Cybersecurity Evaluation of Enterprise Architectures: The e-SENS Case

Tanja Pavleska[1(✉)], Helder Aranha[2], Massimiliano Masi[3], Eric Grandry[4], and Giovanni Paolo Sellitto[5]

[1] Jozef Stefan Institute, Jamova 39, Ljubljana, Slovenia
atanja@e5.ijs.si
[2] Public Administration Shared Services Entity, I.P., Alfragide, Amadora, Portugal
helder.aranha@espap.pt
[3] Tiani Spirit GmbH, Vienna, Austria
massimiliano.masi@tiani-spirit.com
[4] Ministry of Mobility and Public Works, Luxembourg, Luxembourg
eric.grandry@tr.etat.lu
[5] Autorità Nazionale Anticorruzione, Rome, Italy
g.sellitto@anticorruzione.it

Abstract. Technology management through enterprise architectures has already become a widespread practice across large enterprises. Modeling and evaluating the cybersecurity aspect of it, however, has just begun to get the needed attention. This paper presents a cybersecurity evaluation methodology developed for the reference architecture of the e-SENS project and derives a generic framework for cybersecurity evaluation of an enterprise architecture. The evaluation addresses both the high-level design artefacts (the reference architecture) and operational solutions. Therefore, both a conceptual and an empirical framework are developed as part of the methodology. The former extends a goal-based security model with a threat-view incorporating standardized guidelines on security measures, whereas the latter captures and systematizes implemented project-specific security practices. The resulting methodology effectively supports the evaluation and is easy to grasp by non-technical people. Moreover, it is lendable to formalization, supporting a semi-automatic process of solution architecture design.

Keywords: Cybersecurity · Enterprise architecture · e-SENS · Evaluation methodology · Framework

1 Introduction

Supporting the management of technology by enterprise architectures, while essential and useful, poses additional requirements for effectiveness and efficiency, such as: accounting for the life cycle of the different aspects and attributes of the architecture (interoperability, (cyber)security, change management, variability, etc.). Various models to address these requirements have been proposed [1–3]. However, they mainly address small-scale solutions, lack an account of a standardized process of technology

Published by Springer Nature Switzerland AG 2019
J. Gordijn et al. (Eds.): PoEM 2019, LNBIP 369, pp. 226–241, 2019.
https://doi.org/10.1007/978-3-030-35151-9_15

management or require fully manual work on the issue under consideration. In this paper, we present a cybersecurity evaluation methodology developed for the reference architecture of the e-SENS project.[1] The aim is to derive a generic framework for cybersecurity evaluation of enterprise architectures that would be interoperable, applicable to both small and large-scale scenarios, understandable by non-technical people, but also technically sound to the extent that it is fully automatable and reusable.

The Electronic Simple European Networked Services (e-SENS) project aimed at delivering reusable architecture Building Blocks (BBs throughout this paper) for the implementation of cross-border and cross-sector digital services. In addition to developing BBs as elementary parts of the e-SENS Reference Architecture (e-SENS RA), corresponding implementations in several domains were piloted (eHealth/ePrescription, eProcurement, eJustice, Business LifeCycle and eAgriculture), providing a proof of the architecture feasibility and effectiveness. The e-SENS approach adopts the TOGAF9 concept of a building block [1]. The BBs are combined and consolidated into Solution Architecture Templates (SATs), as used by the European Interoperability Reference Architecture[2], and address specific real-world use-case. The BBs are described along common dimensions, captured by the e-SENS Metamodel [4]. The availability of solution templates not only facilitates the use of the BBs, but guides developers in the realization of custom solution architectures. In doing so, significant challenges appear due to the requirements for architecture solutions and the standards and security solutions. Thus, an evaluation methodology is needed that is applicable at architectural level, but which also presents the various features in a uniform way for all of the BBs.

The evaluation presented in this paper includes model-based assessments at SAT-level from the aspect of (cyber)security. Although designed for e-SENS, the methodology has been generalized and proven applicable for other contexts as well [5]. It combines two complementary evaluation frameworks: conceptual and empirical. The former builds on a standard goal-based security model known as the Reference Model for Information Assurance & Security (RMIAS) [6]. This model was augmented by a threat-view incorporating the ENISA guidelines on security measures [7] to provide a holistic account of the security properties of the reference architecture. The empirical framework, on the other hand, is an evaluation tool for the pilots, designed according to the conceptual framework. It captures and systematizes the security practices deployed in the solutions based on the reference architecture and provides recommendations on how the BBs' specifications can be fine-tuned to meet the security goals.[3]

This paper is structured as follows: the next section introduces the two parts of the evaluation methodology – the conceptual and empirical evaluation frameworks. Each is supported by a relevant discussion or recommendations related to the obtained results.

[1] https://www.esens.eu/.

[2] https://ec.europa.eu/isa2/solutions/eira_en.

[3] Note that the terms "security" and "cybersecurity" are used interchangeably throughout the paper: while the RMIAS addresses information security (& assurance) in general, the evaluation described here focuses on cybersecurity, as information in e-SENS is mainly in electronic form.

Then, our work is placed among the state of the art approaches. Finally, we conclude and point to some future work plans.

2 Methodology: The Conceptual Framework

The conceptual framework aims at assessing how the technical specifications contribute to meet the security goals. Two approaches are usually followed in the practice of information assurance and security: a goal-based and a threat-based approach [8]. The former defines the security goals, and then selects the countermeasures to reach these goals [9]. The latter analyzes the threats and vulnerabilities of the system to be secured, and then selects countermeasures mitigating the threats and vulnerabilities [10]. In a cybersecurity evaluation at architecture level, a goal-based approach is usually taken, as a threat-based requires detailed analysis of all system vulnerabilities, and a detailed knowledge of the system behavior history. Such data is not available at system design.

The objective of the proposed methodology is twofold: (1) the core security goals must be general enough to address all of the domain needs; and (2) they should be applicable to any architecture derived from the BBs. Therefore, both a goal-based and a threat-based approach are combined in this work in a coherent manner.

Figure 1 depicts the application of the conceptual framework to the e-SENS System, which is represented in the core diagram with all its assets: Network, Hardware, People, Information, etc.

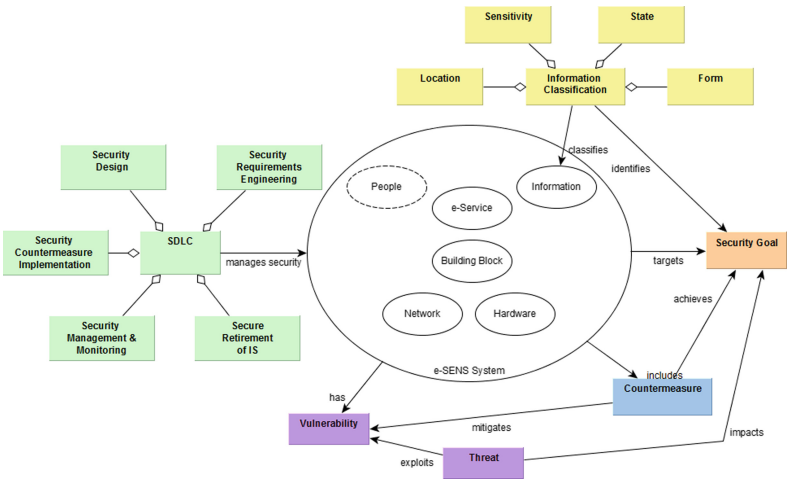


Fig. 1. The conceptual framework of the cybersecurity evaluation (Color figure online)

The security aspects (i.e. dimensions) composing the RMIAS goal-based view are: *Security Development Life Cycle SDLC* (represented in green), *Information Classification* (which corresponds to the RMIAS *taxonomy*), *Security Goals* (in orange) and *Countermeasures* (in blue).

- SDLC illustrates how security is built up along the system development life cycle;
- Information Taxonomy characterizes the nature of information being protected;
- Security Goals contain a broadly applicable list of eight security goals: Confidentiality; Integrity; Availability; Accountability; Authentication (and Trustworthiness); Non-repudiation; Privacy and Auditability.
- Countermeasures categorize the countermeasures available for information protection.

To address the threats and vulnerabilities of the system, the goal-based model is complemented by a threat-view, which is represented by the purple blocks in Fig. 1.

2.1 RMIAS and the Goal-Based View

The evaluation is preceded by goal-based modeling, performed along each of the RMIAS dimensions. Information classification helps to understand the relevant security goals associated with the system under evaluation. Information is classified by:

- Form: in e-SENS information is exclusively manipulated in electronic form;
- State: in e-SENS it can be in one of the following states: Creation, Transmission, Storage, Processing, Destruction;
- Sensitivity: in e-SENS it can be either confidential, or non-confidential;
- Location: in e-SENS it is always at controlled locations.

The e-SENS System can be described through different views; in this evaluation, we concentrate on the architecture description relevant to the various eServices. The evaluation includes the cross-border SATs that were most employed by the pilots while carrying the bulk of the security mechanisms: eID, eDelivery, Non-repudiation, Trust Establishment, eDocuments, and Semantics [11–13].

The goal-based assessment is performed as follows:

1. The architecture of the system to be protected is described, and the various stages of information manipulation are identified;
2. For each stage, the information is categorized according to the information view of the security model. The associated security goals are deduced by the security expert performing the evaluation (See Table 1 for example);

Table 1. Information classification template for the SATs; an example.

Information	Sensitivity	Location	State	Security goal
Authentication request	Non-confidential	Controlled	Transit	Integrity
Secure message transfer	Confidential	Controlled	Transmission, storage	Authentication, Non-repudiation
…	…	…	…	…

3. The security goals devised are then analyzed and classified in relation to the relevant architecture (as shown in Table 2). The most generic description for each column is Node_X - Node_Y; this refers to information exchange in three general cases: (a) National infrastructure (b) Cross border infrastructure and (c) Direct end-to-end.

Table 2. Template for goal-based end-to-end analysis of each SAT

	Name of the SAT being evaluated					
		Point of assessment				
SECURITY GOAL		**End-point 1**	**Node_A**	**…**	**Node_X**	**End-point Y**
	Access Control	Yes	Yes		...	Yes
	Authentication	Yes	Yes		…	Yes
	Confidentiality	No	Yes		…	No
	Integrity	Yes	Yes		…	Yes
	Non-repudiation	No	No		…	…
	Accountability	…	…		…	…
	Auditability	…	…		…	…
	Privacy	…	…		…	…

2.2 ENISA Guidelines on Security Measures and Threat-Based View

The ENISA guidelines on security measures sublime an extensive list of national and international EU electronic communications standards into a set of security objectives divided by domain [7]. They outline 25 security objectives, each analyzed through various security measures and supported by evidence testifying that an objective was met. The security measures are grouped in 3 sophistication levels, whereas the security objectives are divided in 7 domains of application. This provided a suitable framework of complementary views to the goal-based security evaluation.

As information is the main security asset in e-SENS, many of the ENISA security measures and objectives were not addressed by the evaluation. To determine those that are relevant for e-SENS, a mapping of the contextual and security traits between the e-SENS security needs and the ENISA provisions is performed, as presented in Fig. 2 showing the whole set of ENISA security objectives divided by domains. To represent the relevance for the e-SENS context the boxes are colored and assigned the following semantics: red denotes the relevance of that particular security objective (SO) for the evaluation in the concrete domain (Dx); green represents the SOs for which e-SENS can provide recommendations to future adopters of e-SENS building blocks; and transparent (white) boxes denote that the SO is not relevant for the evaluation purposes. Mapping the contextual and the security traits of RMIAS to the ENISA framework

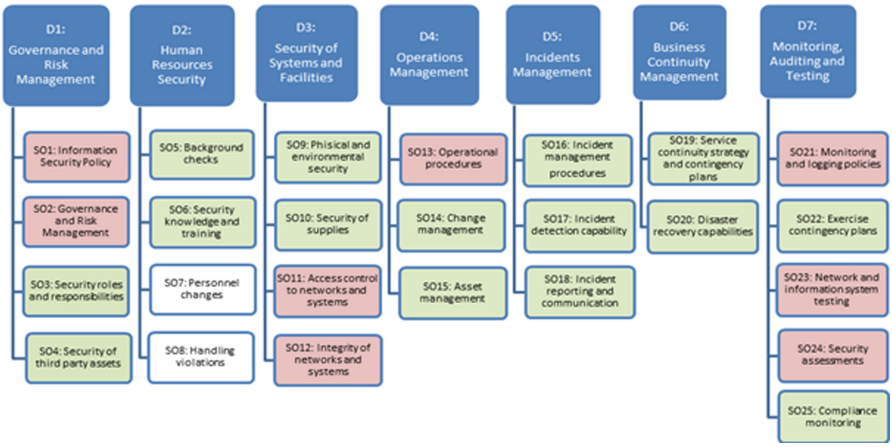


Fig. 2. Relevance of the ENISA guidelines in the context of e-SENS

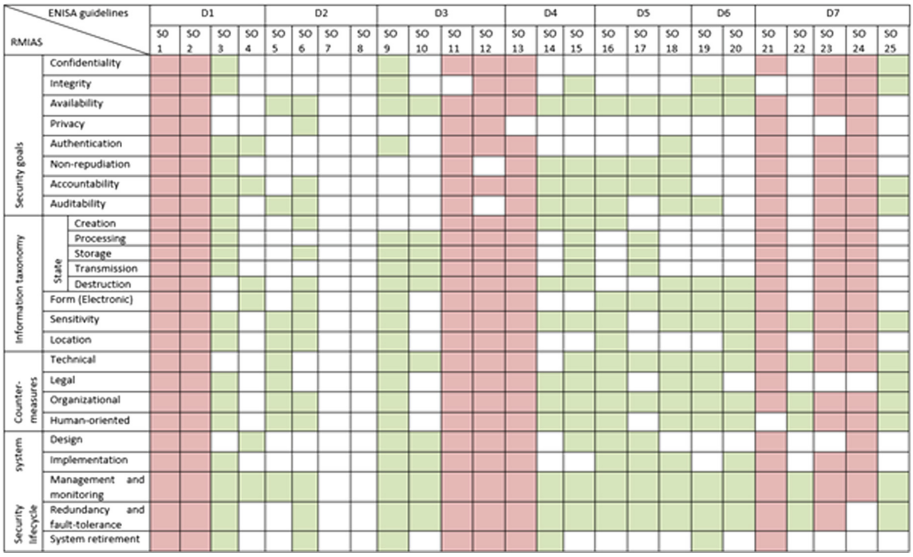
provides sufficient practical and scientific rigor in accomplishing the task of a holistic cybersecurity evaluation. Moreover, it enables the extraction of specific guidelines and recommendations for the security measures that must be adopted to meet the objectives.

2.3 Integrating RMIAS Dimensions and ENISA Objectives

Mapping RMIAS to the ENISA technical guidelines establishes correspondence between each of the RMIAS dimensions and the ENISA Security objectives by domain. It is represented as a matrix: each entry that lays at the intersection of an RMIAS row-entry and an ENISA column-entry contains the information about the reciprocal relevance of the two. The same matrix can also contain the results of the assessing of relevance in the specific context. Such results are denoted by red-green-white coloring the particular entry, with the same meaning as presented in the previous section.

As Information is the main asset to be protected by the security mechanisms specified by the e-SENS RA and implemented by the pilots, the mapping of Information Taxonomy is granulated into: Creation, Processing, Storage, Transmission, and Destruction. The result is a 25 × 25 matrix (see Table 3) with one additional dimension for *Relevance* represented by a particular color, as explained previously. This additional dimension can be further fine-grained, for example by giving it numerical weights. It enables a threat-view by domain for each goal-based dimension and its sub-dimensions. Providing a threat-view starts as a subjective assessment, as the decision to denote a particular table entry as relevant or not depends on the analyst's expertise and experience. This is also one of the inherent drawbacks of a threat-based method. To ensure the least bias possible, the evaluation has been reviewed by more experts who were involved in both the design of specifications and in pilot implementations. The most important result from this cybersecurity evaluation, however, is the methodology

Table 3. Mapping RMIAS to ENISA guidelines by relevance for e-SENS security mechanisms



itself, which not only is it not subjective, but is based on rigorous standards and scientific approaches.

To give an example, we can refer to the goal-based analysis of the pilots (presented in Sect. 3.2). There, we show that the security goal *Availability* requires proper account. In Table 3, there are 19 security objectives that provide a threat-view of Availability relevant for e-SENS across all 7 domains. Eight are mandatory (in red) for specification and implementation, whereas for 11 (in green) e-SENS provides recommendations to future adopters. Depending on the domain, a catalogue of security objectives can be designed to guide the specification and implementation of relevant security measures. Governance and risk management can be similarly addressed.

Finally, it is worth noting that this table can further be checked for compliance with international standards by comparing it against the mapping of ENISA's domains and security objectives to international standards in Sect. 6 of the ENISA report [7].

2.4 Discussion

The evaluation of the e-SENS SATs demonstrated that the specifications are grounded on well-established security standards and solutions. Furthermore, all security goals can be addressed by adopting one or a composition of BBs. Information in all its states and locations can be adequately accounted for, depending on its sensitivity, in order to devise a certain security goal. One of the most important traits of the e-SENS RA is that its BBs are fully interoperable. This implies that by interconnecting the relevant BBs, a certain security property can be leveraged to meet a desired security goal.

By presenting a high-level overview of the architecture to which a security mechanism applies, and by providing a catalogue of the security goals addressed by each of the SATs, a non-technical person is able to grasp the potential of a certain solution to satisfy given security requirements. Moreover, by providing a detailed elaboration of the technical processes behind a solution and reference to the standards on which it is based, a technical person gets the support to build a conceptual evaluation model to satisfy the desired security goals. Hence, the analysis performed here provides a common ground for understanding between various levels of experts in a given organization. It also helps to organize the security policies spread over multiple domains. Furthermore, it not only permits tracing contradictory security policy statements, but also facilitates the identification of weak or omitted security policies. Complemented with the more domain-specific security measures offered by the threat-based analysis, it may contribute to more cost-effective and efficient solutions for both public administrations and private organizations. Finally, the modularity of the analysis by security domain, objective, goal and countermeasures allows to detect opportunities for further improvement of both the system/architecture and the implemented security mechanisms.

3 Methodology: The Empirical Framework

To provide a holistic view of the cybersecurity evaluation of the architecture and validate the conceptual framework as a generic methodological tool, an empirical framework was devised. This framework aims to close the gap between concept and realization. A questionnaire[4] was deemed as the most effective method to gather information, given the time-frame available. It was designed to extract expert knowledge and experience from the implementation of security mechanisms in the pilots. In addition to the security aspects, some general system properties were also investigated. The results obtained with the empirical evaluation framework directly answer to the objectives of this work, while providing insights into the interdependencies between the BBs' specifications and their implementations.

3.1 Questionnaire Design

The questionnaire design follows the RMIAS premises. It contains five sections: four focus on the RMIAS dimensions (Security goals, Countermeasures, Information Taxonomy and System Security Lifecycle), and one obtains information about Trust models implemented by the pilots. The results from the questionnaire in turn fed the threat-view analysis of the architecture, providing the needed knowledge about the system behavior and establishing a feedback loop between the design specifications and the architecture implementation. Moreover, they provided valuable insights into how the SATs address the same security objectives as the architecture building blocks they are composed of.

[4] http://tiny.cc/yjwfaz.

3.2 Results and Analysis

The questionnaire was filled in by the relevant experts of all piloting domains. Following are the comparative and qualitative analysis of their feedback, divided by sections.

Security Goals. The first section investigated the employment of security mechanisms to address the desired security goals. As shown in Fig. 3, all security goals set to be addressed by the specifications have been a requirement that was also addressed by one or more of the pilots. One of the pilots, (eTendering) employed mechanisms for addressing almost all security goals, which was to some extent expected, considering that it was structurally the most complex and had to cope with all information states during its lifecycle.

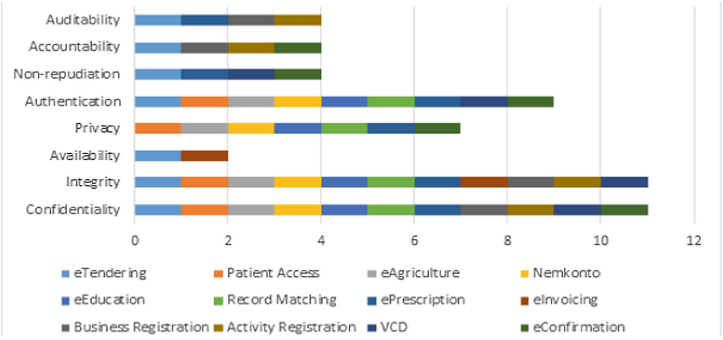


Fig. 3. Security goals addressed by the pilots

Confidentiality and Integrity were addressed by almost all of pilots, whereas the results for Availability reveal that further considerations are needed in this direction. On the one hand, assuring Availability of all resources and hardware, fault-tolerance and redundancy is country-dependent. However, considering the fact that Hardware, Software and Networks are among the security assets stated by the pilots, Availability is expected to be among the top security goals to be addressed. The fact that no pilot has reported consideration of Redundancy and Fault-tolerance, is thus of no surprise. At the same time, it reveals a need for better consideration and proper accounting for Availability as one of the major security goals.

Information Taxonomy. Information in e-SENS is tackled in all states in its lifecycle: Creation, Transmission, Storage, Processing and Destruction. Some pilots did not employ mechanisms to handle information securely in every state (see Fig. 4a), but all pilots ensure secure transmission of information. However, dealing with information in a particular state is highly context-dependent. Thus, no claim can be made on whether some security mechanisms are lacking or if information is not handled securely. Secure processing and creation of information were addressed to a greater or lesser extent.

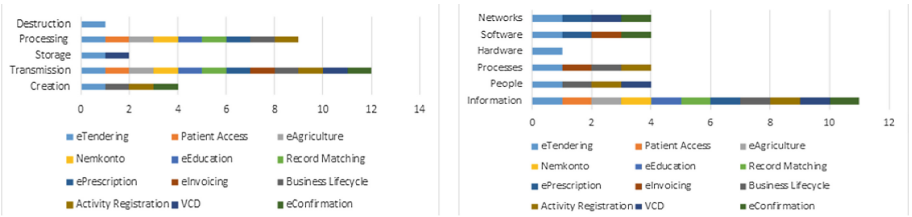


Fig. 4. (a) The state in which Information is being dealt with; (b) Entities concerned by the security mechanisms implemented in the pilots

Variety of entities for which Information is the main asset are concerned in the implementation of security mechanisms (as shown in Fig. 4b). Software, Networks, Processes and People are also major security assets, whereas Hardware is only rarely addressed. However, the number of security assets and the frequency of implementation of certain security mechanism are of less importance; the impact of the particular asset for the overall system and the impact of the failure of a certain security mechanism are crucial. The choice of entities to be addressed by the security goals is both context- and mechanism-dependent. However, as humans are at the core of all systems, it can be observed that the human-factor is poorly addressed by the security mechanisms. This is especially important if one considers that countermeasures can be legal, organizational and purely human-oriented. Next, broader analysis of this issue are presented.

Countermeasures. Regardless of whether a certain pilot implemented security mechanisms with a concrete threat-model in mind, countermeasures could still be in place due to mere operational system requirements. The countermeasures' types investigated here are: (i) Technical; (ii) Legal; (iii) Organizational; and (iv) Human-oriented. Technical countermeasures that are widely employed by the pilots are encryption and authentication. They are complemented with legal countermeasures in the form of agreements/contracts, whose type depends on the pilot's needs. Policies are the organizational countermeasures implemented, whereas audit was reported by only one of the pilots (eConfirmation). Human-oriented countermeasures are largely lacking, with 'Motivation' and 'Operational guidelines' being the only ones considered.

The implementation of countermeasures is highly context-dependent. Not every pilot has the same assets to secure or deals with the same risks. For e.g., whereas most pilots employ only encryption and authentication as technical countermeasures, the eHealth pilot also implements policy-based access control for authorization, and patient-informed consent to address Privacy. However, starting from the lowest level possible, training of both public administration, citizens and workers must be enforced, since user knowledge and behavior are the first line of defense against cyber-threats.[5]

[5] ENISA guidelines (SO6) in D2: Human resources security.

Trust. Trust mechanisms facilitate the accomplishment of Integrity and Accountability. Confidentiality, although mainly addressed through encryption, is also strengthened by trust in the underlying infrastructure. All pilots employ one or more types of trust mechanisms, depending on the needs of the intra-domain or the cross-domain trust establishment. Although the Trust Network PKI[6] is the most widely employed BB, all of the Trust Establishment BBs are used by some of the pilots. One trust issue reported by the pilots is that self-signed certificates are still widely used. Although they may decrease the overall security risk of a transaction in some situations, self-signed certificates cannot be revoked, allowing an attacker with authorized access to monitor and inject data into a connection, or spoof an identity if a private key was compromised. This points to the need for adequate risk analysis, which was not done by any of the pilots.

Trust analysis does not only help in the consolidation of security policies across a system architecture, but it points to the fact that trust in the overall architecture is as important as securing the information that flows through that architecture. The presented methodology enables this kind of trust reasoning and can be used to assure the adopters of any of the architectural solutions of their desired trust properties.

Security System Lifecycle. This section explored the general lines of development of the security mechanisms. In a way, it extracts the bigger picture of the security design and management of the system.

Most e-SENS pilots base the choice for employing trust and security mechanisms on an inherited infrastructure (from previous Large Scale Pilots[7]). The results are to a certain extent a testimony of the ability to adapt novel security mechanisms to earlier security infrastructures. This adaptability of security solutions is also an argument for the architecture sustainability with respect to the BBs' security capabilities. Therefore, the fact that all pilots claim low expectations for frequent mechanism updates comes as no surprise. In terms of stability of the security mechanisms, all security experts responded that small changes in the security mechanisms would not have a big impact on the remainder of the system. However, most of the pilots reported no redundancy considerations in the security mechanism design. This again points to the need for risk-modelling and analysis, and introduction to proper countermeasures during system design.

Overall Evaluation of the e-SENS Security Measures. After performing the cybersecurity evaluation of all SATs, the overall e-SENS security measures have been evaluated and assigned a sophistication level according to ENISA guidelines. The security measures are grouped in three sophistication levels as shown in Table 4.

Each level corresponds to some criteria judging of its attainment. The results are backed by evidence gathered in support of the judgement. The levels are cumulative, so the evidence for attaining level 2 applies to level 1 as well.

[6] PKI stands for Public Key Infrastructure.

[7] EPSOS (eHealth), PEPPOL (eProcurement), E-CODEX (eJustice), to name a few.

Table 4. Evaluation of sophistication level of e-SENS security measures according to ENISA descriptions

ENISA description of sophistication levels	Assessment of the e-SENS security measures	
	Level attained	Evidence
Level 1 (basic) - Basic security measures that could be implemented to reach the security objective - Evidence for that	**Yes**	Basic security measures are in place - the arguments were detailed in the BB's security evaluation and the pilots security evaluation
Level 2 (industry standard) - Industry standard security measures to reach the objective and an ad-hoc review of the implementation, following changes or incidents - Evidence for that	**Yes**	Industry security measures are in place - demonstrated in the pilots security evaluation and in the assessment of technical maturity of the e-SENS RA's building blocks
Level 3 (state of the art) - State of the art (advanced) security measures, and continuous monitoring of implementation, structural review of implementation, taking into account changes, incidents, tests and exercises, to proactively improve their implementation - Evidence for that	**Not Yet**	Not all e-SENS BBs have reached full technical maturity and scalability readiness; no comprehensive documentation is provided to claim accounting for changes, incidents and tests to improve the implementation of the security measures However, solid basis for reaching level 3 can be provided: the current analysis is a form of a structural review and a proactive step towards recommendations to improve the security measures implementation

The possibility of e-SENS RA to be adapted to the domain needs and to evolve with the system speaks of its flexibility to retain the reached sophistication level. This wraps up the complementary view on the goal-based approach and provides the cybersecurity evaluation with operational recommendations for securing the e-SENS RA solutions.

3.3 Discussion

While not all pilots address all security goals or employ countermeasures, the fact that all security goals were addressed, information has been accounted for in all of its states, all entities were tackled by some of the security mechanisms and technical, legal, human and organizational countermeasures are in place, testifies that the e-SENS RA satisfies the cybersecurity requirements by the pilots. However, not all recommendations for a secure system operation and maintenance can and should be addressed by a single project; imposing technical, legal, and organizational requirements is dealt with on national or domain level. While desirable good practices may be part of its recommendations, mandatory security measures are not.

Complementing a reference architecture with a methodology to encompass the security goals from design time with tools to support the cybersecurity assessment is of paramount importance for meeting the regulatory requirements as well. Clearly, the mechanisms employed depend on the particular context and use case and cannot be joined by a universal security mechanism. The results from the questionnaire demonstrate that the generic security properties provided by the e-SENS RA are also reflected in the pilot implementations.

To validate the adoption of e-SENS building blocks, special events named connect-a-thons were organized within the eHealth pilot, where conformance and interoperability tests were performed assisted by tools[8] and skilled personnel [12]. The secure and successful cross-border exchange of patient summaries and ePrescriptions was simulated among at least 4 countries. It is the first attempt to reuse this testing methodology for architectural assets created outside the eHealth domain.

This cybersecurity analysis joins the benefits of a goal-based approach with the systemic nature of a threat-view on security management. It also helps to organize the security policies spread over multiple domains. Furthermore, it not only permits tracing possible contradictory security policy statements, but facilitates the identification of weak or omitted security policies as well.

4 Related Work

The EU is making significant steps toward cross-border eServices interoperability and implementation. The 2018 edition of eGovernment summarizes related policies and activities in 34 countries and enlists cybersecurity as an emerging topic [14]. The NIS Directive aims at ensuring a high level of network and information security across Europe [15]. As a response to the directive requirements, ENISA, national governments and National Regulatory Authorities engaged in joint work in order to achieve harmonized implementation. Three non-binding technical documents were provided as guidance to the NRAs across EU member states [7, 16, 17]. The presented analysis is a contribution in similar direction and an effort to bridge technical solutions with regulatory policies and standardization.

There are approaches that cover one or more aspects addressed by our work [18, 19]. In addition, [20] describes a thorough process to include and evaluate security aspects in all stages of the Information System lifecycle: requirement elicitation, acquisition, design and implementation, operation and maintenance, and disposal. Although security evaluation is included in the process, it follows a threat-based approach and offers no evaluation framework or any reference or enterprise architecture the systems might conform to. Evaluating certain cybersecurity attributes of enterprise architectures was approached in [2, 3], which mainly rely on human effort. The same stands for addressing interoperability in enterprise architectures [21]. Zuccato et al. [22] provide a holistic account of "security requirements profiles" in an organization by

[8] The Gazelle test suite, http://gazelle.ihe.net.

assembling a set of "modular security safeguards". However, they are concerned only with the technical aspects and mainly serve the solution developers.

There is criticism about security design frameworks deemed to be too focused on the technical aspects and falling short in detecting and addressing potential design conflicts [23]. An example of this is a system that should implement both anonymity and auditability. By joining the goal-based approach with a threat-view, the issue of contradictory requirements in technology management through enterprise architectures is addressed from design time. Finally, the generic framework presented here is easy to understand by a non-technical person, while offering sufficient technical guidance for the (cyber)security experts.

5 Conclusion and Future Work

Secure information exchange platforms are crucial to the correct functioning of the services they support. The methodology presented here can be successfully applied for a model-based evaluation in a practical setting. It bridges technical and business solutions with the latest regulatory policies and frameworks. The employment of RMIAS in practice has led to a goal-based security analysis of each architecture construct, identifying how the technical specifications associated with them contribute to meeting the security goals. The empirical security evaluation showed that although the implementations were able to address the security goals, additional availability measures, proper risk analysis, and provision of human-oriented countermeasures require refinement of the architecture to provide further tools to reach the security objectives.

Designing a methodology to analyze security measures provided by the implemented security mechanisms and integrating the outcomes of such analysis into the specifications allows for a technical person to cope more easily with the dynamics of security changes that a system may require. Furthermore, by enabling a non-technical person to understand the needs for implementing a certain security measures and the implications of not addressing it adds value in terms of usability of the system itself and for aligning the managerial requirements with the technical possibilities that an architecture offers.

Although each e-SENS pilot performed the evaluation of the architecture via domain-specific methodologies (e.g., connect-a-thons in eHealth), we pursue two independent approaches for the security assessment of the building blocks. Firstly, we plan to evaluate the eHealth pilot architecture with a tool such as securiCAD[9]. Secondly, we will formalize the conceptual framework of the methodology in order to enable a semi-automatic solution architecture design and help the architect deal with the variability and optionality of the design choices. An immediate step towards the automation of solution architecture design is thus the automation of the quality-attributes check. One way to do that is by employing denotational semantics as the formal apparatus, but other possibilities will also be tested. Therefore, an open-access

[9] https://www.foreseeti.com/community/.

implementation tool will be created to allow reusability and testing of the methodology, and moreover, implementation into real-world setting.

References

1. Korman, M., Lagerström, R., Välja, M., Ekstedt, M., Blom, R.: Technology management through architecture reference models: a smart metering case. In: 2016 Portland International Conference on Management of Engineering and Technology, pp. 2338–2350 (2016)
2. Sommestad, T., Ekstedt, M., Holm, H.: The cyber security modeling language: a tool for assessing the vulnerability of enterprise system architectures. IEEE Syst. J. **7**(3), 363–373 (2013)
3. Holm, H., Shahzad, K., Buschle, M., Ekstedt, M.: P^2CySeMoL: predictive, probabilistic cyber security modeling language. IEEE Trans. Dependable Secure Comput. **12**(6), 626–639 (2015)
4. Grandry, E., e-SENS Architecture team: D6.7 e-SENS European Interoperability Reference Architecture. European Commission, 31 Mar 2017
5. Masi, M., Pavleska, T., Aranha, H.: Automating smart grid solution architecture design. In: 2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), pp. 1–6 (2018)
6. Cherdantseva, Y., Hilton, J.: A reference model of information assurance & security. In: Proceedings of the 2013 International Conference on Availability, Reliability and Security, Washington, DC, USA, pp. 546–555 (2013)
7. ENISA: Technical Guideline on Minimum Security Measures — ENISA (2014)
8. Röhrig, S.: Using Process Models to Analyse IT Security Requirements. University of Zurich (2003)
9. Anton, A.I., Earp, J.B., Reese, A.: Analyzing website privacy requirements using a privacy goal taxonomy. In: Proceedings IEEE Joint International Conference on Requirements Engineering, pp. 23–31 (2002)
10. Pfleeger, C.P., Pfleeger, S.L.: Security in Computing, 4th edn. Prentice Hall PTR, Upper Saddle River (2006)
11. DG CONNECT: Introduction to the Connecting Europe Facility eDelivery building block. European Commission (2015)
12. eHDSI Business Analyst: Non-repudiation mechanism - eHealth DSI Operations - CEF Digital (2019). Accessed 02 Aug 2019
13. What is eID: CEF Digital. https://ec.europa.eu/cefdigital/wiki/cefdigital/wiki/display/CEFDIGITAL/What+is+eID. Accessed 02 Aug 2019
14. Digital Government Factsheets – 2018. Joinup. https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/digital-government-factsheets-2018. Accessed 01 Aug 2019
15. European Commission: The Directive on security of network and information systems (NIS Directive). Digital Single Market, 09 May 2017. Accessed 31 Aug 2017
16. ENISA, "Technical Guideline on Threats and Assets — ENISA." 14-Sep-2014
17. ENISA: Technical Guideline on Incident Reporting — ENISA, 24 Oct 2014
18. ISO/IEC/IEEE 24748–1:2018: ISO. http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/28/72896.html. Accessed 01 Aug 2019
19. Bowen, P., Hash, J., Wilson, M.: SP 800-100. Information Security Handbook: A Guide for Managers. National Institute of Standards & Technology, Gaithersburg, MD, United States (2006)

20. Cyber Security Agency of Singapore: CSA Singapore Security-by-Design Framework v1.0. Cyber Security Agency, Singapore, 09 November 2017
21. Ullberg, J., Johnson, P., Buschle, M.: A language for interoperability modeling and prediction. Comput. Ind. **63**(8), 766–774 (2012)
22. Zuccato, A., Daniels, N., Jampathom, C., Nilson, M.: Report: modular safeguards to create holistic security requirement specifications for system of systems. In: Massacci, F., Wallach, D., Zannone, N. (eds.) ESSoS 2010. LNCS, vol. 5965, pp. 218–230. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-11747-3_17
23. Mercuri, R.: Uncommon criteria. Commun. ACM **45**(1), 172 (2002)