark

Spain

- Users (physicians, nurses, pharmacists) identification
 - Each OpenNCP instance authenticates its users within its national system (no need to use the eID DSI)
 - How we check that a physician is a physician?
 - (National) Attribute Authority?
 - Each OpenNCP instance should trust other instances that the authentication and authorization phases have been performed properly

- Patient identification
 - When it is needed? What if the patient cannot/could not cooperate in the identification phase?
 - The eIDAS unique identifier is used as patient ID number?
 - Yes for some countries (LU, FI, SE, IT?)
 - Not in others (PT, AT) (translation service/attribute authority is needed)

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

Italy:

- Carta Nazionale dei Servizi (smart card)
- Carta d'Identità Elettronica (smart card)
- SPID (server based, but it does not yet provide an high level of assurance)

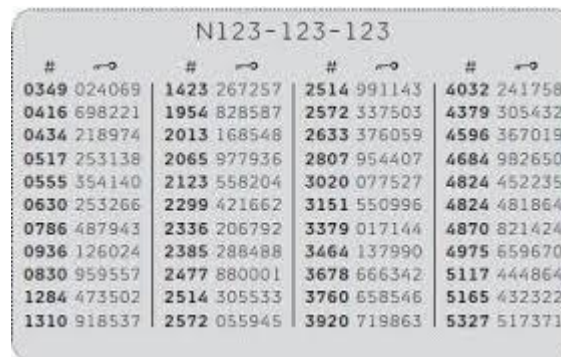
Spain:

- Documento Nacional de Identidad (smart card)
- OCM España: Consejo General de Colegios Oficiales de Médicos de España (smart card)

The first is *issued* to all the citizens, the second is *used* by (almost) all the physicians in Spain working in hospitals

eIDAS means of authentication: Denmark

Denmark uses a combination of user name, password and OTPs arranged on a matrix card



N123-123-123

#	→	#	→	#	→	#	→
0349	024069	1423	267257	2514	991143	4032	241758
0416	698221	1954	828587	2572	337503	4379	305432
0434	218974	2013	168548	2633	376059	4596	367019
0517	253138	2065	977936	2807	954407	4684	982650
0555	354140	2123	558204	3020	077527	4824	452235
0630	253266	2299	421662	3151	550996	4824	481864
0786	487943	2336	206792	3379	017144	4870	821424
0936	126024	2385	288488	3464	137990	4975	659670
0830	959557	2477	880001	3678	666342	5117	444864
1284	473502	2514	305533	3760	658546	5165	432322
1310	918537	2572	055945	3920	719863	5327	517371

Konfido technologies: blockchain based logging

- Country A requires eHealth data for a patient cared for in Country B
- How this two countries could agree now and in the future that an exchange has actually been requested and then performed?
- A blockchain based logging (a distributed ledger) could track all of these business transactions
- Each country could digitally sign its view of the business transaction
- All of these signed transactions are stored inside the ledger

Konfido technologies: Omomorphic Encryption

- Health Data of patient are stored inside a country's eHealth system
- These data will travel outside of the country when a physician request them
- How could the patient be assured that his/her data will be read only by the caring physician, without losing the ability to perform some aggregate statistics?

- A PUF is a way to seed a random number generator using physical defects, intrinsically not reproducible, found in an off the shelf chip
- A physician uses a smartphone to access Konfido system, so she has a lot of possible chips for PUF
- A PUF could be used as an on-the-field provisioning of some kind of digital identity

- OpenNCP lacks a SIEM that, analyzing the different logs produced by the system, could create an ongoing view of the system, to understand what's happening and if some kind of attack is taking place

- The security of the key is the security of the system
- Using a smart card as a key store for an online service brings in some operational problems (e.g. Who will enter the PIN?)
- Intel is developing Software Guard Extensions
 - Enclaves (regions of memory) that are protected from accessing from OS and hypervisor, could be used to store and compute with a private key

- Web site: www.konfido-project.eu
- @konfidoproject
- Why don't you join the Project Advisory Board?
eID experts are more than welcome!
- For more info: pca@bit4id.com