Secure cross-border exchange of health related data: the KONFIDO approach

Ioannis Komnios[1], Dimitris Karamitros[1], Luigi Romano[2*], Luigi Coppolino[2], Vassilis Koutkias[3], Kostas Votis[3], Oana Stan[4], Paolo Campegiani[5], David Mari Martinez[6], Marco Nalin[7], Ilaria Baroni[7], Fabrizio Clemente[8], Giuliana Faiella[8], Charis Mesaritakis[9], Evangelos Grivas[9], Janne Rasmussen[10], Jan Petersen[10], Isaac Cano[11], Elisa Puigdomenech[12], Erol Gelenbe[13], Jos Dumortier[14], and Maja Voss-KnudeVoronkov[15]

[1] EXUS Software LTD
{i.komnios,d.karamitros}@exus.co.uk
[2]Consorzio Interuniversitario Nazionale Per L'Informatica
{luigi.romano,luigi.coppolino}@uniparthenope.it
[3]Centre for Research and Technology Hellas
{vkoutkias,kvotis}@certh.gr
[4]Commissariat a l'Energie Atomique Et Aux Energies Alternatives
oana.stan@cea.fr
[5]Bit4id s.r.l.
pca@bit4id.gr
[6]Fundacio Eurecat
david.mari@eurecat.org
[7]TELBIOS s.r.l.
{marco.nalin,ilaria.baroni}@telbios.com
[8]Fondazione Santobono Pausilipon onlus
fabrizio.clemente@ibb.cnr.it
giuliana.faiella@gmail.com
[9]Eulambia Advanced Technologies LTD
{evangelos.grivas, charis.mesaritak}@eulambia.com
[10]MedCom
{jar,jap}@medcom.dk
[11]Consorci Institut D'Investigacions Biomediques August Pi I Sunyer
iscano@clinic.ub.es
[12]Agencia de Qualitat i Avaluacio Sanitaries de Catalunya
epuigdomenech@gencat.cat
[13]Imperial College of Science Technology and Medicine
e.gelenbe@imperial.ac.uk
[14]Time Lex CVBA

[*] Corresponding Author

jos.dumortier@timelex.eu
[15]Sundhed.dk IS
mvk@sundhed.dk

Abstract

This paper sets up the scene of the KONFIDO project in a clear way. In particular, it: i) defines KONFIDO objectives and draws KONFIDO boundaries; ii) identifies KONFIDO users and beneficiaries; iii) describes the environment where KONFIDO is embedded; iv) provides a bird's eye view of the KONFIDO technologies and how they will be deployed in the pilot studies of the project; and v) presents the approach that the KONFIDO consortium will take to prove that the proposed solutions work. KONFIDO addresses one of the top three priorities of the European Commission regarding the digital transformation of health and care in the Digital Single Market, i.e. citizens' secure access to their health data, also across borders. To make sure that KONFIDO has a high-impact, its results are exposed to the wide public by developing three substantial pilots in three distinct European countries (namely Denmark, Italy, and Spain).

1 Introduction, Rationale, Motivation

One of the top three priorities of the European Commission regarding the digital transformation of health and care in the Digital Single Market constitutes citizens' secure access to their health data, also across borders - enabling citizens to access their health data across the European Union [4]. Up to now, the core effort in the EU for enabling cross-border health data exchange has been resolving interoperability aspects, with projects such as epSOS and OpenNCP (the software implementation of epSOS) providing the foundations for that. However, limited focus has been given on cybersecurity aspects that are entailed in this data exchange, despite the sensitive nature of health data. KONFIDO is an H2020 project aiming to address this issue through a holistic paradigm at the systemic level by gathering a number of state-of-the-art technologies in its toolset, such as blockchain [5], photonic Physical Unclonable Functions [6], homomorphic encryption [7], and trusted execution [8].

In a nutshell, KONFIDO is about improving the security of cross-border exchange of eHealth data using OpenNCP. Since KONFIDO's objective is to improve the security of OpenNCP (and not to extend OpenNCP functions), there is a clean-cut separation in KONFIDO between Functional and Non-Functional requirements, and specifically:

- Functional requirements (particularly, interoperability) must be satisfied by OpenNCP.
- Non-functional requirements (particularly, security) must be satisfied by KONFIDO.

Nevertheless, it is worth noting that even if KONFIDO does not implement new functional requirements for OpenNCP, this does not mean that KONFIDO does not have functional requirements at all. In fact, the addition of security features to OpenNCP results in the need to implement new functions (e.g. for strong authentication of users), and the requirements of these functions collectively represent functional requirements for KONFIDO.

A high-level view of how KONFIDO can be deployed to improve the security of OpenNCP is given in Figure 1.

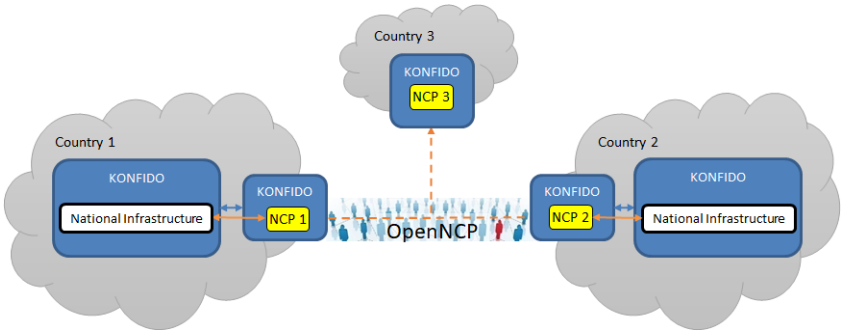

Figure 1 - How KONFIDO can be deployed to improve the security of OpenNCP

It is worth emphasizing that the implementation of secure National Infrastructures is beyond the scope of KONFIDO. Nevertheless, National Infrastructures play an important role in KONFIDO, since they enable the delivery of KONFIDO services to KONFIDO users and beneficiaries. In particular, National Infrastructures are in charge of implementing delegation mechanisms, e.g. enabling a legitimate user of the IT systems of the national eHealth infrastructures of individual Member States that are authorized to access Patient Summaries and ePrescriptions to do so (e.g. a doctor at a hospital emergency service of European country A who has been authorized by a patient of European country B to access his/her data cross-border). Some KONFIDO technologies are dependent on OpenNCP, and are thus only applicable where OpenNCP is available. Several KONFIDO technologies are instead – to a large extent – technically re-usable also outside OpenNCP. These technologies are potentially exploitable within other platforms, including National Infrastructures.

2 KONFIDO Users and Beneficiaries

Since KONFIDO implements secure cross-border data exchange on top of OpenNCP, the only users who interact directly with KONFIDO are the Certified Health Professionals (CHPs) of the National Contact Points (NCPs), NCP system administrators and personnel of the IT staff, and, in general, roles who have direct access to NCP services. We call these users "First Level Users". First Level Users might also – depending on factors such as implementation decisions, deployment options, and policies – include additional stakeholders (e.g. doctors of eHealth institutions in individual Member States). They can also include non-human users (e.g. hardware/software entities).

KONFIDO has also a number of "Second Level Users", i.e. users that do not access KONFIDO directly, but rather delegate First Level Users to do so. These include several categories of stakeholders, virtually all legitimate users of the IT systems of the national eHealth infrastructures of individual Member States that are authorized to access Patient Summaries and ePrescriptions (e.g. a doctor at a hospital emergency service of European country A who has been authorized by a patient of European country B to access his/her data cross-border).

Citizens are not KONFIDO users, as they do not access KONFIDO services directly or by delegating First Level Users to do so. Nevertheless, they benefit from the availability of OpenNCP services (as improved – with regards to security – by KONFIDO). Thus, we call them KONFIDO "Beneficiaries". A bird's eye view of how KONFIDO users and beneficiaries interact with the system and among them is given in Figure 2.

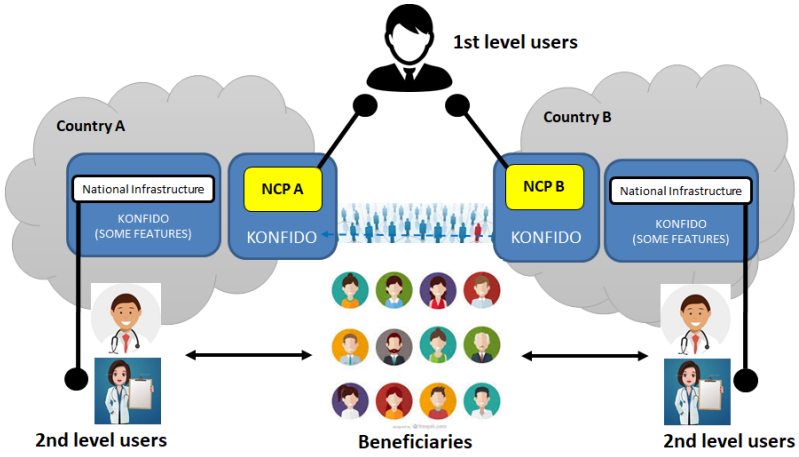

Figure 2 - How KONFIDO users and beneficiaries interact with the system and among them

As already mentioned, some KONFIDO solutions are dependent on OpenNCP, and are thus only applicable where OpenNCP is available, i.e. in the IT infrastructure connecting the NCPs. Nevertheless, although the implementation of secure National Infrastructures is beyond the scope of KONFIDO, some of the KONFIDO solutions that are technically re-usable outside OpenNCP will also be deployed in the National Infrastructures.

Finally, it is worth emphasizing that delegation mechanisms may range from very simple schemes (e.g. a 1-to-1 mapping of a 2nd level user to the corresponding 1st level user) to quite complex ones (e.g. a N-to-1 mapping of multiple 2nd level users to a specific 1st level user). Delegation mechanisms are particularly complex when delegation happens across borders, i.e. a beneficiary from country A delegates a Second Level User of Country B (e.g. an Italian citizen needs treatment at a Spanish Hospital). These mechanisms are being thoroughly analysed in KONFIDO, also based on the requirements set out by the GPDR [10].

3 KONFIDO Design Principles and System Boundaries

KONFIDO takes a user centric approach that it is driven by the real needs of its users and – above all – beneficiaries [9]. It relies on a federated architecture with multiple (2+) levels of hierarchy and on a clean-cut separation between Functional and Non-Functional requirements. More specifically, functional requirements (particularly, interoperability) are satisfied by OpenNCP, while non-functional requirements (specifically, security) must be satisfied by KONFIDO. It is aligned to the eHealth Digital Service Infrastructure (eHDSI or eHealth DSI), the initial deployment and operation of services for cross-border health data exchange under the Connecting Europe Facility (CEF), which is illustrated in Figure 3.

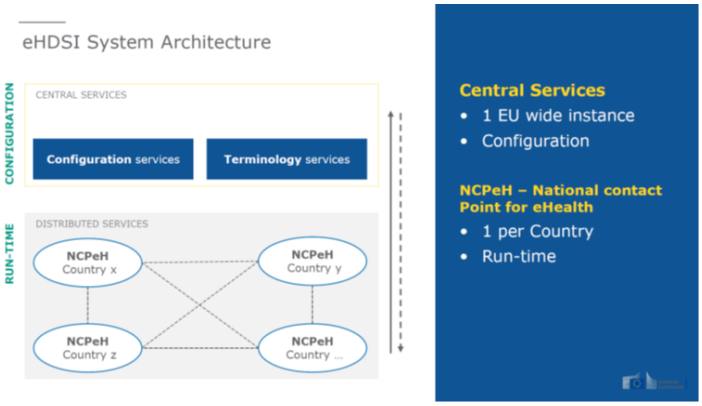

Figure 3 - eHDSI conceptual architecture

To set up KONFIDO validation and demonstration infrastructure, a number of software stubs will have to be developed. By "software stubs" we mean prototype software artefacts – as opposed to commercial grade applications – that implement the "glue code" for exposing OpenNCP functions (as secured by KONFIDO) to pilot users. These stubs are essential to "feed" KONFIDO with inputs and to "consume" KONFIDO outputs. Importantly, these stubs will enable effective demonstration of the KONFIDO results also to Second Level Users and Beneficiaries, to ultimately maximize KONFIDO impact.

4 National Infrastructures of KONFIDO Pilots

4.1 The Italian National Infrastructure

The Italian Healthcare System is a federated system, meaning that each Region is free to implement its own local policies, reimbursement models, structure, etc. For this reason, a real Italian Electronic Health Record does not exist as a unique National Infrastructure. The reference for the its development is the "Fascicolo Sanitario Elettronico" (FSE), a set of functions that must be implemented by each Region for eHealth data exchange in Italy. Every Region will have to implement its own (vendor-specific) version of the FSE and make sure it properly exchanges data with the FSEs of the other Regions through the National Interoperability Infrastructure (INI – Infrastruttura Nazionale per l'Interoperabilità).

Currently, the FSE is only partially implemented and adopted in the different Regions. Data available at the time of the writing of this document are updated at 2018 Q2, and they present a picture where there are 17 (out of 21) active Regions trying to implement the FSE, with 11 of them already adhering properly to the INI. Yet, the actual usage from healthcare professionals and patients is still quite low. Therefore, a unified Italian National Infrastructure is considered as not available, at least not for a research project to be tested out. The identified infrastructure used for the Italian NI is composed by:

- A node representing the Italian NCP equipped with OpenNCP and a gateway to forward the request to the specific Italian regional node;
- Two regional nodes, one for PAUSIL and one for TELBIOS, that use the TELBIOS code.

The two regional nodes can exchange any clinical documents at National level, based on the FSE definition, including tele-monitoring data. However, they will exchange ONLY Patient Summary and ePrescription data at European level.

Since the FSE and the epSOS information included in the documents to be exchanged are the same and the reference format is HL7 CDA v2 [14], the epSOS format for these two documents will also be used in the Italian NI.

Since the actual access to the INI for the exchange of FSE data is not accessible for research purposes, software stubs will be developed for the currently available implementations of the FSE (EHR), whenever possible, for data exchanges between healthcare institutions participating in the construction of KONFIDO input data and/or the consumption of KONFIDO output data.

4.2 The Spanish National Infrastructure

In Catalonia (Spain), the provision of healthcare is done by multiple contracted providers having different ownership: public organizations – the Catalan Health Institute (ICS) is the biggest one –, consortia, municipal foundations and private foundations. The provision of healthcare is organized into four main levels: primary care; specialized or hospital care; socio-sanitary care; and mental health. Primary care is the gatekeeper and responsible for coordinating the patients' care along the care continuum. Since the primary healthcare reform (in 1985), primary care has evolved from a predominantly curative care model (upon demand from the user population and the work of individual healthcare professionals) to a model that focuses simultaneously on preventive healthcare, curative healthcare, rehabilitative care and the promotion of community health. This transformation was structurally achieved through the creation of basic health areas and the gradual introduction of primary care teams. Nowadays, there are 369 primary care centres, with around 77% of them being managed by the public provider ICS.

Specialized or hospital care acts as a consultant of primary care and is responsible for more complex care. There is a public network of hospitals distributed over the territory following the schemes of population distribution. The model of hospital has changed in recent years, progressing from a traditional model of a more closed centre that provides conventional inpatient care, emergencies and an outpatient department, to a centre with a greater outpatient focus, with significant roles for ambulatory major and minor surgery, day hospital and home hospitalization. Nowadays, there are 69 hospitals (the ICS manages 8 of those). Around 79% of the specialized care is managed by non-public providers.

The current development of the Spanish National Contact Point is provided under the framework of the European call "Connecting Europe Facility (CEF) 2017"[†].

The OpenNCP project in Spain consists of funding 14 national regions executing and preparing their local IT infrastructures to be able to connect to the Spanish NCP. The goal of the project is to deploy the Patient Summary interchange for 2019 and ePrescription capabilities for 2020.

To align the implementation of KONFIDO with the results of the CEF project, the following infrastructure will be considered:

- A patient management platform with Adaptive Case Management and Self-Management Services as the main emulator;
- An OpenNCP node to be integrated with the emulator platform, enhanced by the KONFIDO cybersecurity toolkit.

[†] https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2017-cef-telecom-call-ehealth-cef-tc-2017-2

4.3 The Danish National Infrastructure

The Danish infrastructure builds on a national Health Data Network for secure exchange of all health-related information between all actors in health and social care provision and the National Service Platform (NSP) for the instant and on-demand access to all national registries and services. The NSP is the central national infrastructure for access to and sharing of health information. Through this platform, all relevant partners in the Danish health care services are able to access and share health data using common standardized interfaces and exchange formats. A part of the health data are based on HL7 CDA standards made accessible through an IHE framework. The platform also facilitates uniform access control and common security components.

Denmark also has a national eHealth portal 'sundhed.dk', where not only citizens can access their own medical information, but also authenticated health care professionals have access to the same information.

During the epSOS project, Denmark established an NCP and OpenNCP node to test ePrescriptions across borders. Since, the node has become inactive and, at present time, it seems very unlikely that Denmark is going to use OpenNCP anytime soon. To provide tangible evidence of the advantages that could be brought to Danish citizens, as well as to European citizens visiting Denmark, KONFIDO will stick to its commitment (as per the DoA) of setting up a Danish pilot based on an OpenNCP instance created specifically for KONFIDO. A detailed plan will be issued in the related KONFIDO deliverables.

5 Integration, Validation, and Demonstration in KONFIDO

It is important to clearly distinguish between integration, validation, and demonstration. In KONFIDO, system integration is the process of bringing together individual sub-systems into one system. The system is an aggregation of subsystems cooperating so that it is able to deliver its overarching functionality. Sub-systems include computing systems, software applications, and physical devices. Validation is the process of demonstrating that the proposed solutions are valid, meaning that they solve the problems they were designed for. Demonstration includes all the activities needed to expose the proposed solutions to potential stakeholders (i.e. KONFIDO 2nd level users) and/or to the public in general (i.e. KONFIDO beneficiaries).

Figure 4 provides a high-level view of the approach taken by KONFIDO for integration and validation.

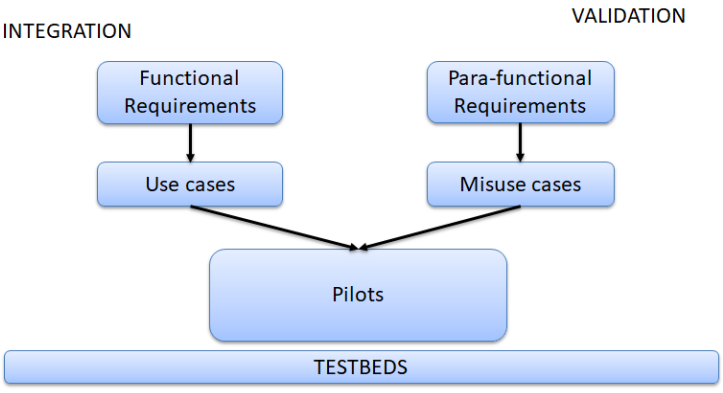

Figure 4 - KONFIDO approach to integration and validation

A use case is an example of correct – proper and, in particular, non-malicious – use of a system. Since KONFIDO is "added" to OpenNCP, integration in KONFIDO means providing evidence that OpenNCP still works properly after KONFIDO has been applied. As such, use cases are the right tool for demonstrating that the integration of KONFIDO (in OpenNCP and in the surrounding context) has been successful.

A misuse case is an example of malicious use of a system. Since KONFIDO's goal is to "add" security to OpenNCP, validating KONFIDO, i.e. providing evidence that it does what it is supposed to do, means collecting tangible evidence that KONFIDO effectively protects OpenNCP from major risks, such as putting the infrastructure out of service; stealing confidential data from eHealth documents; modifying sensitive fields of clinical documents; enabling a malicious user to impersonate a legitimate user. Thus, misuse cases are the right tool for validating KONFIDO para-functional requirements, since they test the ability of KONFIDO to protect OpenNCP from attempts of violating the security of the data that is exchanged and/or of the infrastructure that enables data exchange.

To counter a misuse, monitoring and control actions can be taken within the system, both at the request (A) level, and at the receiver (B) level. In fact, for each attempted use of the system, we can imagine that such controls will be carried out by both parties, and that further controls may also take place at a higher system level where reports from the bilateral lower levels can also be monitored. At the same time, we may consider that an attempted misuse, when detected and rejected, may come back, either in a similar or disguised form, so that such detections and rejections will not be "final" but may lead to repeated attempts under different guises. In addition to the effect of the misuse itself, even with a perfect detection and rejection system, the whole security detection and control scheme creates additional workload and possible congestion for the system which will need to be evaluated and quantified, and for which resources have to be provisioned during normal system operations [11][12][15].

In addition, detection schemes are not perfect and will be subject to false alarms. Thus, the analysis should also provide estimates of the additional delays, costs and user frustration that is introduced by such false alarms. This analysis can lead to a cost/benefit study of the misuse and attack detection schemes that are introduced into the system.

A pilot is a realistic application – i.e. one that already exists (or that will exist) in the real world or close to one that already exists (or that will exist) in the real world – that has the capability of exercising the proposed solutions. It is an infrastructure that allows the pilots to run and exercise the proposed solutions.

Since demonstration consists of activities needed to expose the proposed solutions to potential stakeholders (i.e. KONFIDO 2nd level users) and/or to the public in general (i.e. KONFIDO beneficiaries), the same infrastructure that will be used for integration and validation (possibly simplified‡ for practical reasons) will also be used for demonstration.

‡ As an example, for demonstration purposed it might be irrelevant if the pilots run on an infrastructure that spans multiple countries or if they are deployed on a more compact – yet fully fledged – distributed setup.

Annex: Glossary

This glossary explains the meaning of terms in the context of KONFIDO. Some definitions are taken from standards and/or documents on which there is general consensus (e.g. [1], [2], [3], and [13]), possibly contextualized to the KONFIDO setup.

1st level user	These are direct users of the KONFIDO tools. They include the Certified Health Professionals (CHPs) of the National Contact Points (NCPs), NCP system administrators and personnel of the IT staff, and, in general, roles who have direct access to NCP services. They might also – depending on factors such as implementation decisions, deployment options, and policies – include additional stakeholders (e.g. healthcare professionals of clinical institutions in individual Member States). They can also include non-human users (e.g. hardware/software entities).
2nd level user	Second level users do not access KONFIDO directly, rather they delegate First Level Users to perform actions on their behalf. These include several categories of stakeholders, virtually all legitimate healthcare professionals that are authorized to access Patient Summaries and ePrescriptions (e.g. a doctor at a hospital emergency service of European country A who has been authorized by a patient of European country B to access his/her data cross-border). It is worth emphasizing that delegation mechanisms may range from very simple schemes (e.g. a 1-to-1 mapping of a 2nd level user to the corresponding 1st level user) to quite complex ones (e.g. a N-to-1 mapping of multiple 2nd level users to a specific 1st level user).
Beneficiary	Beneficiaries are not KONFIDO users, meaning they do not access KONFIDO services directly. Nevertheless, they benefit from the availability of OpenNCP services (as improved – with regards to security – by KONFIDO). Thus, we call them KONFIDO "Beneficiaries". Virtually, all citizens of European Union countries are KONFIDO beneficiaries.
Functional requirement	A functional requirement specifies what the system should do. In other words, a functional requirement describes a particular behaviour or function of the system (possibly when certain conditions are met).
Delegation	Delegation is a mechanism that allows/enables an entity to perform an action on behalf of another entity.
Non-functional requirement	A non-functional or para-functional requirement specifies how the system performs a certain function. In other words, a non-functional requirement describes how a system should behave and what limits there are on its functionality.
Integration	In KONFIDO, system integration is the process of bringing together individual sub-systems into one system. The system is an aggregation of subsystems cooperating so that it is able to deliver its overarching functionality. Subsystems include computing systems, software applications, and physical devices.
Validation	Validation is the process of demonstrating that the proposed solutions are valid, meaning that they solve the problems they were designed for.
Demonstration	Demonstration includes all the activities needed to expose the proposed solutions to potential stakeholders and/or to the public in general. Demonstration of an activity is of paramount importance in KONFIDO.

Use case	A use case is an example of correct – proper and, in particular, non-malicious – use of a system. Since KONFIDO is "added" to OpenNCP, integration in KONFIDO means providing evidence that OpenNCP still works properly after KONFIDO has been applied. As such, use cases are the right tool for demonstrating that the integration of KONFIDO (in OpenNCP and in the surrounding context) has been successful.
Misuse case	A misuse case is an example of malicious use of a system. Since KONFIDO's goal is to "add" security to OpenNCP, validating KONFIDO – i.e. providing evidence that it does what it is supposed to do – means collecting tangible evidence that KONFIDO effectively protects the infrastructure of eHealth data exchange from attacks that can result in major impacts, such as: i) putting the infrastructure out of service; ii) stealing confidential data from eHealth documents; iii) modifying sensitive fields of eHealth documents; and iv) enabling a malicious user to impersonate a legitimate user. Thus, misuse cases are the right tool for validating KONFIDO, since they test the ability of KONFIDO to protect OpenNCP from attempts to violate the security of the data that is exchanged and/or of the infrastructure that enables data exchange.
Pilot	It is a realistic application – i.e. one that already exists (or that will exist) in the real world, or close to one that already exists (or that will exist) in the real world – that has the capability of exercising the proposed solutions. Pilots play a key role in KONFIDO.
Testbed	It is an infrastructure that allows the pilots to run and to exercise the proposed solutions.
Identification	The process in which a user of a system states his/her identity, without any supporting evidence.
Authentication	The process through which a user of a system proves his/her identity, i.e. that he/she is who he/she claims to be.
Authorization	The process by which the access to a resource is granted (or denied) to a user, once he/she has authenticated, according to a specific security policy.
Accounting	The process of keeping track of which resources an authenticated user has accessed.
NCPeH	National Contact Point for eHealth, which may act as an organisational and technical gateway for the provision of eHealth Cross-Border Information Services.

Acknowledgements

The authors are grateful to the following people, for their valuable contributions to this paper: Salvatore D'Antonio and Giovanni Mazzeo (CINI), Pantelis Natsiavas (CERTH), Charidimos Chaintoutis (Eulambia), Jesper Soederberg Knudsen (MEDCOM).

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 727528 (KONFIDO - Secure and Trusted Paradigm for Interoperable eHealth Services). This paper reflects only the authors' views and the Commission is not liable for any use that may be made of the information contained therein.

References

[1] https://reqtest.com/requirements-blog/understanding-the-difference-between-functional-and-non-functional-requirements/

[2] "Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design", Craig Larman

[3] ISO 24765: https://www.smaele.nl/documents/iso/ISO-24765-2010.pdf

[4] European Commission, "Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society", Brussels, 25.4.2018 COM(2018) 233 final, Available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51628

[5] A. Theodouli, S. Arakliotis, K. Moschou, K. Votis, D. Tzovaras, "On the design of a Blockchain-based system to facilitate Healthcare Data Sharing", in Proc. of the 17th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications / 12th IEEE Int. Conf. on Big Data Science and Engineering (TrustCom/BigDataSE), 2018, pp. 1374-1379.

[6] C. Mesaritakis, M. Akriotou, A. Kapsalis, E. Grivas, C. Chaintoutis, T. Nikas and D. Syvridis (2018). Physical Unclonable Function based on a Multi-Mode Optical Waveguide. Scientific Reports, 8(1), 9653. https://doi.org/10.1038/s41598-018-28008-6

[7] S. Carpov and T. Tortech (2018). Secure top most significant genome variants search: iDASH 2017 competition. BMC Medical Genomics, 11(Suppl 4):82. https://doi.org/10.1186/s12920-018-0399-x

[8] L. Coppolino, S. D'Antonio, G. Mazzeo, L. Romano, L. Sgaglione. "Exploiting New CPU Extensions for Se-cure Exchange of eHealth Data at the EU Level". 14th European Dependable Computing Conference (EDCC2018). https://doi.org/10.1109/EDCC.2018.00015

[9] 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 and V. Koutkias (2018). Comprehensive user requirements engineering methodology for secure and interoperable health data exchange. BMC Medical Informatics and Decision Making, 18(1):85. https://doi.org/10.1186/s12911-018-0664-0

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) ELI: http://data.europa.eu/eli/reg/2016/679/2016-05-04

[11] Mariacarla Staffa, Luigi Sgaglione, Giovanni Mazzeo, Luigi Coppolino, Salvatore D'Antonio, Luigi Romano, Erol Gelenbe, Oana Stan, Sergiu Carpov, Evangelos Grivas, Paolo Campegiani, Luigi Castaldo, Konstantinos Votis, Vassilis Koutkias, Ioannis Komnios, An OpenNCP-based Solution for Secure eHealth Data Exchange, Journal of Network and Computer Applications, Volume 116, 2018, Pages 65-85, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2018.05.012

[12] Erol Gelenbe, Paolo Campegiani, Tadeusz Czachórski, Sokratis K Katsikas, Ioannis Komnios, Luigi Romano and Dimitrios Tzovaras, "Security in Computer and Information Sciences", First International ISCIS Security Workshop 2018, Euro-CYBERSEC 2018,

London, UK, February 26-27, 2018, Revised Selected Papers, Lecture Notes Vol. CCIS 821, Springer Verlag, Berlin, 2018, https://link.springer.com/content/pdf/10.1007%2F978-3-319-95189-8.pdf

[13] https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/eHDSI+Glossary

[14] http://www.hl7.org/implement/standards/product_brief.cfm?product_id=185

[15] Mariacarla Staffa, Luigi Coppolino, Luigi Sgaglione, Erol Gelenbe, Ioannis Komnios, Evangelos Grivas, Oana Stan, Luigi Castaldo, "KONFIDO: An OpenNCP-Based Secure eHealth Data Exchange System", Euro-CYBERSEC2018: 11-27, Springer Lecture Notes Vol. CCIS 821, Springer Verlag, Berlin, 2018, https://link.springer.com/chapter/10.1007%2F978-3-319-95189-8_2