KONFIDO

KONFIDO means “trust” in Esperanto

Increasing digital security of health related data on a systemic level

Luigi Romano
University of Naples “Parthenope”

71th Meeting of the IFIP 10.4 Working Group
on Dependability and Security
Queenstown, New Zealand - January 26-30, 2017

Problem statement

- Ideally, EU citizens should be guaranteed uniform QoS of health care
- Uniform here means:
  - Does not depend on the specific country of origin
  - Does not depend on the specific country of (possibly temporary) stay
- Potentially, this can be enabled by ehealth technology
- However, current ehealth technology is hampered by two main limitations:
  - Lack of interoperability
  - Lack of security

Claim of this talk

- Advancements are needed wrt the SOTA of eHealth technology, to provide better security while achieving interoperability
- This requires a holistic approach to security challenges related to protection, processing, transfer, and storage of eHealth data
- Solutions must:
    - Allow independence of individual stakeholders/domains while favouring cooperation
    - Comply to existing solutions and/or standards
    - Build on previous investments/achievements

Challenges

- Develop a **holistic secure solution** for **interoperable eHealth services**
- Consider all stages/layers, namely: **storage, dissemination, processing,** and **presentation**
- Handle **legal**, **privacy,** and **ethical** issues
- Ensure **interoperability** and **scalability**
- Build on **existing solutions (OpenNCP, STORK, etc.)**
- **Commercially** exploit the outcomes

Innovation Pillars

1st Pillar: Enhancement of the trust and security of interoperable eHealth services

2nd Pillar: Continuous validation and Proof of concept demonstrations

3rd Pillar: Focus on stakeholders, improving user acceptance, adhering to standards and legal and ethical directives

Technology pillars

- 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 secure 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 **STORK compliant eID infrastructure**

Organization of the European ehealth infrastructure - 1

- Each country has its own federated architecture, where individual local governments that are relatively independent of each other coexist and cooperate (to some extent)

- Multiple regions can cooperate to provide health services at a national level

- This results in a first level of hierarchy already at the national level

- No standard solutions exist that are widely accepted

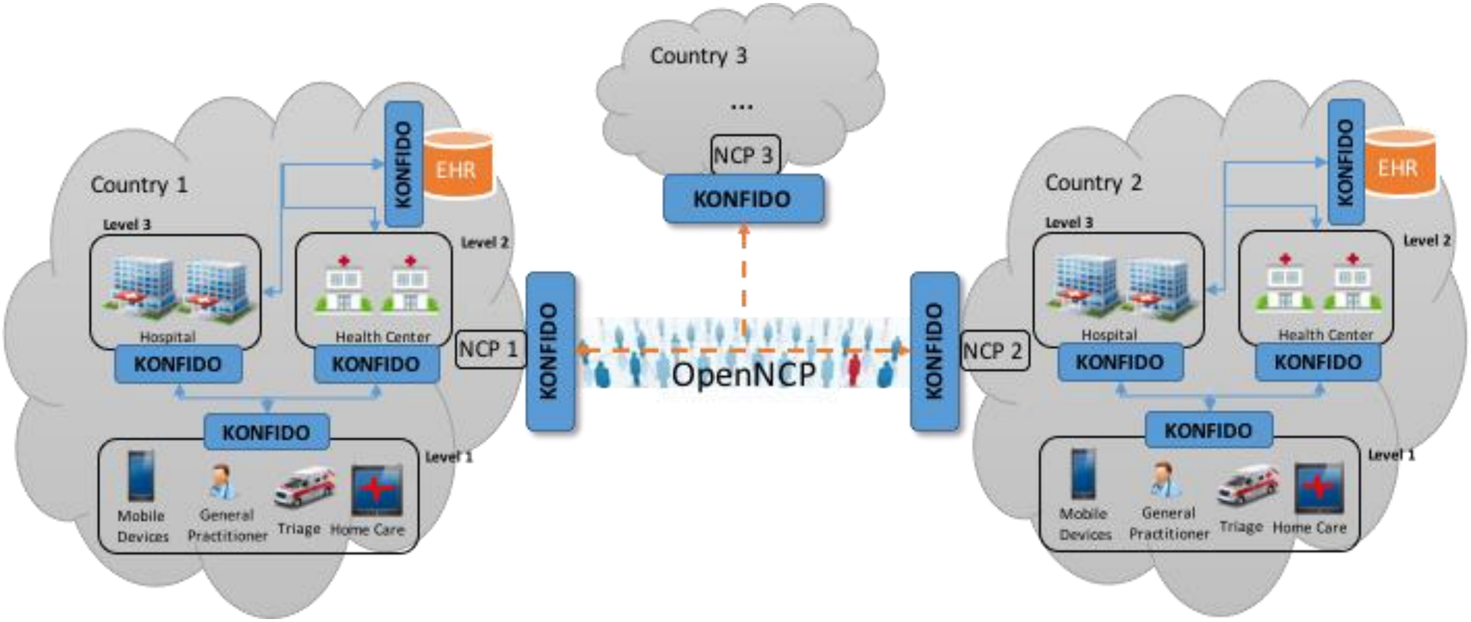
Organization of the European ehealth infrastructure - 2

- Multiple countries can then cooperate – through their National Contact Points (NCPs) - to provide health services at the European level
- This creates a second level of hierarchy
- Such a complex organization has challenging interoperability and security requirements (focus of the talk will be on security)
- Some standard solutions are emerging, e.g. OpenNCP and STORK
- Currently, the interoperation of information systems of individual countries is characterized by a security level that is not sufficient
- This prevents the real take up of integrated ehealth services at the EU level

Requirements/constraints

- Must comply to existing standards and build upon common frameworks - such as Electronic Health Record (EHR) and ePrescription - to ensure interoperable operation particularly in support of cross-border eHealth services
- Must take into account legal requirements in order to meet relevant legal developments both at the EU and at the national level
- For user authentication must exploit customized eID solutions compliant to STORK specifications, as well as satisfying the new requirements that might possibly result from future evolutions of EU regulations and directives
- Must fulfil all requirements imposed by current and upcoming European and national legal frameworks with regard to personal data protection and patients’ rights

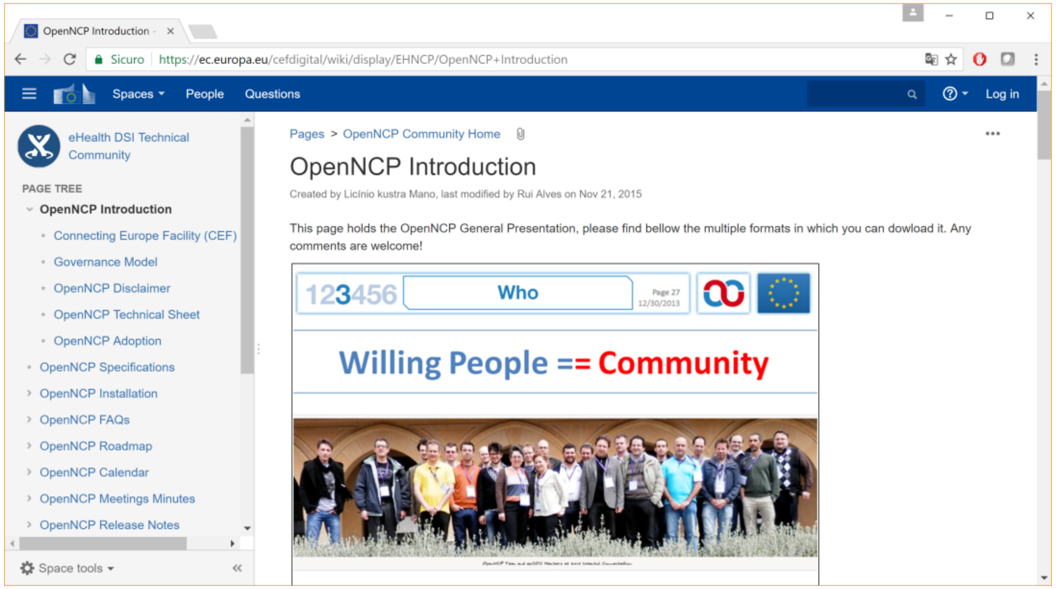
KONFIDO conceptual architecture



- KONFIDO is interposed between the National Contact Point (NCP) of the participating countries and the OpenNCP infrastructure
- By doing so, the information systems of individual countries can interoperate in a secure way
- Multiple countries can cooperate to provide health services using KONFIDO and OpenNCP to implement a federated organization

OpenNCP

- **Vision:**
  - ...design and develop a set of Open Source Components (OpenNCP) that can be adopted by Participating Nations (PNs), to build their local implementation of the National Contact Point (NCP)
- **Definition:**
  - “epSOS NCP software publicly available under Open Source licensing”

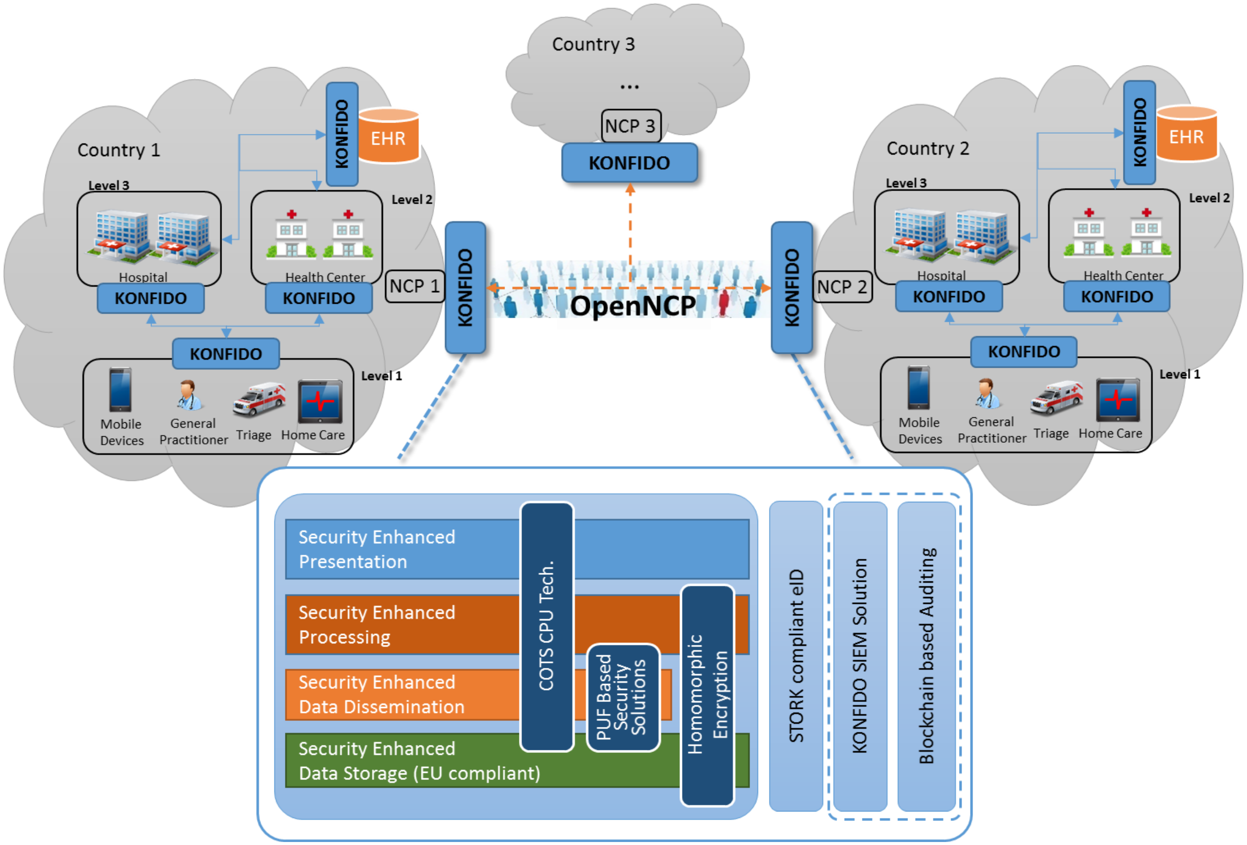


OpenNCP Introduction

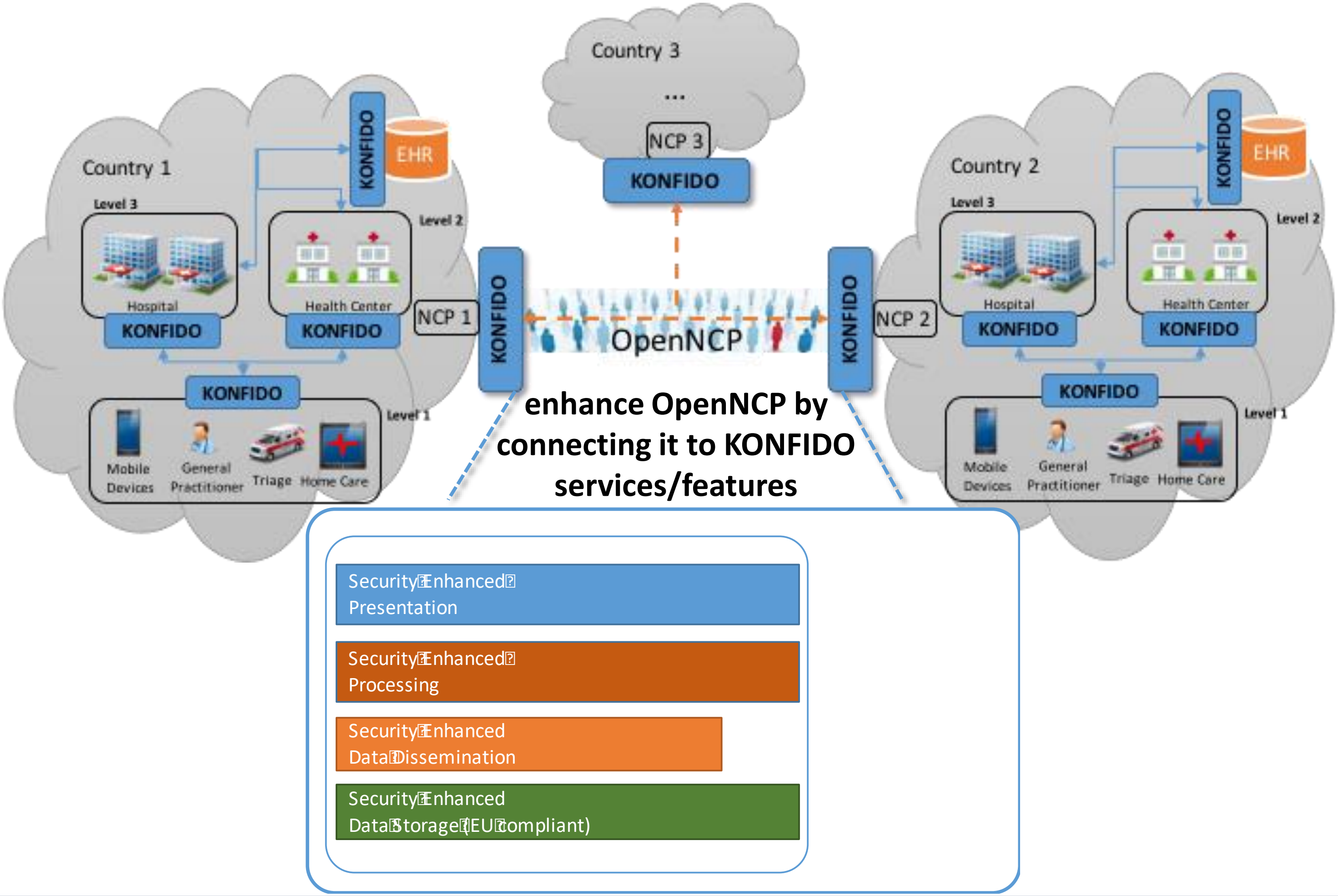
Created by Licínio kustra Mano, last modified by Rui Alves on Nov 21, 2015

This page holds the OpenNCP General Presentation, please find bellow the multiple formats in which you can dowload it. Any comments are welcome!

KONFIDO conceptual architecture



KONFIDO conceptual architecture



enhance OpenNCP by connecting it to KONFIDO services/features

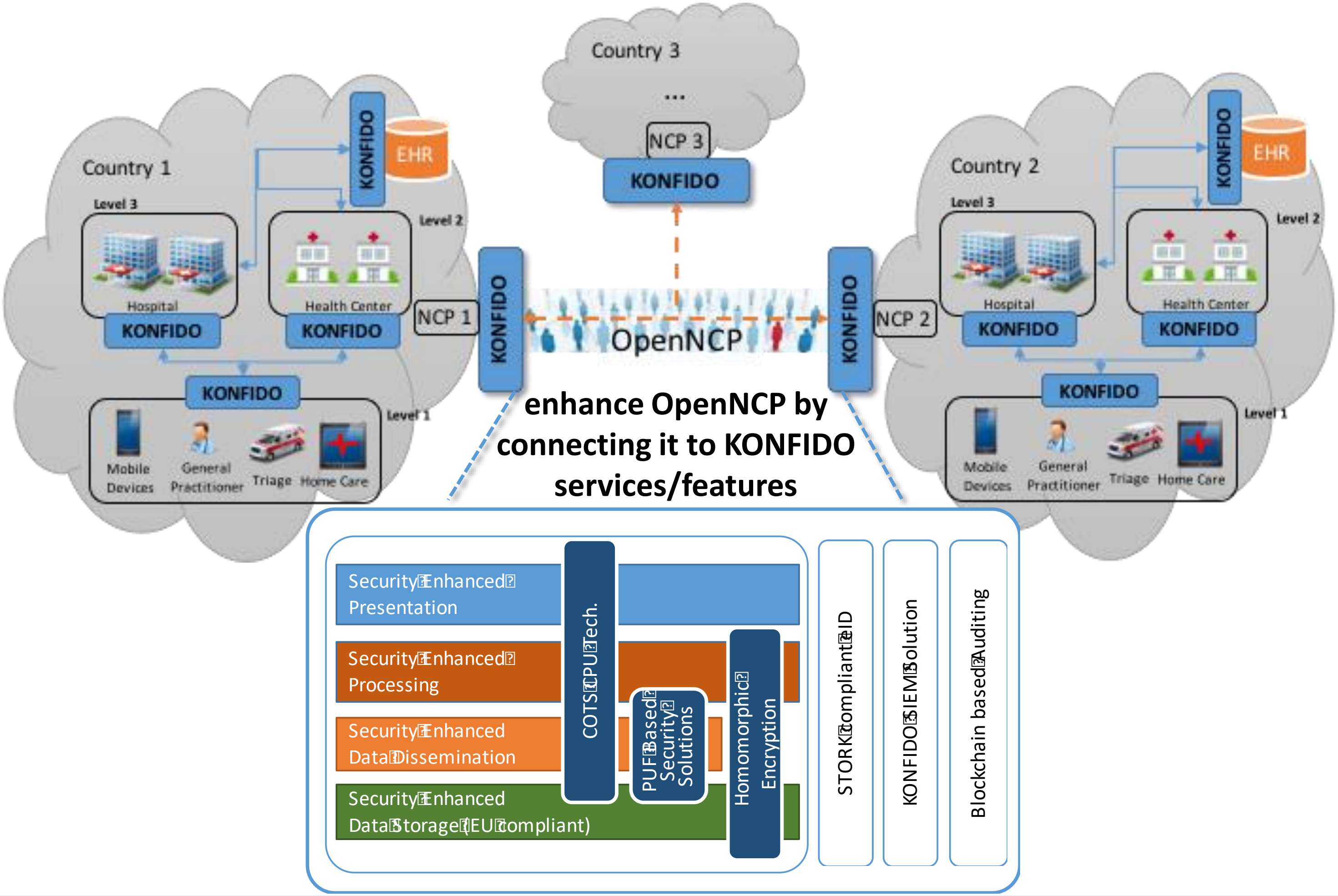
Security-Enhanced Presentation

Security-Enhanced Processing

Security-Enhanced Data Dissemination

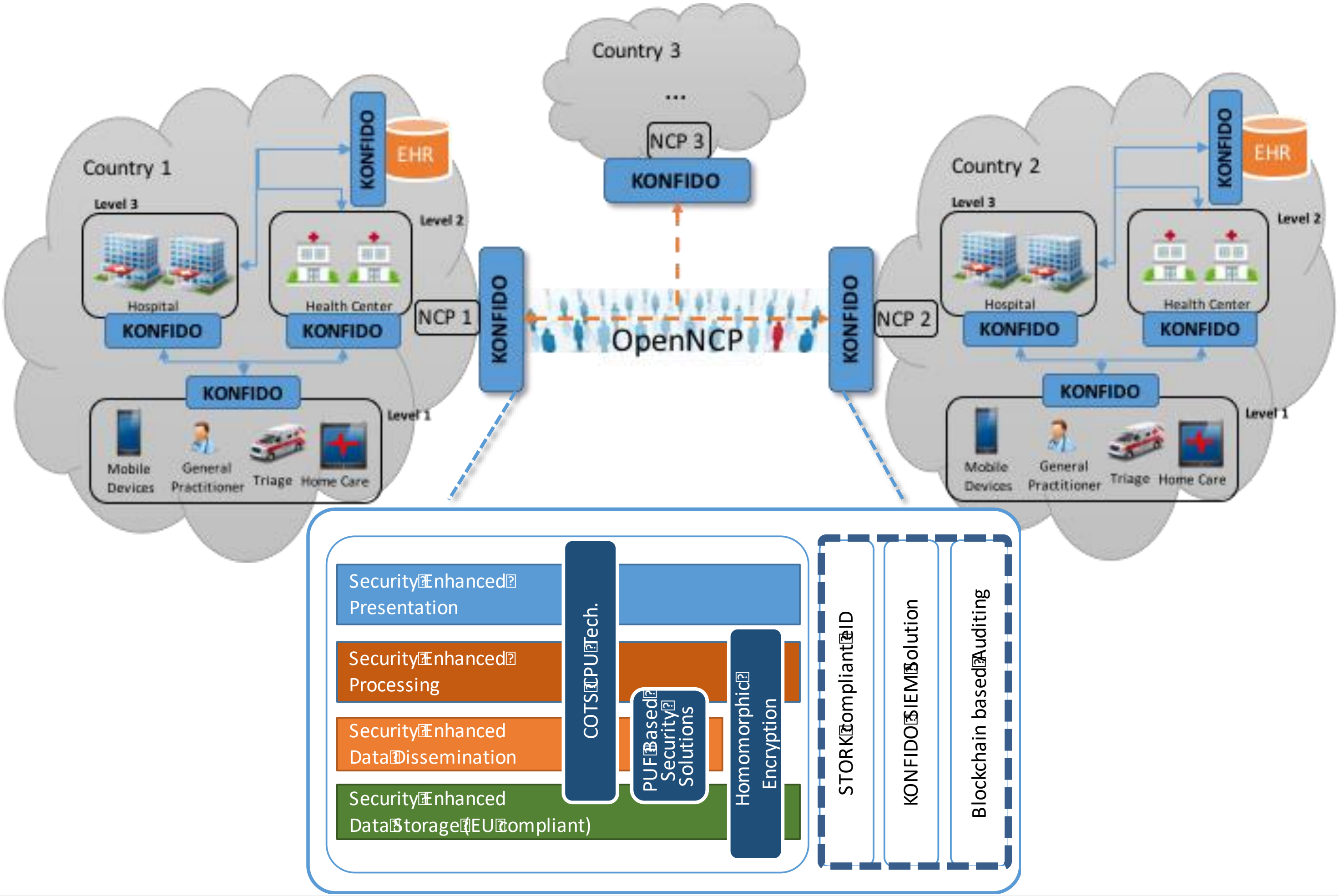
Security-Enhanced Data Storage (EU compliant)

KONFIDO conceptual architecture

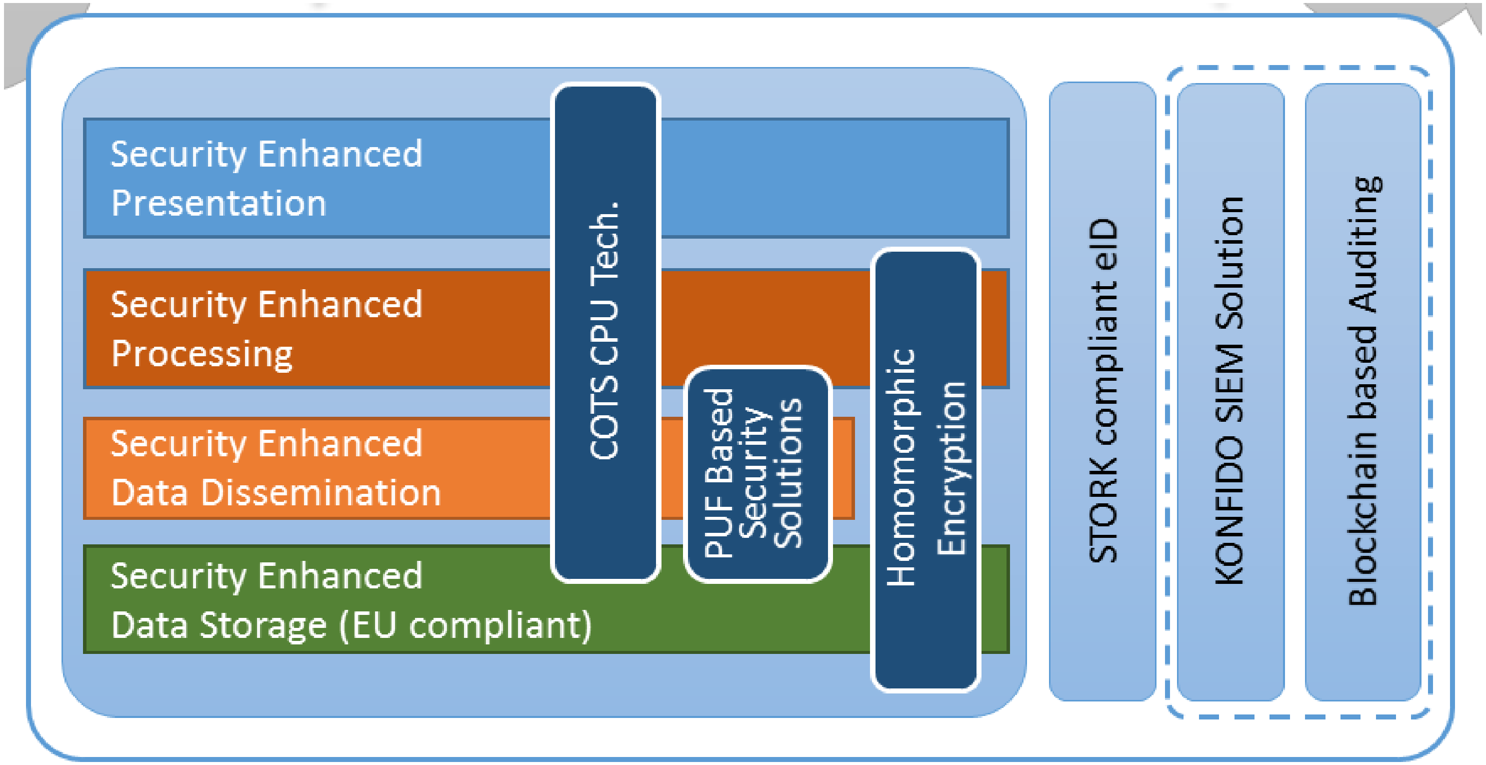


enhance OpenNCP by connecting it to KONFIDO services/features

KONFIDO conceptual architecture



Main KONFIDO components/layers


Security Enhanced Presentation
Security Enhanced Processing
Security Enhanced Data Dissemination
Security Enhanced Data Storage (EU compliant)
COTS CPU Tech.
PUF Based Security Solutions
Homomorphic Encryption
STORK compliant eID
KONFIDO SIEM Solution
Blockchain based Auditing

Use of secure CPU technology

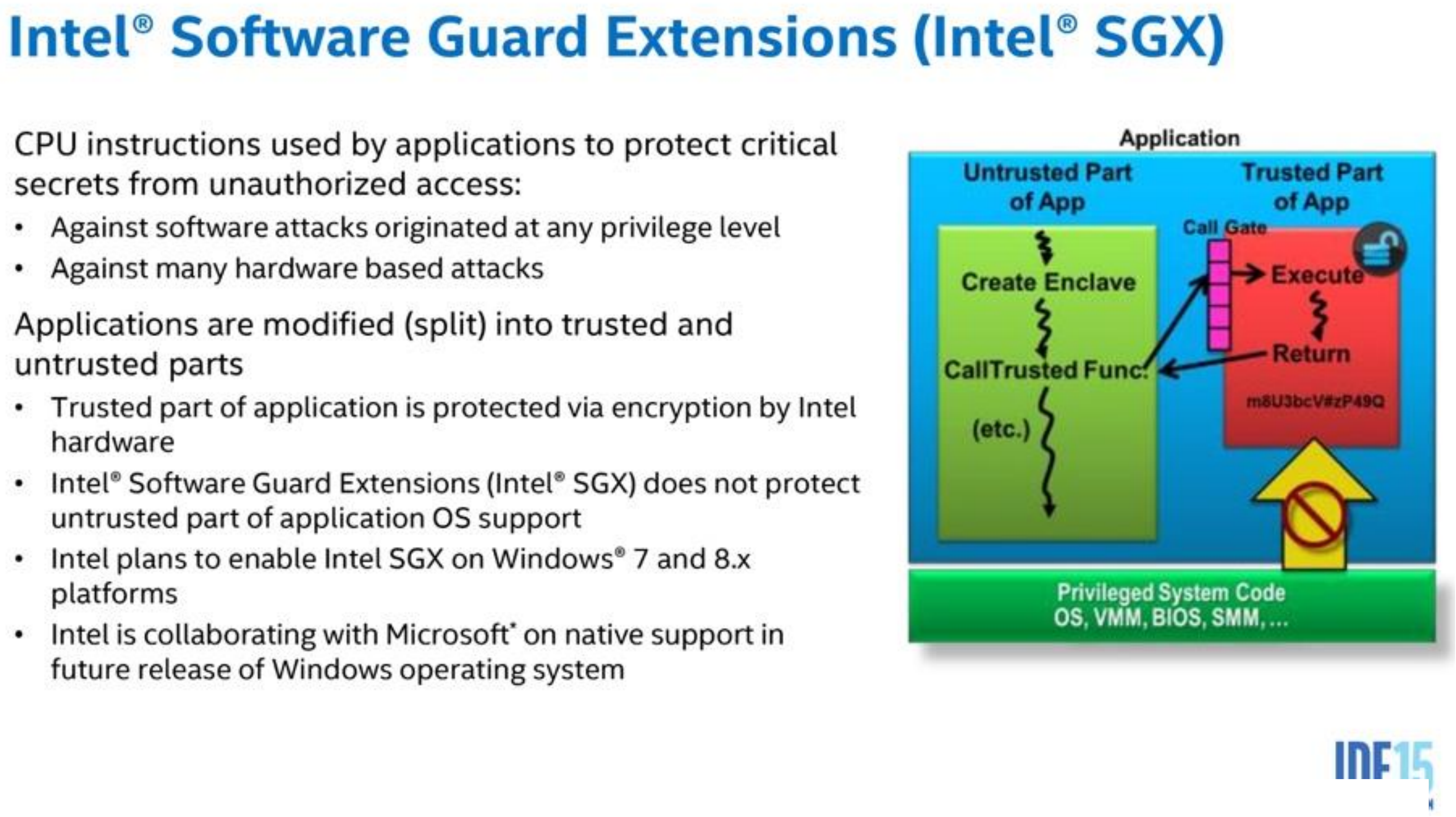
- Exploit the new security features that are being made available by major CPU vendors (notably, ARM and Intel) for creating execution environments that will be protected from attacks launched at multiple architectural levels, even by privileged software (e.g. the Operating System or the Hypervisor), or privileged users (e.g. the System Administrator or the Cloud Provider)
- CPU hardware security features will be integrated in the OpenNCP reference implementation, to provide:
  - Remote integrity attestation of the destination federated domain
  - Protection of delivered sensitive data in spite of the actual security conditions of the receiving system
- Protected execution environments will be created that exploit the new security extensions of COTS CPUs for use by eHealth applications

SOTA of Secure COTS CPU Technologies

Secure CPU hardware is already available and in growing use across a number of domains, including embedded systems, smartcards, and the military

Nowadays it has become popular even in commodity processors such as mainstream Intel CPUs, in the form of Intel Secure Guard Extensions (SGX) [16], as it was already on ARM TrustZone [17] CPUs.

[16] https://software.intel.com/en-us/blogs/2013/09/26/protecting-application-secrets-with-intel-sgx
[17] http://www.arm.com/products/processors/technologies/trustzone



Intel® Software Guard Extensions (Intel® SGX)

CPU instructions used by applications to protect critical secrets from unauthorized access:

- Against software attacks originated at any privilege level
- Against many hardware based attacks

Applications are modified (split) into trusted and untrusted parts

- Trusted part of application is protected via encryption by Intel hardware
- Intel® Software Guard Extensions (Intel® SGX) does not protect untrusted part of application OS support
- Intel plans to enable Intel SGX on Windows® 7 and 8.x platforms
- Intel is collaborating with Microsoft* on native support in future release of Windows operating system

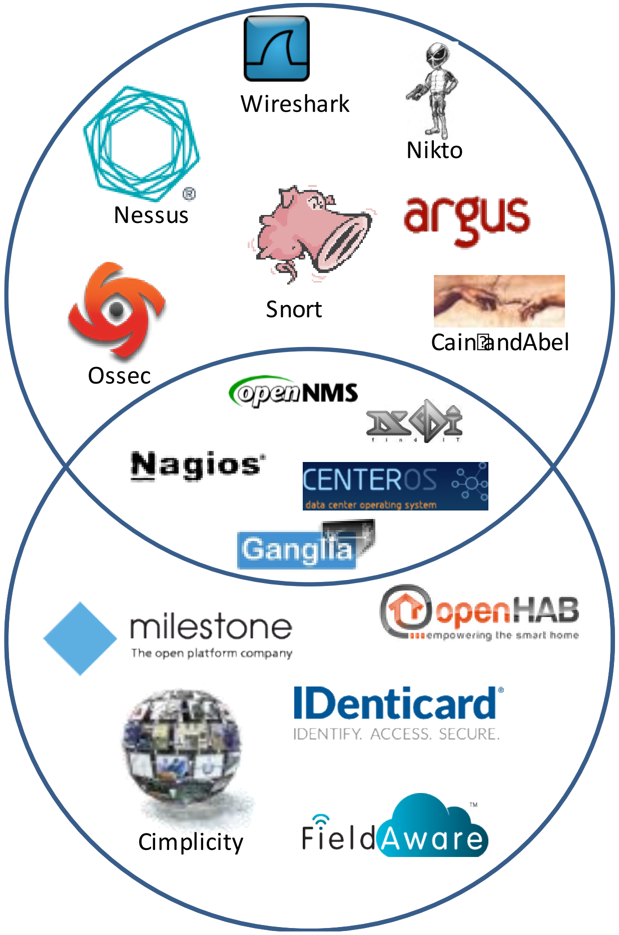
SIEM solutions customized for eHealth applications

Extend selected existing SIEM solutions, and customize them based on the specific requirements of a federated environment compliant to the OpenNCP model

Solutions will be tailored to the healthcare, and in particular they will:

1) *Support sophisticated authentication and delegation mechanisms*
2) *Detection potential threats and anomalies*
3) *Inclusion comprehensive and intuitive (visual) analytics*
4) *Support for of a variety of mitigation strategies*

Security Information and Event Management (SIEM)

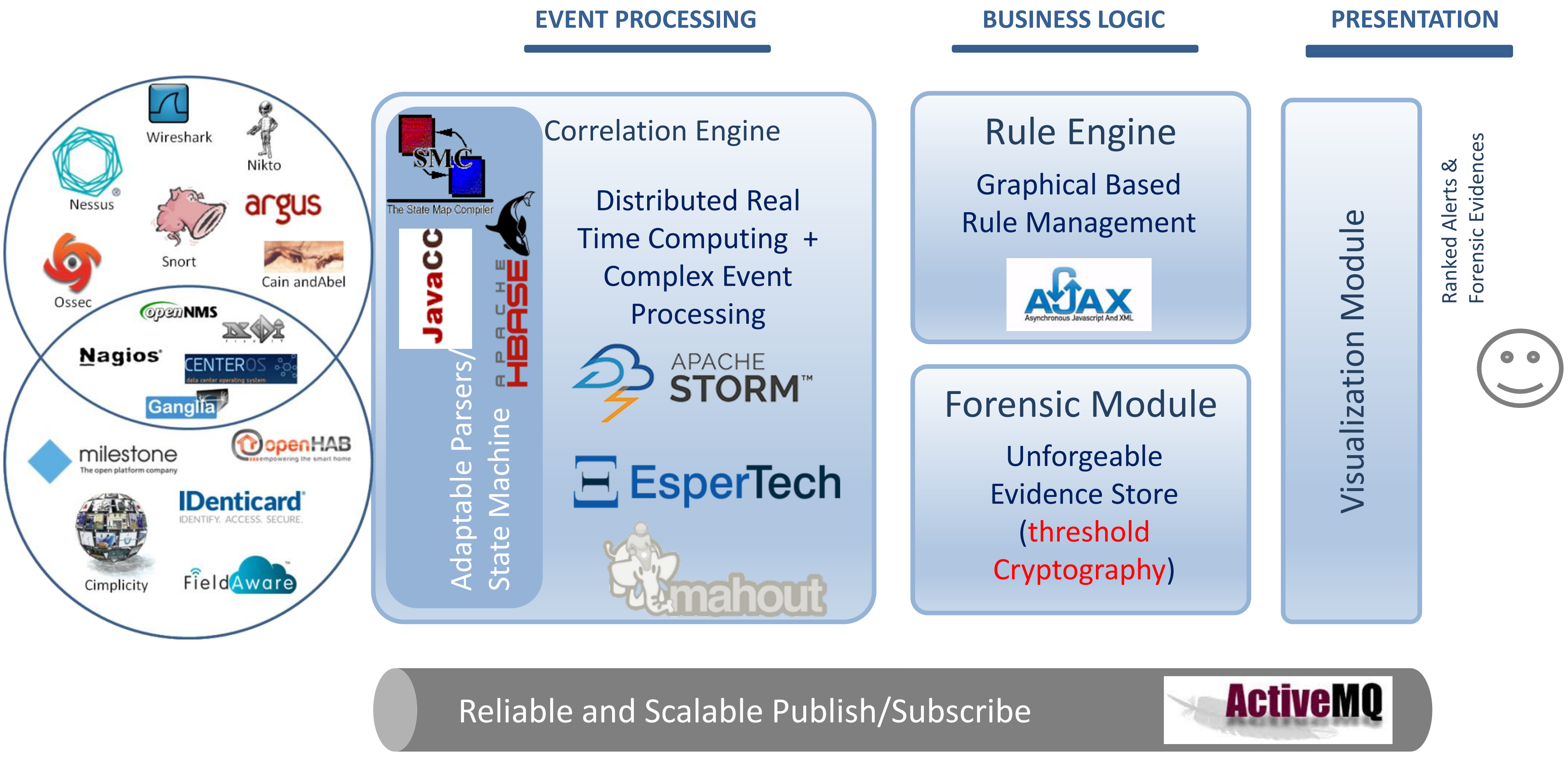


Logical World System and Security Monitoring

+

Physical World System and Security Monitoring

Building blocks of the proposed Solution



EVENT PROCESSING

BUSINESS LOGIC

PRESENTATION

Adaptable Parsers/ State Machine

Correlation Engine

Distributed Real Time Computing + Complex Event Processing

Rule Engine

Graphical Based Rule Management

Forensic Module

Unforgeable Evidence Store (threshold Cryptography)

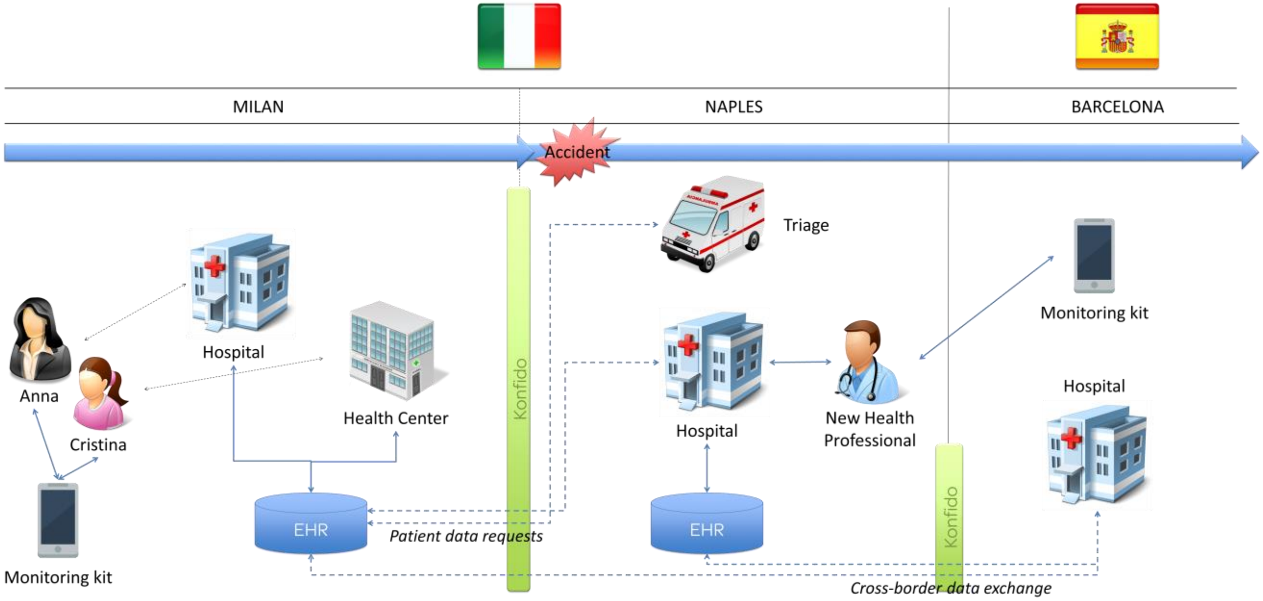
Visualization Module

Ranked Alerts & Forensic Evidences

Reliable and Scalable Publish/Subscribe

Use case scenario: Secure cross-region and cross-border mobility for patient empowerment

- A patient is discharged from a hospital in her home town
- She has a car accident in a different city (but in the same country)
- She receives treatment for a few days
- She leaves for vacation towards a foreign country

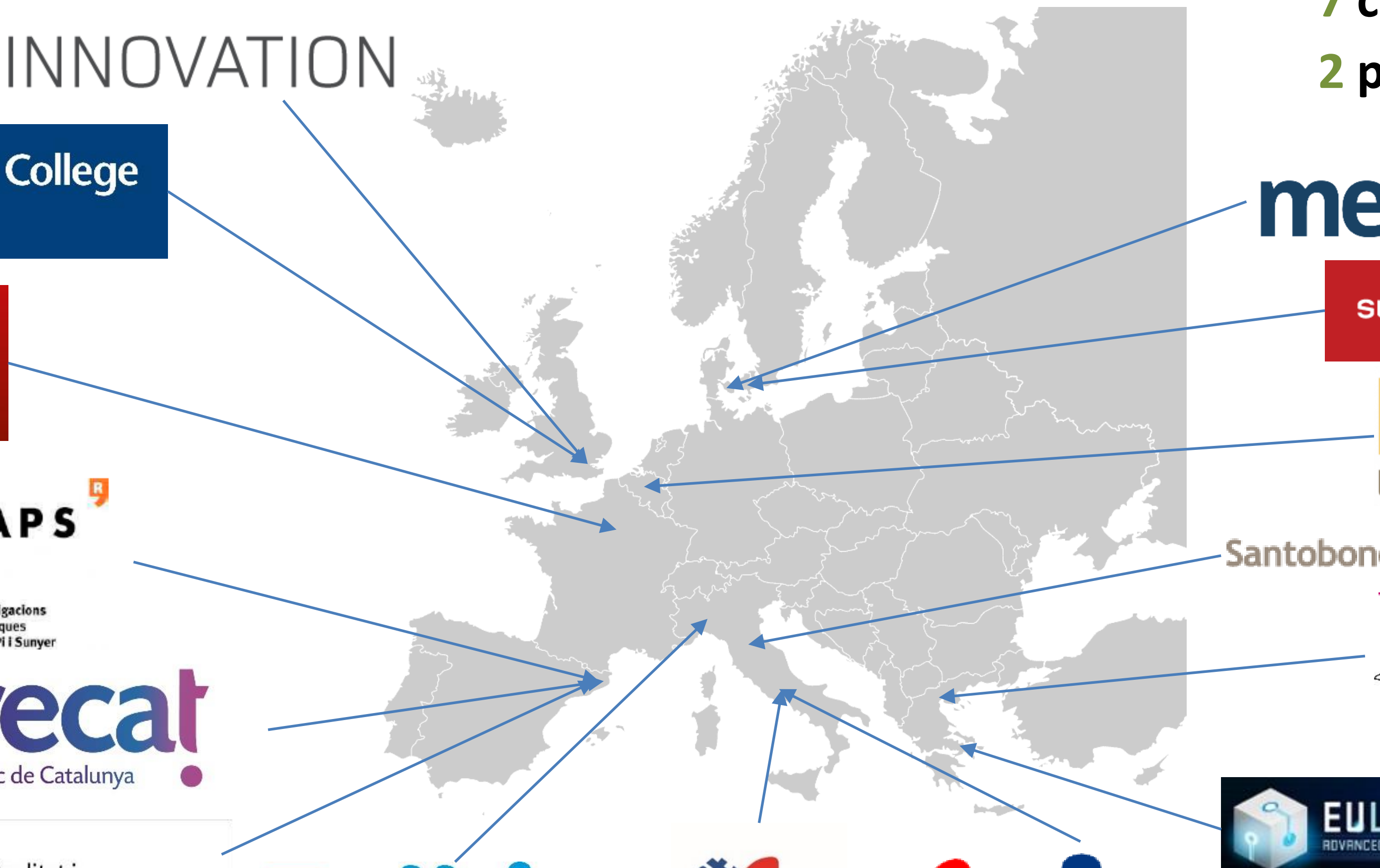


Consortium

15 partners

7 countries

2 pilots



EXUS INNOVATION

Imperial College London

FROM RESEARCH TO INDUSTRY cea

IDIBAPS Institut D'Investigacions Biomèdiques August Pi i Sunyer

eurecat Centre Tecnològic de Catalunya

Agència de Qualitat i Avaluació Sanitàries de Catalunya AGENCY FOR HEALTH QUALITY AND ASSESSMENT OF CATALONIA

Telbios

bit4id

cini consorzio interuniversitario nazionale per l'informatica

medcom

sundhed.dk

time.lex

Santobono Pausilipon fondazione

EULAMBIA ADVANCED TECHNOLOGIES LTD

Thank you for your attention

Luigi Romano
KONFIDO Technical Coordinator
prof.luigi.romano@gmail.com
+39 333 301 68 17

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

Partners
EXUS (Coordinator), CERTH, CINI, CEA, TLX, EULAMB, TLB, EURECAT, MEDCOM, ICL, BIT4ID, PAUSIL, SUNDHED, AQUAS, IDIBAPS