Gap Analysis for Information Security in Interoperable Solutions at a Systemic Level: The KONFIDO Approach

J. Rasmussen[1], P. Natsiavas[2], K. Votis[3], K. Moschou[3], P. Campegiani[4], L. Coppolino[5], I. Cano[6], D. Marí[7], G. Faiella[8], O. Stan[9], O. Abdelrahman[10], M. Nalin[11], I. Baroni[11], M. Voss-Knude[12], V.A. Vella[13], E. Grivas[14], C. Mesaritakis[14], J. Dumortier[15], J. Petersen[1], D. Tzovaras[3], L. Romano[5], I. Komnios[16] and V. Koutkias[2]

[1]MedCom, Odense, Denmark
[2]Institute of Applied Biosciences, Centre for Research & Technology Hellas, Thermi, Greece
[3]Information Technologies Institute, Centre for Research & Technology Hellas, Thermi, Greece
[4]Bit4id S.r.l., Napoli, Italy
[5]Department of Engineering, University of Naples "Parthenope", Naples, Italy
[6]IDIBAPS, Hospital Clinic de Barcelona, Universitat de Barcelona, Barcelona, Spain
[7]eHealth R&D Unit, EURECAT, Barcelona, Spain
[8]Fondazione Santobono Pausilipon, Naples, Italy
[9]CEA, LIST, Point Courrier 172, 91191 Gif-sur-Yvette Cedex, France
[10]Dept. of Electrical and Electronic Engineering, Imperial College of Science Technology and Medicine, London, UK
[11]Telbios S.r.l., Milan, Italy
[12]Sundhed.dk, Copenhagen, Denmark
[13]Agency for Health Quality and Assessment of Catalonia, Barcelona, Spain
[14]Eulambia Advanced Technologies Ltd, Athens, Greece
[15]Time.lex, Brussels, Belgium
[16]Exus Software Ltd, London, UK

Abstract—**In this paper, we present a gap analysis study focusing on interoperability of eHealth systems and services coupled with cybersecurity aspects. The study has been conducted in the scope of the KONFIDO EU-funded project, which leverages existing security tools and procedures as well as novel approaches and cutting-edge technology, such as homomorphic encryption and blockchains, in order to create a scalable and holistic paradigm for secure inner and cross-border exchange, storage and overall handling of healthcare data in compliance with legal and ethical norms. The gap analysis relied on desk research, expert opinions and interviews across four thematic areas, namely, eHealth interoperability frameworks, eHealth security software frameworks, end-user perspectives across diverse settings in KONFIDO pilot countries, as well as national cybersecurity strategies and reference reports. A standards-based template has been created as a baseline through which the analysis subjects have been analyzed. The gap analysis identified barriers and constraints as well as open issues and challenges for information security in interoperable solutions at a systemic level. Recommendations derived from the gap analysis will be brought into the forthcoming phases of KONFIDO to shape its technical solutions accordingly.**

Keywords—**Gap analysis, eHealth, interoperability, cross-border health data exchange, cybersecurity.**

I. Introduction

Important systematic efforts have been made recently in the field of digital security and data privacy protection worldwide. Especially in the EU, driven by the need for cross-border health data exchange across Member States, diverse projects have conducted research along this line, by focusing on access policies, as well as on how to enforce security measures in the underlying data transfers and subsequent storage. Equally important, interoperability is an aspect that is explicitly linked with the technical solutions that shall be in place and their user acceptance.

The EU-funded KONFIDO project (http://konfido-project.eu/) aims to leverage proven tools and procedures as well as novel approaches and cutting-edge technology, in order to create a scalable and holistic paradigm for secure inner and cross-border exchange, storage and overall handling of healthcare data in a legal and ethical way at both national and European level. The project aims to: (a) enhance the trust and security of interoperable eHealth services; (b) provide continuous validation and proof of concept demonstrations, and (c) focus on stakeholders, improving user acceptance as well as adherence to standards, legal rules and ethical directives. To achieve these goals, KONFIDO is organized in four distinct though complementary phases, interacting with each other, namely, 'User requirements'; 'Design'; 'Technology development'; and 'Integration, testing and validation'. As part of the 'User requirements' phase, a systematic gap analysis has been conducted focusing on the security and privacy mechanisms developed and/or used in other projects and initiatives in relation to interoperability at a systemic level.

In general, a gap analysis serves the purpose of identifying the difference (gap) between the current and the target state of affairs (product, process, organization, market etc.). Current state refers to the actual state regarding the analysis focus, while the target state refers to the future state where it should be. This entails the comparison between actual performance with potential or desired performance across a range of areas. For the current study, it means that it is possible to see how well a project, initiative, technology, solution etc. meets a set of requirements as identified as relevant for KONFIDO's further work and final output. This analysis is expected to significantly contribute to an improved design of the project's technical solution as a whole and each of its components /tools separately.

The current paper presents the methods employed as well as the consolidated outcomes of the gap analysis study.

II. Material & Methods

A. Material

As analysis subjects we identified a range of relevant projects, technologies, initiatives, end-user organizations and strategies across four thematic areas, which have been analyzed in detail in the scope of the gap analysis. These were:

- *eHealth Interoperability Frameworks*: Antilope [1], epSOS [2], the Joint Action to Support the eHealth Network (JASeHN) [3] and SemanticHealthNet [4].
- *eHealth Security Software Frameworks*: DECIPHER [5], OpenNCP [6] and STORK 2.0 [7].
- *End-user perspectives across diverse settings in KONFIDO pilot countries*: OUH Odense University Hospital & Svendborg Hospital (Denmark), Santobono Pausilipon Hospital (Italy) and Hospital Clínic Barcelona (Spain).
- *National cybersecurity strategies and reference reports*: the Danish, Italian and Spanish Cybersecurity Strategies as well as relevant ENISA reports [8, 9].

B. Methods

For each area, a group of organizations and people with knowledge and experience in the particular area has been identified and a Working Group within the KONFIDO Consortium was formed per thematic area. The analysis subjects have been reviewed by topic experts against a baseline template of security-oriented criteria (or controls), primarily based on the ISO 27k family of standards concerning information security [10]. The ISO 27k family consists of a broad range of standards that addresses information security either to a specific sector / technology, at an overall management level or with specific topic guidelines. In the scope of this study, the following standards have been considered:

a) ISO/IEC 27002 — Information technology — Security techniques — Code of practice for information security controls (https://www.iso.org/standard/54533.html);

b) ISO/IEC 27010 — Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications (https://www.iso.org/standard/68427.html);

c) ISO/IEC 27040 — Information technology — Security techniques — Storage security (https://www.iso.org/standard/44404.html);

d) ISO 27799 — Health informatics — Information security management in health using ISO/IEC 27002 (https://www.iso.org/standard/62777.html);

e) ISO 22857 — Health informatics — Guidelines on data protection to facilitate trans-border flows of personal health information (https://www.iso.org/standard/52955.html), and

f) ISO/IEC 25010 — Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) -- System and software quality models (https://www.iso.org/standard/35733.html).

Based on the above standards and with input from HIMSS EMR Usability Evaluation Guide for Clinician's Practices (http://www.himss.org/himss-emr-usability-evaluation-guide-clinicians-practices-sample-post-test-questionnaires), a systematic and detailed template for each of the four thematic areas included in the gap analysis was produced. Each Working Group was provided with a baseline template of security-oriented controls organized in various sections and worked in parallel as no group was dependent on the work of the others. In summary, the baseline template relied on the following, upper–level structure: *Security policy; Organizing information security; Asset management; Human resources security; Physical and environmental security; Communications and operations management; Access Control; Information systems acquisition, development and maintenance; Information security incident management;) Business continuity management; Compliance,* and *Usability*.

Instructions on how to use the template were offered to the respondents via examples. Furthermore, predefined sets of responses have also been defined where applicable, in order to prevent errors while facilitating the analysis process for the reviewers. Introductory, interim and final meetings were held across the Working Groups to discuss the plan, their progress and results, respectively. Despite that the utilized templates were identical for the four types of subjects considered in the gap analysis, these were distributed with the understanding that for some of the analysis subjects, a part of the security aspects and control questions might not be relevant in all cases, due to the level of details and specifics that were addressed. Respondents were notified of this aspect and, given their knowledge and expertise, they were able to evaluate the relevance and applicability of each security aspect.

The gap analysis data on each analysis subject were obtained via one or a combination of the methods listed below:

- *Desk research*: A review of available material on the analysis subject. This can be project material (reports/deliverables, presentations, videos etc.) as well as articles and other published material.
- *Expert opinion*: The information is from a source with concrete detailed expertise about the analysis subject. It can be someone who was directly involved in the project, or who works in the respective organization.
- *Interview*: The analysis subject was analyzed through an interview with a person with particular knowledge on the analysis subject and security aspects.

As a result, a comprehensive dataset was compiled for our analysis, but the process also flagged some weaknesses and risks, e.g. relevant projects and initiatives are still evolving. Therefore, mitigations were put in place during the process when possible, making the gap analysis an iterative process.

III. Results

A. eHealth Interoperability Frameworks

The gap analysis of existing eHealth interoperability frameworks showed that while the SemanticHealthNet project refers to information security and references ISO standards as guidelines, the project per se does not provide details concerning information security. The Joint Action to support the eHealth Network (JAseHN) focuses on semantic interoperability of exchanging information in a cross-border fashion and Antilope on quality management and testing processes. In both cases, while some security aspects identified in the baseline template are addressed in the projects, most topics can be considered out of these projects' scope. Concerning epSOS, a distinction must be made between the project itself and the open-source software that came out of the project, namely, OpenNCP (included in the gap analysis of eHealth Software Security Frameworks).

Some indicative common gap patterns were identified through the reviewed interoperability projects/initiatives:

- Cases of inadequate information on aspects concerning 'Information security policy' and 'Management commitment'. For epSOS, the scope of the security policy might have been too narrow concerning also the National Contact Points (NCP) and internal organizational matters.
- 'Assets management' in terms of responsibility, classification and exchange protection may be enhanced.
- 'Compliance' in terms of cryptographic control and information system audit could have been added.

B. eHealth Security Software Frameworks

The gap analysis of STORK 2.0 disclosed an overall adherence to the information security aspects according to the standards. Most gaps were related to what can be considered as local operations rather than the technology per se. However, the reviewed STORK 2.0 documentation, for instance, does not reference any controls against 'Protection against malicious and mobile code', 'Back-up' and to some extent 'Network security' and 'Media handling'. The STORK 2.0 project results are carried over to eIDAS, which is the Regulation 2014/910 on electronic identification and trust services for electronic transactions in the internal market. Furthermore, the review of DECIPHER showed several gaps. However, DECIPHER is a pre-commercial procurement (PCP) project, which to a large extent impacts its applicability and relevance in relation to a gap analysis of existing eHealth security software. In DECIPHER, the security aspects are not dealt with as the standards define, since the main focus of the project is on the PCP process itself. Finally, according to the OpenNCP project's gap analysis, some shortcomings in relation to 'Information security' have been identified: an audit trail that is potentially forgeable; no protection against malicious cloud provider or administrator; and only basic encryption technologies are used.

C. Local End-user Organisations

A gap analysis of the local end-users was conducted through desk research, interviews with relevant people and expert opinions (e.g. IT staff in hospitals and healthcare professionals) and reveals that the local end-user hospitals in Spain, Denmark and Italy, respectively, all adhere to a high-level compliance with the background standards on information and health security. The gaps identified related mostly to whether or not there was full compliance to the ideal procedures according to the standards.

D. National and European Cybersecurity strategies and Reference reports

The national cybersecurity strategies and ENISA reports address security at a general level given their strategic perspective, so many operational gaps were expectedly identified. However, for the most part, these gaps were not considered as significant. Nevertheless, it has been identified that there are aspects of the baseline template, which are not at all addressed. Furthermore, it should be noted that further elaboration regarding local operational application should be considered.

E. Consolidation of Gap Analysis Outcomes

The gap analysis uncovered barriers and constraints as well as open issues, challenges and recommendations for information security in interoperable solutions at a systemic level. The consolidated outcomes are summarized below:

a) Barriers and constraints:

- Adherence to the security targets and controls set by international standards are met to various degrees but rarely regardless of the analysis subjects.
- Technological advances happen at a pace which can quickly render security mechanisms applied outdated or not state-of-the-art.
- The activities of the projects and frameworks are developed in parallel but not integrated.

b) Open issues and challenges:

- The level of adherence to standards on information security management varies between end-users (very high) to the frameworks, strategies etc.
- Analyzing frameworks does not address the details of the local operations and execution, hence some aspects are perhaps not captured.
- The dependency on adaption and implementation of specific technologies deriving from the frameworks impacts the KONFIDO solution.

c) Recommendations:

Based on the full outcome of the gap analysis, five recommendations for addressing information and cybersecurity in an eHealth setting at a systemic and holistic level were formulated, which are applicable to KONFIDO and its future activities as well as in a broader setting:

- Strive for high adherence to standards across all domains and subjects as it ensures trust and is in line with the end-users' approach.
- Take into account the users of a centralised technology / framework in terms of details of information security.
- Implement state-of-the-art security technologies and measures.
- Ensure information security sustainability in technical solutions.
- Explore further the implementation issues of the relevant security software frameworks.

IV. Conclusions

The conducted analysis has shown a range of gaps in other projects and initiatives, which does give indication of gaps at a systemic level and raises specific issues to consider. Recommendations derived from the gap analysis will be brought into the forthcoming phases of our project, but also have a wider European added value and, hence, will be disseminated appropriately. An iterative process for the gap analysis will strengthen the knowledge pool for KONFIDO and other relevant projects in the domain.

Acknowledgment

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.

Conflict of Interest

The authors declare that they have no conflict of interest.

References

1. The Antilope project: https://www.antilope-project.eu/, last access October 6, 2017.
2. The epSOS project: http://www.epsos.eu/, last access October 6, 2017.
3. The JASeHN project: http://jasehn.eu/, last access October 6, 2017.
4. The SemanticHealthNet project: http://www.semantichealth-net.eu/, last access October 6, 2017.
5. The DECIPHER project: http://www.decipherpcp.eu/, last access October 6, 2017.
6. The OpenNCP project: https://openncp.atlassian.net/wiki/, last access October 6, 2017.
7. The STORK 2.0 project: https://www.eid-stork2.eu/, last access October 6, 2017.
8. European Union Agency for Network and Information Security, Security and Resilience in eHealth: Security Challenges and Risks, December 18, 2015.
9. European Union Agency for Network and Information Security, Cyber security and resilience for Smart Hospitals, November 24, 2016.
10. The ISO 27k family of standards: http://www.iso27001security.com/, last access October 6, 2017.

Author: Janne Rasmussen
Institute: MedCom
City: Odense
Country: Denmark
Email: jar@medcom.dk