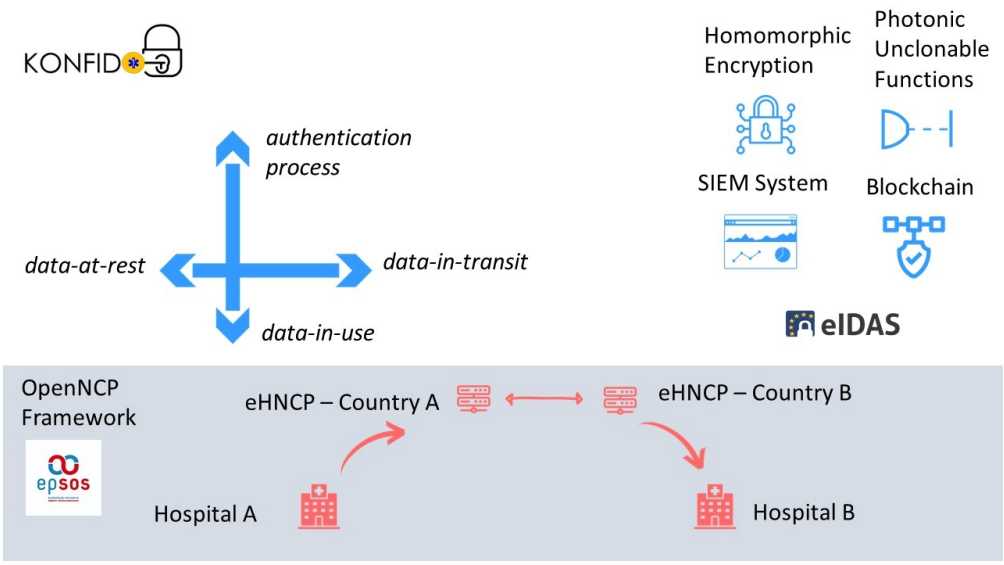
Developing an infrastructure for secure patient summary exchange in the EU context: Lessons learned from the KONFIDO project

Journal:	*Health Informatics Journal*
Manuscript ID	HIJ-20-0321.R1
Manuscript Type:	Original Research Article
Keywords:	Cybersecurity, Interoperability, Health Information Technologies, Cross-border Health Data Exchange, Barriers and Facilitators for HIT Acceptance
Abstract:	Background: The increase of healthcare digitalization comes along with potential information security risks. Thus, the EU H2020 KONFIDO project aimed to provide a toolkit supporting secure cross-border health data exchange. Methods: KONFIDO focused on the so-called "User Goals", while also identifying barriers and facilitators regarding eHealth acceptance. Key user scenarios were elaborated both in terms of threat analysis and legal challenges. Moreover, KONFIDO developed a toolkit aiming to enhance the security of OpenNCP, the reference implementation framework. Results: The main project outcomes are highlighted and the "Lessons Learned", the technical challenges and the EU context are detailed. Conclusions: The main "Lessons Learned" are summarized and a set of recommendations is provided, presenting the position of the KONFIDO consortium towards a robust EU-wide health data exchange infrastructure. To this end, the lack of infrastructure and technical capacity is highlighted, legal and policy challenges are identified and the need to focus on usability and semantic interoperability is emphasized. Regarding technical issues, an emphasis on transparent and standards-based development processes is recommended, especially for landmark software projects. Finally, promoting mentality change and knowledge dissemination is also identified as key step towards the development of secure cross-border health data exchange services.



KONFIDO rationale

338x190mm (96 x 96 DPI)

Developing an infrastructure for secure patient summary exchange in the EU context: Lessons learned from the KONFIDO project

Abstract

Background: The ~~constant~~ increase of healthcare ~~the~~ digitalization ~~of healthcare services~~ comes along with potential information security risks. Thus, the EU H2020 KONFIDO project aimed to provide a toolkit ~~to~~ supporting secure cross-border health data exchange ~~based on innovative technical paradigms~~.

Methods: ~~The project~~KONFIDO focused on the so-called "User Goals", while also identifying ~~a set of B~~barriers and ~~f~~Facilitators regarding eHealth acceptance ~~were identified~~. ~~To this end, k~~Key user scenarios were elaborated both in terms of threat analysis and ~~also regarding~~ legal challenges. ~~On the technical side~~Moreover, KONFIDO developed a toolkit aiming to enhance the security of OpenNCP, the reference implementation framework~~, in terms of information security~~.

Results: The main project outcomes are highlighted and~~,~~ ~~focusing on the technical solution provided by KONFIDO. Furthermore,~~ the "Lessons Learned" ~~based on end-user inputs~~, the technical challenges and the EU context are detailed.

Conclusions: The main "Lessons Learned" are summarized and a set of recommendations ~~are~~ is provided, ~~to present~~presenting the position of the KONFIDO consortium ~~regarding~~ towards a robust EU-wide health data exchange infrastructure. To this end, the lack of infrastructure and technical capacity is highlighted, legal and policy challenges are identified and the need to focus on usability and semantic interoperability is emphasized. Regarding technical issues, an emphasis on transparent and standards-based development processes is recommended, especially for landmark software projects. Finally, promoting mentality change and knowledge dissemination is also identified as key step towards the development of secure cross-border health data exchange services.

Keywords: Cybersecurity; Interoperability; Health Information Technologies; Cross-border Health Data Exchange; Barriers and Facilitators for HIT Acceptance.

Background

Digital applications in healthcare, typically referred as Health Information Technologies (HIT) are transforming healthcare delivery. This increased use of electronic applications and distributed services in the context of healthcare, almost inevitably includes the use of sensitive data and therefore increases the information security risks. A series of prominent information security incidents in the healthcare industry highlight the need to enhance the security measures both regarding technical and also policy aspects, as these failures clearly undermine the provided services' quality and result in patients' and healthcare providers' (HCPs) unwillingness to adopt HIT.

In the European context and especially in European Union (EU) countries, the number of citizens who travel for work, education, training, and tourism constantly increases, and creates the need for cross-border health data exchange. Citizens are also seeking scheduled care abroad for reasons related to price or availability of (more) specialized health services, as the reimbursement of healthcare costs for scheduled care abroad has become easier in Europe as a consequence of the European patient mobility directive of 2011. Typically, travelling citizens can be hospitalized or treated in the EU country visited. However, the lack of healthcare data access from their home country, i.e. the medical history in the form of a Patient Summary (PS) document could significantly hinder the quality of the healthcare services that are provided leading to potential health risks and/or cost increase.

Moreover, the recent COVID-19 pandemic has clearly shown that cross-border health data exchange should be revisited as it could be a significant technical tool in the context of the EU-wide COVID-19 response. A secure and robust cross-border health data exchange framework could be useful in the process of (at least partially) preventing horizontal lockdowns between countries, enabling people to travel based on their personal medical background (e.g. based on their personal lab test results etc.) and in a safer manner as they would have access to their personal medical records in case of hospitalization needed. Such an approach could be an asset in the effort to reduce COVID-19 prevalence and could have a significant impact on huge sectors of the economy (e.g. tourism industry, aviation industry) reducing the financial burden. Furthermore, the ability to access personal medical history in a EU level could enhance the healthcare quality in the case of a visiting person hospitalized due to COVID-19. To this end, cross-border health data exchange on a personal basis could be considered one of the ways to restore "normality" in terms of travelling across Europe, in the context of COVID-19 or other future epidemics.

KONFIDO is a recently completed project [1] aiming to develop a technical toolkit supporting secure, cross-border health data exchange among European countries. Technologically, KONFIDO solution was based on modern technical paradigms, such as photonic Physical Unclonable Functions (p-PUF) [2], blockchain-based auditing [3], homomorphic encryption [4], and the deployment of a Security Information and Event Management (SIEM) system [5].

One of the main KONFIDO goals was to align with existing or under development European Union (EU) infrastructure (EHDSI) and therefore it built its solution upon OpenNCP [6], i.e. the reference open-source software implementation of OpenNCP standard developed to support the interoperable communication of the so-called National eHealth Contact Points (eHNCPs). OpenNCP was developed in the context of epSOS (European Partners – Smart Open Services) [7] which has also developed the

reference Patient Summary (PS) template used to exchange patient information among EU countries. More recently, in 2013, the eHealth Network adopted its guidelines on a minimum patient summary dataset[1]. Furthermore, eIDAS (electronic IDentification, Authentication and trust Services) [8] was used as the main user identification infrastructure, as eIDAS is part of the EU regulation on electronic identification and trust services for electronic transactions. An overview of the KONFIDO technical solution and its links with the abovementioned frameworks is presented in [9].

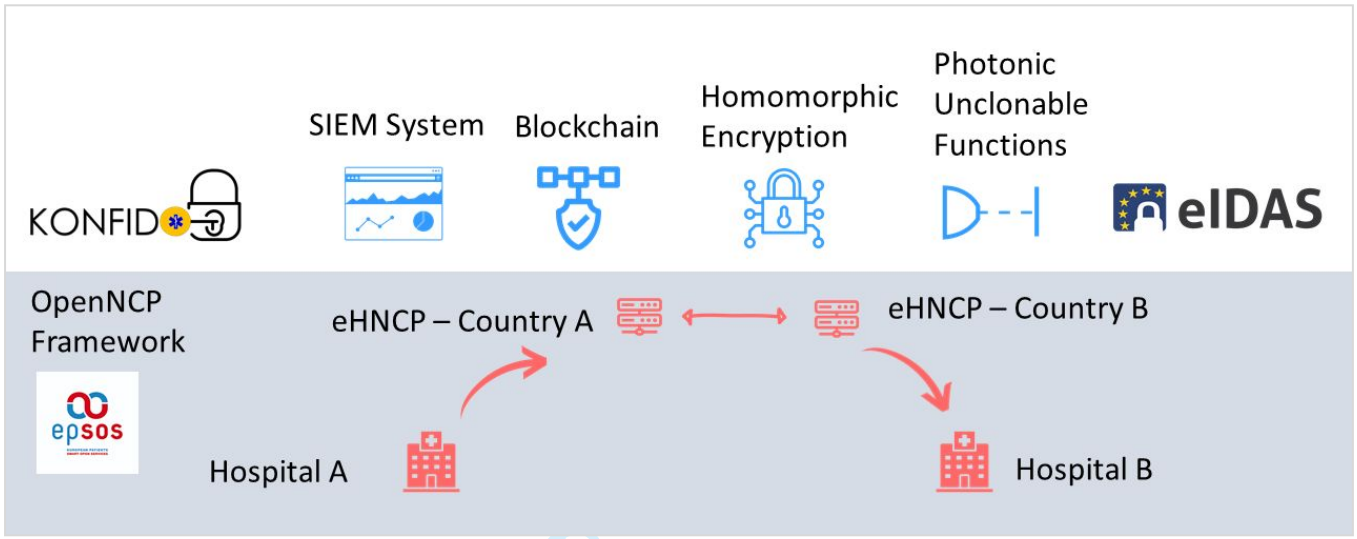


Figure 1: KONFIDO rationale

In this paper, we provide ~~an~~ a high-level overview ~~of the achievements~~ of the KONFIDO project, and we also provide insights regarding the ongoing challenges, with an emphasis on technical and policy aspects, engaging a wide variety of stakeholders. Finally, we highlight some "Lessons Learned" and provide recommendations that elaborate on the authors' position towards the development of EU-wide cross-border health data exchange framework.

Methods

~~KONFIDO was organized in four complementary phases, namely, 'User requirements analysis'; 'Design'; 'Technology development'; and 'Integration, testing and validation'.~~

Elaboration of end user, policy and strategical issues

Elaborating on the end user needs, the respective policies and the best practices along EU initiatives was one of the main objectives of KONFIDO. As part of the KONFIDO "User requirements analysis" phase [10][11], technical and legal frameworks as well as ethical and social norms at the European level were reviewed emphasizing on the project's pilot-site countries (i.e. Denmark, Italy and Spain). This process included a gap analysis of the respective initiatives and the analysis of user scenarios focusing on both cross-border and inter-regional health data exchange. Based on this analysis, the underlying Business Processes (BPs) were elaborated in the context of a threat analysis to identify respective assets, threats and, ultimately, define high-level user goals regarding cross-border health data exchange. On the other hand, the KONFIDO consortium actively pursued interaction with the

[1] https://ec.europa.eu/health/sites/health/files/ehealth/docs/guidelines_patient_summary_en.pdf

wider healthcare community, aiming to identify the key facilitators and barriers for the acceptance of HIT solutions linked to cybersecurity. To this end, an online survey targeting all possible relevant stakeholders (i.e. Health Care Professionals - HCPs, hospital staff at IT departments, industrial HIT stakeholders, and patients/citizens) was conducted, as well as an end-user Workshop.

On another perspective related with the end-user needs, ethical and legal aspects regarding cross-border health data exchange were thoroughly investigated. For example, the aspects of the protection of personal/sensitive health data, the patient's consent, trust, equity and accessibility were highlighted as key ethical issues. The complex landscape of ethics issues was outlined using a comprehensive framework as KONFIDO was committed on an 'ethics by design' approach [12]. From a legal and policy point of view the KONFIDO consortium continuously kept an eye on the activities of the eHealth Network, the first implementations of the EHDSI in the Member States and the work performed in JASeHN (Joint Action Supporting the eHealth Network.) As far as possible the progress made in the framework of the eHMSEG (eHealth Member States Expert Group)[2] Legal Taskforce has been followed up, e.g. with regard to the legal agreement between national authorities[3] on the criteria required for the participation in cross-border eHealth information services under the GDPR.

Furthermore, the KONFIDO consortium established communication channels with selected stakeholders across Europe (e.g. ENISA[4] and AgID[5]) to obtain useful insights on a wider technical or policy level and important feedback focusing on the practicability of the implemented approaches.

Technical approach

The KONFIDO technical solution focused on the improvement of the security of the OpenNCP framework via a set of advanced and non-invasive hardening solutions. Based on the respective threat analysis, the KONFIDO "hardening" mechanisms focused on:

- the *data-in-transit* among distributed eHNCP brokers against code-injection or denial of service attacks leveraging a privacy-preserving SIEM system that ensured the non-disclosure of patients' sensitive data and the respect of countries' regulations
- the *data-at-rest* in eHNCP servers (e.g., sensitive logs) using a blockchain-enabled auditing solution
- the *data-in-use* in the eHNCP hosting machines using technologies like TEE, PUF, and HE to enable a protected eHealth data processing
- the *authentication* of users to the system via an eIDAS-compliant access control.

As OpenNCP is a framework under development and therefore not yet fully stable, the KONFIDO consortium decided to apply a "loose coupling" approach, to avoid binding with a specific version of OpenNCP which could be obsolete in the near future, resulting to a "moving-target" problem. To this end, the KONFIDO technical solution was architecturally based on a "toolkit" approach, where each component would be developed independently of OpenNCP developments in order to be able to be

[2] https://ec.europa.eu/cefdigital/wiki/display/EHMSEG/eHDSI+MS+Expert+Community+Home
[3]
[4] http://enisa.europa.eu
[5] http://agid.gov.it

used in a stand-alone fashion, also implementing specific interfaces to integrate with OpenNCP infrastructure.

Emphasizing the crucial role of end-user authentication, the KONFIDO technical solution has been based on the framework established by the eIDAS regulation [13]. eIDAS enables a European citizen to use a digital identity issued in his/her home country, for accessing digital public services provided by other European Union Member States. From this perspective, eIDAS is also relevant for the services related with the so-called eHealth Digital Service Infrastructure (eHDSI), aiming to support citizens when they are abroad and need to access a healthcare service from their temporary country of stay and not from their country of origin.

The KONFIDO toolkit, was validated as a whole during a pilot test upon a simulated integration of national healthcare infrastructures with the eHNCPs of Italy, Spain and Denmark, enabling the systematic test against the "malicious use cases" defined during the conducted threat analysis [14].

~~Apart from the technical solution aiming to harden the OpenNCP framework, in terms of basic research, the KONFIDO project also developed "behavioural" models using agent-based modelling and Finite State Machines (FSMs) to simulate potential malicious behaviours and their impact.~~

Results

End user, policy and strategic issues

~~As part of its user requirements engineering phase, KONFIDO consortium~~Based on the above, ~~identified~~ a set of barriers and facilitators regarding the adoption of HIT have been identified, also based on the various stakeholders' input [15]. To this end, the results of the respective online survey engaging responders from 14 European countries [16] and the results of the gap analysis have been published [17]. Finally, a number of challenges and a potential roadmap towards the adoption of cloud as the main infrastructure technical paradigms were also elaborated in [11], based on the BPs, the threats identified as part of the respective *threat analysis* process and the finally defined *User Goals.* During this process *usability* was identified as a first-class priority based on end-user input and the need to focus also on *semantic interoperability* beyond the syntactic compatibility of information exchange was highlighted. Furthermore, the need for a horizontal *mentality* improvement was identified, along all aspects of healthcare processes towards an overall information security culture.

Regarding the analysis conducted based on the respective ethical analysis framework defined in the context of KONFIDO, a key conclusion was that responsibility for confidentiality cannot be shifted completely to the technology as technical measures could not replace organisational and policy related measures [12][18]. To this end, in order to reinforce the *autonomy* principle, an Informed Consent process has been elaborated emphasizing on information about the service and processing of patients' personal data. Moreover, along the *proportionality* principle, it was clearly defined that the health data should be deleted after their use in the context of their original use purpose. Finally, it was concluded that the *accountability* principle could be relatively easily enforced via technical measures (e.g. the use of blockchain enhanced auditing mechanism developed as part of the KONFIDO toolkit).

From a legal perspective, the cross-border exchange of patient summaries must take into account the provisions of Regulation (EU) 2016/679 and of national data protection and health law. Sharing a patient summary between healthcare providers, whether or not established in different countries, can be legally mandatory in one country (like, for example, in Denmark) but may be illegal without previous written consent of the patient in another country (for example in Italy). Moreover, the rules on who has access to a patient summary and under which conditions, are very divergent among Member States. National requirements regarding technical and organisational security measures to be implemented when exchanging health data are not harmonised. Finally, KONFIDO also looked at the specific legal issues related to the implementation of the European eHDSI initiative, such as the roles of data controllers and data processors, the duties of the actors involved and their liabilities.

Technical component developments

~~It should be clarified that KONFIDO results (e.g. software components, or legal documents etc.) have not been published online in full detail due to complicated intellectual privacy issues. However, they could be available upon requests.~~

Trusted Execution Environment (TEE) component

The Trusted Execution Environment (TEE) component was based on the new Intel's CPU extension, namely *Software Guard Extension (SGX)*, and it was adopted to ~~ensure security along the following three axes:~~

~~A. the TEE provided protection to the OpenNCP software module responsible for clinical data transformation procedures (i.e., the *Transformation Manager*) against privileged attackers such as a malicious employee trying to steal~~handle sensitive information from clinical documents~~. In this regard,~~ in terms of ~~the cross-border functionalities of~~ translating and transcoding HL7 Clinical Document Architecture (CDA)~~-~~based information in SGX aiming to protect them against privileged attackers (e.g. a malicious employee~~ were both moved in a secure memory area, inaccessible to unauthorized users.)~~. Furthermore, SGX was used

~~B. In the second case, the SGX technology was used to set up a TEE-terminated TLS channel between eHNCPs in order to protect the communication protocol from key-stealing attacks.~~

~~C.~~ ~~Last but not least, TEE ensured the integrity of the eHNCP software endpoints as before allowing the transmission of CDA documents from one country to another the *remote attestation* mechanism of the SGX technology was employed to verify the validity~~to validate ~~of~~ the eHNCP software running in the TEE, ensuring that no malwares were added.

Security Information and Event Management (SIEM) component

The KONFIDO Security Information and Event Management (SIEM) extended already existing technical components in a ~~solutions, by customizing them on the specific requirements of a~~ federated ~~sensitive environment compliant to the OpenNCP model. Applying SIEM solutions to a federated eHealth system, such as the one addressed by the KONFIDO project, posed a number of challenges and required the development of ad-hoc solutions~~monitoring system aiming to detect "suspicious" network traffic patterns in a timely fashion and provide useful insights via advanced analytics. ~~First of all, the lack of an individual owner of the overall infrastructure required that the KONFIDO SIEM~~

guaranteed the appropriate level of confidentiality. The implemented KONFIDO SIEM was able to analyze information and events collected at different granularity levels of the monitored system to discover possible ongoing attacks, or anomalous situations, with an ultimate goal to ensure data privacy via an extensive user analytics graphical suite, providing warnings for dangerous network traffic patterns. Furthermore, KONFIDO SIEM component used HE provided by HE component ensuring data privacy when identifying potential "risky" data components exchanged.

Homomorphic Encryption (HE) component

KONFIDO Homomorphic Encryption (HE) component was utilized as part of the SIEM functionality. More specifically, typical SIEM operators (e.g., join, count, sum) and analytics were adapted to be used in HE-protected realm. Via the use of these HE-enhanced operators, KONFIDO SIEM enabled the protection against code injection attacks (i.e. from malicious code injected in sensitive CDA fields), while also leveraging HE to protect sensitive content from unauthorized access, based on .

The homomorphic encryption technology was also used to provide an alternative solution to the TEE-based cross-over functionalities of translating PS data. As such, with minimal changes to the OpenNCP framework, it is possible to protect the sensitive patient information, not only during its transmission but also during its treatment by the OpenNCP Transformation Manager module. The blind translation of PS via homomorphic encryption and using Cingulata[6] crypto-compiler can ensure thus protection against threats on the eHNCP either from attackers or unauthorized users.

Photonic Physical Unclonable Functions (p-PUF) component

Most encryption processes are heavily based on the use of "strong" keys, i.e. long numbers, which are used to identify persons or various system actors. In the KONFIDO context, the photonic Physical Unclonable Functions (p-PUF) component was used in order to provide strong unbreakable keys used as input to the HE module.

eIDAS component

In the context of KONFIDO toolkit validation phase, the simulated eHDSI infrastructure has been extended to allow for the eIDAS Authentication of the citizens (note that healthcare practitioners are identified inside their home country, so although they are possibly using eIDAS compliant authentication means, the eIDAS Network per se is not involved in the authentication process).

Blockchain component

The KONFIDO project has designed and implemented a blockchain based permissioned logging system [19] that is only accessible from the respective eHNCPs. Sensitive data in this system are encrypted in such a way that each country participating in an exchange of health data (either being the requester or the giver) could decrypt them autonomously from the other, while other countries cannot decrypt these data. The overall availability of the blockchain is provided by its redundancy as it is replicated among many (possibly all) the participating countries, while privacy is provided by the aforementioned cryptographic scheme. Each exchange of eHealth data is logged at national level as a series of ATNA events [20], while those that correspond to critical actions (e.g. Patient Informed Consent, Retrieval of Patient Summary, Exchange of Patient Summary etc.) are stored inside the

[6] https://github.com/CEA-LIST/Cingulata

blockchain once encrypted. ~~Due to the inherent properties of blockchain, critical actions are logged in an immutable way allowing for non-repudiation of these actions from the part of the involved stakeholders, even if the corresponding logs are modified or deleted by malicious users who have obtained access to the eHNCP databases.~~

Agent-based modelling

~~As the local access to national or regional nodes, the remote access from local nodes to remote nodes, and the data transfers between different national or remote nodes, are all subject to access controls playing two roles:~~

- ~~They limit potential malicious overload attempts (Denial of Service – DoS attacks) including requests which are not complying with the required protocols,~~
- ~~They insure the security of the request made by the access, both at the local (national or regional node) and at the remote node.~~

The developed agent-based "behavioural" simulation scheme focused on modelling software agents in the form of finite state machines (FSM), where FSM's may be specialized in specific bilateral relations, e.g. the FSM at the France Node that is specialized in data exchanges with the FSM at the Belgium Node.

In addition, a token-based permit system has been introduced, aiming to support the control of flow of unilateral access requests, enabling both the "client" and the "server" nodes the possibility of running attack or anomaly detection methods, and control accesses accordingly. More specifically, both the client and the server nodes can control the flow and throttle or reduce requests classified as part of potential anomaly or attack patterns exploiting advanced queueing network techniques known as G-networks [21] and deep learning [22]. The detailed results of our analysis have been published in recent papers [14] [13].

Lessons learned

Technical integration

One of the key technical activities of the KONFIDO project aimed to integrate the developed technical solution with a federation of different "actors" at Regional, National and European level, with several threats to security and integrity of personal health data that might arise. To this end, two key EU wide infrastructures were part of the KONFIDO integration process, i.e. OpenNCP and eIDAS frameworks:

Integration with OpenNCP

As the KONFIDO pilot infrastructure was built on cloud, a key conclusion was that OpenNCP could be used as a valid eHNCP connector with national eHealth infrastructures to securely exchange patient data, i.e. Patient Summaries, also via cloud infrastructures. Apart from the fact that OpenNCP is currently actively developed and this inevitably leads to several technical challenges, another aspect which needs to be emphasized is that these technical challenges very often can be attributed to vague end-user and technical requirements (system specifications) provided by various actors.

Integration with eIDAS

Technically, the eHDSI main technical paradigm provisions a set of national nodes, managing all the inbound and outbound request of data, with a Circle of Trust based architecture where the list of all of these nodes is centrally managed and distributed to the different health authorities of the participating countries. In a typical data flow of operation, a patient in a visiting country contacts the eHDSI National node of country B (B Node) and, after a proper authentication phase, asks for health data of the patient. The B Node redirects these requests to the A Node, where A is the country of origin of the patient and where his eHealth data are stored.

This process masks all the complexities of retrieving the data from Country A national infrastructure, that are nonetheless present. The request could get lost, data could be provided in a non-timely manner, and as such Country B could not get them in an effective way to allow for proper treatment of patient. As such, Country B has a strong interest in being able to show that these data have been requested; in the same way, Country A wants to have a way to show that data have been effectively provided. In order to allow these two parties to reach an agreement, a shared data storage should be defined, with strong immutability features, and a permissioned blockchain for all of the European member states has been implemented. To this end, in the KONFIDO simulation testbed, the eHDSI system has been integrated into the eIDAS Network, with the role of Service Provider, allowing it to request qualified (i.e. legally binding) authentications for the patients. It should be noted that as the eIDAS Network provides its services only to public services, considering that the KONFIDO project is developing innovative services to be applied for the eHDSI system but it lacks a proper legal status, the actual integration happened over the so called sample implementation of the eIDAS Node [23].

Agent-Based modelling

Summarizing the main lessons learned by the “Agent Based” modelling research line, it was clearly depicted that complex distributed systems have systemic interactions that are difficult to understand and predict in advance. In particular, it has also raised some interesting questions about how security control is actually closely coupled with system performance. We have seen that security driven questions such as the accuracy of attack detectors, in terms of the probability of false alarm and the probability of correct detection, directly relate to the effective throughput that the system can achieve in terms of successfully processing requests for secure health data transfer. Another question that our work has raised is the need for attack traces of different types in order to test the robustness of the system, as well as to test our ability to detect and mitigate attacks and to evaluate the system's robustness. Our work has also raised some new problems, such as the role of control schemes which are multi-lateral rather than just bilateral, since the effects of one node on another in such a system can affect third party nodes which are not directly involved in the bilateral exchange.

Barriers

Moving beyond the technical part, throughout the whole KONFIDO project lifecycle, it became evident that the main barriers regarding the implementation of a secure and robust health data exchange framework are not technical, but organizational and can be summarized as following:

a) the Member States are not all aligned with JASeHN agreement [24];

b) different consent mechanisms among Member States;

c) lack of standard electronic health record-system among Member States;

d) different implementation of EU regulations among Member States;

e) different information workflows among National Infrastructure, Regional infrastructures and healthcare organizations;

f) lack of harmonization of rules, processes and safeguards;

g) eHNCP deployments in Member States are still in early stages;

h) lack of the budget to address security aspects by healthcare organizations.

Discussion

In this paper we provided an overview of the KONFIDO project and its technical achievements, as it emphasized on the use of high-end technical paradigms and frameworks. Finally, we summarize and highlight the "lessons learned" during the project's lifecycle, moving beyond technical issues. Hopefully, these lessons could be a beacon in terms of policy making or technical infrastructure development. Based on the interaction with the various stakeholders and the technical experience during the project's pilot phase, KONFIDO team identified challenges across administrative, legal, technical and semantic interoperability issues, summarized as following:

Lesson 1: Infrastructure is not there yet

The development of eHNCPs in most of the EU countries is still in a rather immature stage. Technically, many of the infrastructure frameworks do not yet have robust implementations and they seem to constantly evolve. However, technical reasons would only partially explain the lack of the infrastructure, as based on the KONFIDO consortium interaction with various stakeholders, administrative and political reasons are also part of the explanation. Many of the stakeholders concluded that "cross-border health data exchange is not yet a priority for national healthcare systems in every Member State".

Lesson 2: Legislation and Administrative issues could significantly impact technical developments

Legal and administrative issues were identified as a profound factor to affect technical developments. For example, it was highlighted that while building a centralized SIEM would be technically feasible and perhaps preferable, this technical decision would probably not be compliant with EU legislation. Furthermore, as the administrative handling of cross-border health data exchange is rather new for all EU member states, the assignment of responsibilities is not yet clear and this might also lead to setbacks, e.g. reallocating the responsibility of eHNCP deployment which could cause delays or even significant changes in technical developments.

Lesson 3: Central Policy decisions make a difference and could intersect technical decisions

As an example, the eIDAS Regulation is the world's largest and most complex federation of sovereign digital identity systems, and it is still under deployment as different member states are progressively notifying their electronic identity means to the other, the first step for cross-border recognition. As a work in progress, this means that not all citizens in Europe are provided with an eIDAS Identity, nor that the access to the network for research purposes is simple to obtain.

Lesson 4: Usability should be a top priority

While KONFIDO components have no end-user interface as they mostly work on the "background" and therefore usability seems to be marginally in KONFIDO scope, it should be noted that usability was one of the key issues raised in each step, from user requirements engineering until the pilot validation workshops discussions. This repeated pattern of identifying usability as one of the top concerns, highlights its importance for relevant technical solutions.

Lesson 5: Semantic Interoperability is an underestimated issue

Another issue highlighted was the difficulty regarding the semantic interoperability of the exchanged information. While epSOS framework provides a template to exchange patient summary information, the translation between various languages could be a significant issue as it could heavily impact clinical decisions and should not be considered a trivial process. Furthermore, interlinking with widely accepted knowledge structures (e.g. terminologies/thesauri/ontologies) could also significantly enhance the value of extended data. To this end, using Semantic Web technologies and the Linked Data paradigm could facilitate the data handling based on FAIR principles [25] and provide a gateway to relevant data models, also enabling "intelligent" reasoning (adverse drug reactions could be a very important case as depicted in [26]).

Lesson 6: Technical expertise lack

The lack of technical expertise regarding highly skilled IT security professionals was also identified as a barrier regarding the deployment and maintenance of technical solutions like KONFIDO.

Lesson 7: Integration of reference implementations frameworks or libraries is not always a straight forward task

The integration of OpenNCP reference implementation framework in the KONFIDO pilot setup was far from trivial. To this end, the OpenNCP framework architecture patterns could perhaps be revisited to facilitate its integration in other IT systems or its extension in order to fit in a wide range of setups.

Based on these "lessons learned", the recommendations regarding the further adoption of KONFIDO technical solution or the development of other similar solutions can be summarized as following:

Recommendation 1: Technical developments should adopt agile methodologies embracing potential changes

As legal, technical and administrative context regarding cross-border health data exchange is not yet stable, technical solutions developments should also adapt accordingly. As new technical paradigms engaged in healthcare also produce data (e.g. IoT, machine-to-machine technologies etc.) they will probably alter the needs of the respective cross-border health data exchange processes. The use of agile methodologies during the development process might be a good way to embrace potential changes in the process of technical development and reduce risks.

Recommendation 2: Technical developments should be based on standards and widely accepted practices

Using technical standards (e.g. the ones produced by ISO) would typically facilitate compliance with legal artifacts too. Practically, in the KONFIDO project we focused on the use of standards during the requirements engineering phase, enabling us to identify gaps and define end user goals. Furthermore, adopting widely accepted best practices (e.g. using cloud infrastructure to host pilot eHNCPs and the micro-services architectural paradigm to implement the KONFIDO technical solution as a toolkit rather

than as a monolithic software) enabled KONFIDO to overcome the issues of lacking infrastructures and also reducing dependencies on other software components.

Recommendation 3: Promoting mentality change and know-how is a crucial factor

As in the policy making process regarding cross-border health data exchange a number of diverse stakeholders is involved (e.g. IT technical staff, managers, healthcare professionals, legal experts etc.). the benefits of adopting sophisticated technical solutions might not be obvious to all. To this end, promoting mentality change and know-how towards a holistic information security approach would play a critical role in the design, development, deployment and practical adoption of KONFIDO-like solutions.

The fact that the main outcomes of this article, i.e. the "lessons learned" and the respective "recommendations" are not based on quantified data, but they are based on qualitative hands-on experience gained as a whole during the project's implementation, could be identified as a limitation of the presented study, as they could be biased due to a number of factors.

However, we argue that ~~T~~the need for cross-border health data exchange and ~~therefore~~ the potential impact of these "lessons learned" and the respective "recommendations" is further highlighted due to the recent COVID-19 pandemic. ~~It should also be highlighted that many of these could also be relevant with the deployment of systematic tele-monitoring solutions developed in a national level.~~ To this end, we consider that technical approaches like the one elaborated on KONFIDO and the respective lessons learned should be seriously considered in the context of the new healthcare service paradigms elaborated as part of the (inter)national response to COVID-19 pandemic and beyond [27].

Abbreviations

BP: Business Process

eHDSI: eHealth Digital Service Infrastructure

EHR: Electronic Health Record

eID: electronic IDentification

eIDAS: electronic IDentification, Authentication and trust Services

ENISA: European Union Agency for Network and Information Security

epSOS: European Partners – Smart Open Services

GDPR: General Data Protection Regulation

HCP: Healthcare professional

HE: Homomorphic Encryption

HIT: Health Information Technologies

IT: Information Technologies

JASeHN: Joint Action to Support the eHealth Network

eHNCP: eHealth National Contact Point

OpenNCP: Open-source and reference version of the eHNCP software

PS: Patient Summary

SGX: Software Guard Extension

TEE: Trusted Execution Environment

References

[1] KONFIDO project website, (n.d.). http://www.konfido-project.eu/konfido/ (accessed January 15, 2018).

[2] C. Mesaritakis, M. Akriotou, A. Kapsalis, E. Grivas, C. Chaintoutis, T. Nikas, D. Syvridis, Physical Unclonable Function based on a Multi-Mode Optical Waveguide, Sci. Rep. 8 (2018) 9653. https://doi.org/10.1038/s41598-018-28008-6.

[3] S. Angraal, H.M. Krumholz, W.L. Schulz, Blockchain Technology: Applications in Health Care., Circ. Cardiovasc. Qual. Outcomes. 10 (2017) e003800. https://doi.org/10.1161/CIRCOUTCOMES.117.003800.

[4] X. Yi, R. Paulet, E. Bertino, Homomorphic Encryption, in: Homomorphic Encryption Appl., Springer, Cham, 2014: pp. 27–46. https://doi.org/10.1007/978-3-319-12229-8_2.

[5] S. Bhatt, P.K. Manadhata, L. Zomlot, The Operational Role of Security Information and Event Management Systems, IEEE Secur. Priv. 12 (2014) 35–41. https://doi.org/10.1109/MSP.2014.103.

[6] M. Fonseca, K. Karkaletsis, I.A. Cruz, A. Berler, I.C. Oliveira, OpenNCP: a novel framework to foster cross-border e-Health services., Stud. Health Technol. Inform. 210 (2015) 617–21. http://www.ncbi.nlm.nih.gov/pubmed/25991222 (accessed March 1, 2017).

[7] epSOS project web site, (n.d.). http://www.epsos.eu/ (accessed November 16, 2018).

[8] eIDAS web site, (n.d.). https://www.eid.as/home/ (accessed November 16, 2018).

[9] M. Staffa, L. Sgaglione, G. Mazzeo, L. Coppolino, S. D'Antonio, L. Romano, E. Gelenbe, O. Stan, S. Carpov, E. Grivas, P. Campegiani, L. Castaldo, K. Votis, V. Koutkias, I. Komnios, An OpenNCP-based Solution for Secure eHealth Data Exchange, J. Netw. Comput. Appl. 116 (2018) 65–85. https://doi.org/10.1016/j.jnca.2018.05.012.

[10] P. Natsiavas, J. Rasmussen, M. Voss-Knude, K. Votis, L. Coppolino, P. Campegiani, I. Cano, D. Marí, G. Faiella, F. Clemente, M. Nalin, E. Grivas, O. Stan, E. Gelenbe, J. Dumortier, J. Petersen, D. Tzovaras, L. Romano, I. Komnios, V. Koutkias, Comprehensive user requirements engineering methodology for secure and interoperable health data exchange, BMC Med. Inform. Decis. Mak. 18 (2018) 85. https://doi.org/10.1186/s12911-018-0664-0.

[11] V. Koutkias, P. Natsiavas, C. Kakalou, K. Votis, D. Tzovaras, N. Maglaveras, Requirements Elicitation for Secure and Interoperable Cross-Border Health Data Exchange: the KONFIDO Study, IET Softw. (2019). https://doi.org/10.1049/iet-sen.2018.5292.

[12] G. Faiella, I. Komnios, M. Voss-Knude, I. Cano, P. Duquenoy, M. Nalin, I. Baroni, F. Matrisciano, F. Clemente, Building an ethical framework for cross-border applications: The KONFIDO project, in: Commun. Comput. Inf. Sci., Springer Verlag, 2018: pp. 38–45. https://doi.org/10.1007/978-3-319-95189-8_4.

[13] E. Gelenbe, M. Pavloski, Performance of a Security Control Scheme for a Health Data Exchange System, in: 2020.

[14] M. Nalin, I. Baroni, G. Faiella, M. Romano, F. Matrisciano, E. Gelenbe, D.M. Martinez, J. Dumortier, P. Natsiavas, K. Votis, V. Koutkias, D. Tzovaras, F. Clemente, The European cross-border health data exchange roadmap: Case study in the Italian setting, J. Biomed. Inform. 94 (2019) 103183. https://doi.org/10.1016/J.JBI.2019.103183.

[15] P. Natsiavas, C. Kakalou, K. Votis, D. Tzovaras, N. Maglaveras, I. Komnios, V. Koutkias, Identification of Barriers and Facilitators for eHealth Acceptance: The KONFIDO Study, in:

Springer, Singapore, 2018: pp. 81–85. https://doi.org/10.1007/978-981-10-7419-6_14.

[16] P. Natsiavas, C. Kakalou, K. Votis, D. Tzovaras, V. Koutkias, Citizen Perspectives on Cross-Border eHealth Data Exchange: A European Survey., Stud. Health Technol. Inform. 264 (2019) 719–723. https://doi.org/10.3233/SHTI190317.

[17] J. Rasmussen, P. Natsiavas, K. Votis, K. Moschou, P. Campegiani, L. Coppolino, I. Cano, D. Marí, G. Faiella, O. Stan, O. Abdelrahman, M. Nalin, I. Baroni, M. Voss-Knude, V.A. Vella, E. Grivas, C. Mesaritakis, J. Dumortier, J. Petersen, D. Tzovaras, L. Romano, I. Komnios, V. Koutkias, Gap Analysis for Information Security in Interoperable Solutions at a Systemic Level: The KONFIDO Approach, in: Springer, Singapore, 2018: pp. 75–79. https://doi.org/10.1007/978-981-10-7419-6_13.

[18] E. Papaleo, G. Faiella, R. Orofino, F. Borrometi, F. Clemente, TELPASS Project: B2B Teleconsultation for Pediatric Hospices, in: 7th IEEE Int. Conf. E-Health Bioeng. - EHB 2019, IEEE, Iasi, Romania, 2019: pp. 1–4. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8969882 (accessed June 19, 2020).

[19] L. Castaldo, V. Cinque, Blockchain-based logging for the cross-border exchange of ehealth data in Europe, in: Commun. Comput. Inf. Sci., Springer Verlag, 2018: pp. 46–56. https://doi.org/10.1007/978-3-319-95189-8_5.

[20] Audit Trail and Node Authentication - IHE Wiki, (n.d.). https://wiki.ihe.net/index.php/Audit_Trail_and_Node_Authentication (accessed June 19, 2020).

[21] E. Gelenbe, G-networks with signals and batch removal, Probab. Eng. Informational Sci. 7 (1993) 335–342. https://doi.org/10.1017/S0269964800002953.

[22] O. Brun, Y. Yin, E. Gelenbe, Deep Learning with Dense Random Neural Network for Detecting Attacks against IoT-connected Home Environments, in: Procedia Comput. Sci., Elsevier B.V., 2018: pp. 458–463. https://doi.org/10.1016/j.procs.2018.07.183.

[23] Documentation eID, (n.d.). https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Documentation+eID (accessed June 19, 2020).

[24] Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth on the Criteria required for the participation in Cross-Border eHealth Information Services, 2011. https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20170509_co06_en.pdf (accessed July 14, 2020).

[25] M.D. Wilkinson, M. Dumontier, I.J.J. Aalbersberg, G. Appleton, M. Axton, A. Baak, N. Blomberg, J.-W. Boiten, L.B. da Silva Santos, P.E. Bourne, J. Bouwman, A.J. Brookes, T. Clark, M. Crosas, I. Dillo, O. Dumon, S. Edmunds, C.T. Evelo, R. Finkers, A. Gonzalez-Beltran, A.J.G. Gray, P. Groth, C. Goble, J.S. Grethe, J. Heringa, P.A.C. 't Hoen, R. Hooft, T. Kuhn, R. Kok, J. Kok, S.J. Lusher, M.E. Martone, A. Mons, A.L. Packer, B. Persson, P. Rocca-Serra, M. Roos, R. van Schaik, S.-A. Sansone, E. Schultes, T. Sengstag, T. Slater, G. Strawn, M.A. Swertz, M. Thompson, J. van der Lei, E. van Mulligen, J. Velterop, A. Waagmeester, P. Wittenburg, K. Wolstencroft, J. Zhao, B. Mons, The FAIR Guiding Principles for scientific data management and stewardship., Sci. Data. 3 (2016) 160018. https://doi.org/10.1038/sdata.2016.18.

[26] P. Natsiavas, R.D. Boyce, M.-C. Jaulent, V. Koutkias, OpenPVSignal: Advancing Information Search, Sharing and Reuse on Pharmacovigilance Signals via FAIR Principles and Semantic Web Technologies, Front. Pharmacol. 9 (2018) 609. https://doi.org/10.3389/fphar.2018.00609.

[27] R. Ohannessian, T.A. Duong, A. Odone, Global Telemedicine Implementation and Integration

Within Health Systems to Fight the COVID-19 Pandemic: A Call to Action, JMIR Public Heal. Surveill. 6 (2020) e18810. https://doi.org/10.2196/18810.