Secure Cross-Border eHealth Data Exchange in EU: the KONFIDO Project

Luigi Coppolino

13th TAROT Summer School
Naples, Italy
June 30th, 2017
# TABLE OF CONTENTS

1. Intro to EHR and interoperability issues
2. Cross Border EU level eHealth data exchange
3. The KONFIDO Project
4. Technology Pillars
5. The KONFIDO Solution
# TABLE OF CONTENTS

1. Intro to EHR and interoperability issues
2. Cross Border EU level eHealth data exchange
3. The KONFIDO Project
4. Technology Pillars
5. The KONFIDO Solution
The growing of electronic Health Services: Electronic Medical Record
The growing of electronic Health Services: Electronic Medical Record

DICOM  ANSI X12
HL7     SDMX-HD
CDA     EDIFACT
CCD     ASTM
IXF     ...

13th TAROT Summer School
Thursday, 29 June 2017
TABLE OF CONTENTS

1. Intro to EHR and interoperability issues
2. Cross Border EU level eHealth data exchange
3. The KONFIDO Project
4. Technology Pillars
5. The KONFIDO Solution
Cooperation is the key

Oh so you are also implementing eHealth?
The epSOS Project

• **Smart Open Services for European Patient**
• **Duration:** **6 Years** (epSOS I & II) (2008 - 2013)
• **Goal:** **to develop a practical eHealth framework and ICT infrastructure**, based on existing national infrastructures, that enables secure access to patient health information, particularly with respect to a basic **Patient Summary** and **ePrescription**, between European healthcare systems.
General information about the patient

Most important clinical patient data

Current medications
ePrescription: A prescription for medicines or treatments, provided in electronic format.
Pillars for eHealth Interoperability in EU

• **Existing national healthcare infrastructures / legislation remain unchanged**
  - Member States are reluctant to accept impositions on their own legislation
  - Call for interoperability between legislations
  - Easiness of implementation

• **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
    - It is guaranteed about the enforcement of the security policy in the other MS by the signature of the National Contact Point (NCP)

• **Information is exchanged but not shared. Any epSOS user (HCP(O)) MAY NOT modify an original document from abroad. The user retrieves a «read - only» document.**
Cross-Border eHealth Data Retrieval

- Country B should be aware
  - of data formats and protocols of every country A
  - of the national infrastructure of every country A
  - of regulations of every country A
The epSOS Mediated Approach
The epSOS Mediated Approach

NCP in charge of:
- Interacting with the other NCPs
- Pivoting documents
- Encode the pivoted document in the national structure
- Interact with the NI
The Circle of Trust

Country B

Country A

epSOS Circle of Trust

National Circle of Trust

National Circle of Trust

13th TAROT Summer School

Thursday, 29 June 2017
Retrieve Operation: from Country A
Retrieve Operation: to Country B

HCP in MS - B

- Medical data (CTR-B)
  - Signature verification
  - Decryption
  - Medical data (CTR-B)
  - NCP-B

NCP - B

- Pivoting
- Authorized med. data (epSOS)
- Access Control Authorization
- HCP Assertion
- Laws of MS - B

- Medical data (CTR-B)
  - Signature
  - Signature verification
  - Decryption
  - Medical data (CTR-B)
  - NCP-B
  - Med. data (epSOS + CTR-A)
  - NCP-A

- Medical data (epSOS + CTR-A)
  - NCP-A

13th TAROT Summer School
1. Intro to EHR and interoperability issues
2. Cross Border EU level eHealth data exchange
3. The KONFIDO Project
4. Technology Pillars
5. The KONFIDO Solution
100 million EHR accessed by hackers in 2015

48 NHS Trusts affected by the ramsonware WannaCry in May 2017
100 million EHR accessed by hackers in 2015. 48 NHS Trusts affected by the ransomware WannaCry in May 2017.
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 pretended 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
TOPIC: Increasing digital security of health related data on a systemic level

<table>
<thead>
<tr>
<th>Topic identifier:</th>
<th>DS-03-2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publication date:</td>
<td>14 October 2015</td>
</tr>
<tr>
<td>Types of action:</td>
<td>RIA Research and Innovation action</td>
</tr>
<tr>
<td>Deadline Model:</td>
<td>single-stage</td>
</tr>
<tr>
<td>Opening date:</td>
<td>20 October 2015</td>
</tr>
<tr>
<td>Deadline:</td>
<td>16 February 2016 17:00:00</td>
</tr>
<tr>
<td>Time Zone:</td>
<td>(Brussels time)</td>
</tr>
</tbody>
</table>

Horizon 2020
Pillar: Societal Challenges
Work Programme Year: H2020-2016-2017
Work Programme Part: Secure societies – Protecting freedom and security of Europe and its citizens
Call: H2020-DS-2016-2017

Call budget overview

H2020 website
TOPIC: Increasing digital security of health related data on a systemic level

**Specific Challenge:**

Full implication of different private and public actors, as well as empowered citizens, is needed in order to unlock eHealth potential in Europe. To achieve the trust of users, measures of safety have to be taken into consideration in accordance with the "privacy by design" approach. This requires secure storage of information including personal data but also guaranteeing safe exchange of these data over a number of architectures of differing security levels preventing unauthorised access, loss of data and cyber-attacks. A systemic approach to security will increase patients' empowerment, help protect their health also while abroad, and possibly encourage a larger number of Member States to apply it and adapt national legislations.
Project Summary

- KONFIDO - Secure and Trusted Paradigm for Interoperable eHealth Services
- Grant Agreement No: 727528
- Start Date: 01/11/2016
- Duration: 36 Months
- www.konfido-project.eu
KONFIDO Consortium
KONFIDO Vision

- Advance the state of the art of eHealth technology by providing a holistic approach to address the challenges of:
  - Secure storage and protection of eHealth data
  - Protection and control over personal data
  - Security of health related data gathered by mobile devices

KONFIDO is an integrated security solution!
Conceptual view of KONFIDO architecture
Conceptual view of KONFIDO architecture

- Security Enhanced Presentation
- HW Assisted Security
- Security Enhanced Processing
- PUF Based Security Solutions
- Security Enhanced Data Dissemination
- Homomorphic Encryption
- Security Enhanced Data Storage (EU compliant)
- STORK compliant eID
- KONFIDO SIEM Solution
- Blockchain based Auditing
TABLE OF CONTENTS

1. Intro to EHR and interoperability issues
2. Cross Border EU level eHealth data exchange
3. The KONFIDO Project
4. Technology Pillars
5. The KONFIDO Solution
Traditional trust Model:
Is it Trustworthy?

![Diagram showing the relationship between APP, Protected Mode, Attack, Exploit, and Vulnerability]
Trusted Execution Environment (Intel SGX)

Application splitted in:
- **Trusted and Untrusted parts**
- App runs & creates **enclave** which is placed in trusted memory
- **Only** code running inside enclave sees data in clear

**Application**

- **Untrusted Part of App**
  - Create Enclave
  - CallTrusted Func.
  - (etc.)

- **Trusted Part of App**
  - Call Gate
  - Execute
  - Return

Privileged System Code, OS, VMM, BIOS, SMM, ...
Memory Snooping Attacks

Data stay encrypted within the enclave
Before leaving the enclave
data are encrypted with a Seal key provided by the processor

SGX provides a Remote Attestation mechanism to verify authenticity and integrity of the Enclave before data provisioning
Physically Unclonable Function (PUF)
Physically Unclonable Function (PUF)

- A Physically Unclonable Function (PUF) is an hardware device who produces a repeatable output given an input, but the output is unpredictable.
- The input is in general a physical stimulus.
- PUFs reach truly unclonability by:
  - Physical unclonability
    - Each device reacts to the stimulus in a way depending from its microstructure, and the microstructure is not replicable even with the same production process and materials.
  - Mathematical unclonability
    - It is unfeasible to compute the output given the input and other input – output pairs, without knowing all the details of the microstructure of the PUF.
PUF Examples

- DRAM PUF
- SRAM PUF
- FPGA PUF (Anderson PUF)
- Delay PUF
- Optical PUF
- Photonic PUF
**PUF Uses**

- Strong cryptographic keys requires random seed to be generated
- PUFs can be employed as **True Random Number Generators (TRNG)** to derive secure keys
- Particularly suitable to generate private keys
  - No need to deliver the private key
  - Simply generate and share the corresponding private key
- Symmetric keys can also be derived, but they require a secure channel to be delivered to the communicating parties
  - A solution is a *keychain* at the server
- PUFs can also be employed as an authentication mean for the device
Homomorphic Encryption
Data Privacy

- Standard cryptography requires that data is decrypted before working on it
- There are situations where it is desirable to work on data without decrypting it first
  - When computation is offloaded to a third party facility, it is desirable to not disclose sensitive data to the facility owner
  - This is the case of cloud computing
  - Or to perform analysis on medical data without violating the patients’ privacy
Homomorphic Encryption made easy

![Diagram](image-url)
Homomorphic Encryption

• A cryptosystem is **homomorphic** w.r.t. an operation $\otimes$ iff $D(\mathcal{E}(a) \otimes \mathcal{E}(b)) = a \otimes b$ or equivalently $\mathcal{E}(a) \otimes \mathcal{E}(b) = \mathcal{E}(a \otimes b)$

• **RSA** and **ElGamal** cryptosystem are homomorphic w.r.t. the multiplication

• **Pallier** is additively homomorphic

• A cryptosystem is **fully homomorphic** if it is homomorphic $\forall \otimes$
Homomorphic Encryption made easy
Homomorphic Encryption Limitations

• Spatial Overhead: in a somewhat Homomorphic Encryption with a good level of security: 1 bit -> 1 Kb

• Temporal Overhead: strongly depends on data size and key length
TABLE OF CONTENTS

1. Intro to EHR and interoperability issues
2. Cross Border EU level eHealth data exchange
3. The KONFIDO Project
4. Technology Pillars
5. The KONFIDO Solution
OpenNCP data exchange
DOMAIN TRANSLATION

Country B

NCP-B

Country A

NCP-A

NI
DOMAIN TRANSLATION

Country A

Country B

NCP-B

NCP-A

Attack

NI
DOMAIN TRANSLATION WITH KONFIDO

Country B

NCP-B

Country A

NCP-A

SGX

Enclave

NI
SIEM Service

Country B

NI
sgx enclave

Mutual Remote Attestation

NCP B
sgx enclave

NCP A
spx enclave

... Secure Enclave

Country A

KONFIDO Services

Log chain
eDAS
Homomorphic Processor

KONFIDO Services

Homomorphic Processor
PUF Generator
Log chain
eDAS

SGX homomorphically encrypted hook

SGX hook
REFERENCES

1. www.konfido-project.eu
Thank you!!!

Luigi Coppolino, PhD
FITNESS Research Group
University of Naples Parthenope
Department of Engineering
Mail: luigi.coppolino@gmail.com
Skype: luigi.coppolino (Caserta)
Mob.: +393396218570
Web: www.fitnesslab.eu