KONFIDO: An OpenNCP-Based Secure eHealth Data Exchange System

Mariacarla Staffa[1(✉)], Luigi Coppolino[2], Luigi Sgaglione[2], Erol Gelenbe[3], Ioannis Komnios[4], Evangelos Grivas[5], Oana Stan[6], and Luigi Castaldo[7]

[1] Department of Physics, University of Naples Federico II, Naples, Italy
mariacarla.staffa@unina.it
[2] Department of Engineering, University of Naples Parthenope, Naples, Italy
[3] Department of Electrical and Electronic Engineering, Imperial College, London, UK
[4] EXUS Software LTD, London, UK
[5] Eulambia Advanced Technologies LTD, Athens, Greece
[6] CEA, LIST, Point Courrier 172, 91191 Gif-sur-Yvette Cedex, France
[7] Bit4ID s.r.l., Naples, Italy

Abstract. Allowing cross-border health-care data exchange by establishing a uniform QoS level of health-care systems across European states, represents one of the current main goals of the European Commission. For this purpose epSOS project was funded with the objective to overcome interoperability issues in patients health information exchange among European healthcare systems. A main achievement of the project was the OpenNCP platform. Settled over the results of the epSOS project, KONFIDO aims at increasing trust and security of eHealth data exchange by adopting a holistic approach, as well as at increasing awareness of security issues among the healthcare community. In this light, the paper describes the KONFIDO project's approach and discusses its design and its representation as a system of interacting agents. It finally discusses the deployment of the provided platform.

1 Introduction

The health-care sector has been impacted by the extraordinary evolution of electronic Health (eHealth) applications able to implement health-care practises supported by electronic processes and communication. There are many examples of technology adoption in this area: (i) Electronic Health Records (EHR); (ii) Tele-monitoring Solutions; (iii) Mobile Health (mHealth) applications and (iv) Coordinated care. The implementation of these innovative technologies has been extending the boundaries of national health care systems, but realizing an effective cross-border healthcare data exchange remains hard to achieve. In order to carry out health care services able to operate across countries, issues related to security and privacy, as well as legal constraints, must be faced. The increased number of people traveling for business, education and leisure purposes makes these issues more relevant inside the European panorama thanks to the set-up of

E. Gelenbe et al. (Eds.): Euro-CYBERSEC 2018, CCIS 821, pp. 11–27, 2018.
https://doi.org/10.1007/978-3-319-95189-8_2

the so called Shengen Area[1]. In addition, to reach a high level of human health protection within the European Union, the Directive 2011/24/EU[2] establishes the right for EU citizen to access to the same level of health-care provisioning when they travel across all the EU Member States. EpSOS project represented the first attempt in order to achieve interoperability among Member States while complying with both National and European laws. In particular, by developing the OpenNCP platform it tried to overcome interoperability issues in patients health information exchange among European healthcare systems. However, the growing use of eHealth solutions has led to many advantages in terms of patients life expectancy, but simultaneously has resulted in a proliferation of cyber-crime and in the creation of malicious applications aiming at accessing sensitive health-care data, the privacy and confidentiality of which must be guaranteed. In recent years, several malicious attacks have been indeed observed such as: (i) 100 million Electronic Health Record accessed by hackers in 2015; (ii) 90% of industries outside healthcare are affected by data breaches disclosing health related data they are unaware to store; (iii) 48 National Health Service Trusts affected by the ramsonware WannaCry in May 2017. It is relevant to underline that security problems in health care sector are especially due to the lack of awareness among people. Focusing on the patients, health workers pay less attention to the risks connected to the digital security. In this light, the epSOS European Project aimed by implementing the OpenNCP Platform to guarantee secure access to patient health information between European healthcare systems. It was a relevant step forward the security goal, but a holistic approach to this issue is still a faraway target. Started from the results of OpenNCP, the KONFIDO project aims to increase trust and security of eHealth data exchange as well as to increase awareness of security issues among the healthcare community, adopting a holistic approach. In this light, the KONFIDO solution provides first of all a reference scenario with basic context information on the eHealth data exchange platform provided by the epSOS project; then, we provide a description of the KONFIDO deployment architecture in the context of the OpenNCP platform, by highlighting how the security of OpenNCP data exchange is improved by using KONFIDO; we describe in detail the interaction among the KONFIDO components and we finally give our conclusions. Other aspects of the KONFIDO project are discussed in detail in other recent papers. In particular, the ethical framework that covers such transborder or inter-regional health data exchanges is discussed in [6]. The important issue of user requirements is developed in [11]. Specific physical-based techniques that can be used to generate seeds for cryptography are proposed in [1]. The potential use of the novel technology of blockchains in this context is investigated in [2].

[1] https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen_en.

[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:en:PDF.

2 Cross-Border eHealth Data Exchange in Europe: epSOS/OpenNCP Project

The **epSOS**[3] project (Smart Open Services for European Patient I & II 2008–2014) has provided a practical eHealth framework and ICT infrastructure, based on existing national infrastructures, that enables secure access to patient health information, particularly with respect to a basic Patient Summary (patient general info, clinical data, prescribed medicines, etc.) and ePrescription/eDispensing (electronic prescribing of medicine/retrieving prescriptions), between European healthcare systems. The key aspects used in the epSOS project to guarantee eHealth Interoperability in EU have been the following: (i) Existing national healthcare infrastructures/legislation remain unchanged; (ii) Trust among Member State (MS) is based on contracts and agreed policies; (iii) Information is exchanged but not shared.

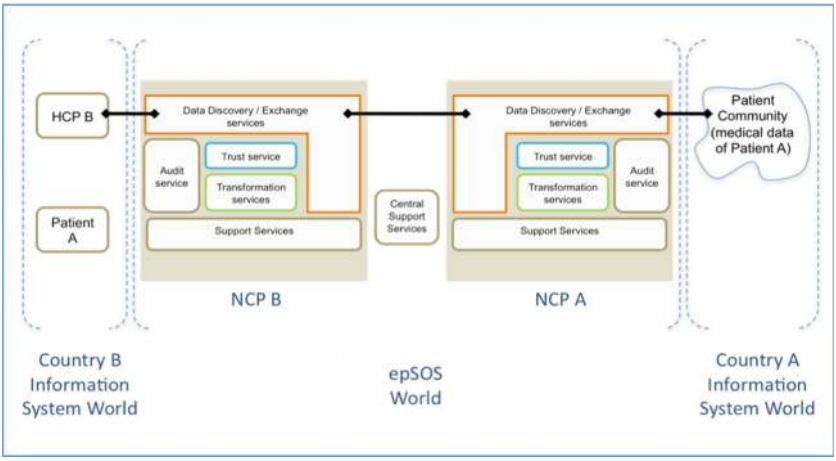

Fig. 1. epSOS logical view (epSOS documentation).

The epSOS architecture is implemented as a set of interacting National Contact Points (NCPs) built on top of Web technologies (SOAP). The platform model adopted by epSOS can be viewed as a federations of services connected with service interfaces defined by specified contracts (a SOA system) (see Fig. 1). In epSOS, the NCP is the main module of cross-border interoperability, exploiting the role of connection the National Infrastructure (NI) to the European Level environment. The components of an NCP can be viewed as a logical wrapper of the different NI. As seen in Fig. 1, the main NCP components are:

[3] http://www.epsos.eu.

- Data discovery exchange services: establish the communication in order to exchange patient data and retrieve information;
- Trust services: ensure the circle-of-trust, i.e. the validation, verification, signing, mapping of messages;
- Transformation services: needed to transform clinical document, i.e. their translation and mapping of taxonomy;
- Audit services: assuring the operations audit and the logs traceability;
- Support services: ensure response time, guaranteed message delivery and session, response time.

The basic blocks of the architecture (epSOS profiles) are built upon three main operations: Query, Retrieve and Notify. Those operations are the unitary blocks needed to perform data exchange between countries in the openNCP context. The approach implemented by epSOS is based on the mediation performed by the NCP. A Health Care Professional (HCP) requests specific information (like a patient summary) from the NCP (or to the NI) of its country. The NCP is in charge of interacting with the other NCPs to retrieve the required information, pivoting the documents (changing the position of information to allow for example the compatibility between different patient summary formats), encoding the pivoted document in the national structure, and interact with the NI.

This approach implements the so called "Circle of Trust". Within epSOS, the consumer (performing query operations) and the provider (retrieve operations) do not know each other. On national side, a Member State may have multiple gateways outside the NCP - representing Member State's health information systems, such as regional ones in order to identify and, later, access patient data. The Circle of Trust is among NCPs. They are solely able to establish mutual trust relationships. An NCP acts as a legal entity which creates a secure link between the epSOS trust domain from the national trust domain. It is the only component that has an identity in both domains. The framework implemented by epSOS to achieve the aforementioned scope has been named OpenNCP.

epSOS Security Aspects. In epSOS, the security of communications is ensured by employing cryptography and secure protocols. The security of communicating parties is not enforced by technical means; it is instead provided by legally binding agreement. Furthermore, epSOS does not offer any protection against the propagation of cyber attacks, because they are out of the project scope. Therefore, attacks which succeed in compromising a NI can exploit the NCP to propagate to other countries. This means that, due to this chain of trust between the NCPs, if one NCP states that someone is authenticated, this will be accepted by the NCPs of other countries. Thus, compromising one NCP (having control of it) can potentially affect the whole infrastructure. In particular, looking at the Patient Summary response process (see Fig. 2), we can observe that the medical data is in plain text in almost all phases performed by the NCP. This means that the security level of these phases is the same as the NCP itself and, hence, an NCP vulnerability can be exploited to generate a data breach on the OpenNCP processes. The KONFIDO toolbox can be used to overcome the

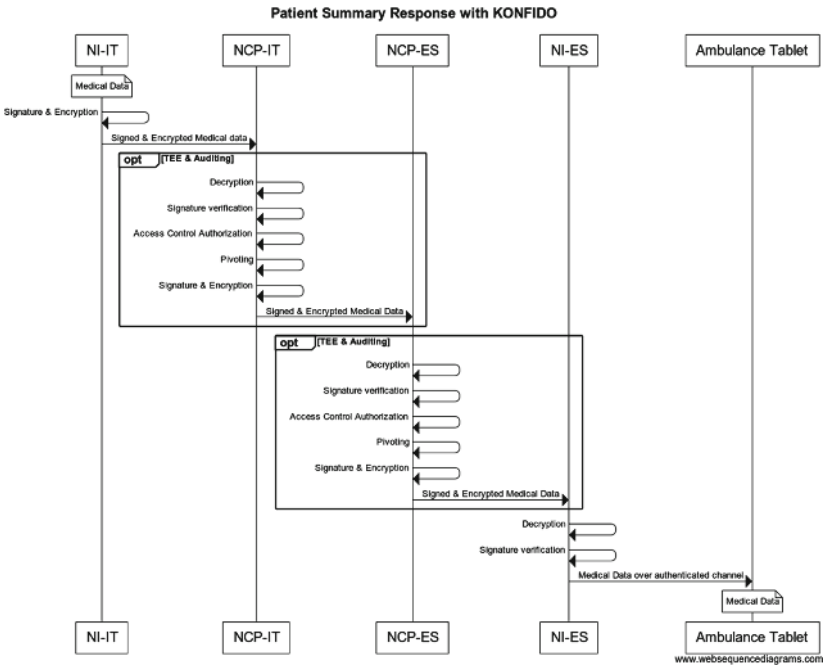

Fig. 2. Patient Summary response with KONFIDO on-top of OpenNCP processes. The *opt* rectangles highlight the actions that will be performed in a Trusted Execution Environment (TEE) and supported by the other KONFIDO technologies. In particular, these actions will be executed in a TEE to guarantee a trust and secure processing of the data, transmitted via a secure communication channel, and supported by an efficient auditing mechanism.

identified vulnerabilities by deploying a set of functionalities to guarantee, for example, that the health data will be never exposed as plain text in an insecure area.

3 Secure and Trusted Paradigm for Interoperable eHealth Services: KONFIDO

KONFIDO[4] is a H2020 project [5], that aims to advance the state-of-the-art of eHealth technologies by providing a scalable and holistic approach for secure inner- and cross-border exchange, storage and overall handling of healthcare data in a legal and ethical way both at national and European levels. In order to address these challenges, KONFIDO takes on a holistic approach by targeting all architectural layers of an IT infrastructure, such as storage, dissemination, processing and presentation.

[4] http://www.konfido-project.eu.

More specifically, KONFIDO will provide a modular set of tools that can be composed to improve the resilience of eHealth data-exchange applications by allowing to address a wide range of possible eHealth scenarios (not only the ones related to OpenNCP) and to solve vulnerabilities in the exchange and processing of health data. As a first step, KONFIDO performed a gap analysis for information security in interoperable solutions at a systemic level [13].

The toolbox offered by KONFIDO includes the following tools/services:

- Trusted Execution Environment (TEE): the new security extensions provided by some of the main CPU vendors;
- Physical Unclonable Function (PUF)-based security solutions that are based on photonic technologies;
- Homomorphic Encryption (HE) mechanisms;
- Customized extensions of the selected Security Information and Event Management (SIEM) solutions;
- A set of disruptive logging and auditing mechanisms developed in other technology sectors such as blockchain and transferred to the healthcare domain;
- A customized eIDAS implementation;
- Publish/Subscribe communication channel;
- TEE communication channel.

The high modularity of the KONFIDO toolbox, allows to address a wide range of possible eHealth scenarios (not only the ones related to OpenNCP) and to solve many vulnerabilities in the exchange and processing of health data.

Trusted Execution Environment. The Trusted Execution Environment (TEE) is created starting from security Software Guard eXtension (SGX[5]) of Intels CPU that allows the creation of protected areas of memory inside the address space of an application. These TEEs, known as *Secure Enclaves* in SGX jargon, provide strong protection of code and data residing inside through encryption and integrity checks of their memory range, performed directly by the CPU. SGX can be considered as a *reverse sandbox*, i.e., it protects applications from the untrusted system outside, comprising the OS, implying that system calls cannot be performed into the enclaves. In KONFIDO, we want to perform specific functions of OpenNCP in SGX enclaves. More precisely, we focus on the enhancement of the NCP host, which is the national gateway in charge of transforming Patient Summaries (PS) from one language to another and where most critical operations take place. As mentioned above, during the PS exchange, in fact, the patient health record is exposed to attacks (see Fig. 2), when it is unencrypted and re-encrypted into the NCP. That is, when the NCP-A receives from the NI-A (National Infrastructure of Country A) a encrypted PS and needs to decrypt, transcode, and re-encrypt before sending it towards another NCP or HCP, an attacker landed on the NCP host may steal or tamper the sensitive patient data by duping the memory content. Hence, the idea is to perform decryptions, transformations, and encryptions of PS into the TEE provided by SGX by integrating

[5] https://software.intel.com/en-us/sgx.

part of the transformation and security modules into an enclave. We also take advantage of an additional important feature of SGX provided by the Remote Attestation (RA) mechanism, which enables service providers to provision applications, and to know with confidence their secrets are properly protected. In this way, an enclave must convince the other enclave with which it is communicating that it has a valid measurement hash, running in a secure environment and that it has not been tampered by establishing trusted channels between end-nodes via the remote attestation of enclaves in order to ensure secure communication among NCP nodes belonging to the community.

PUF-Based Random Number Generator. A photonic device will be designed and developed to enable trusted data sharing and exchanging at cross-border level. The operational properties of this device are based on the intrinsic physical mechanisms that are enabled by a photonic Physical Unclonable Function (p-PUF) [10]. The complexity of the utilized function makes it practically impossible for someone to predict or manipulate the random numbers generated by this device. In more detail, p-PUF devices will be employed in the NCP that will operate as true random number generators and key generators. More specifically, the p-PUF module will be used for generation of:

- True random numbers following either a uniform or a normal distribution for the needs of the HE cryptosystem scheme based on TFHE library.
- Special key triples for the needs of the HE cryptosystem based on the FV scheme. These keys will be delivered to HE module through the TEE module over an SSL enabled channel.
- Keys for enabling SSL communication of the TEE with other TEEs running on different NCP systems.
- True random bits that will be used to increase the entropy of the NCP system, enabling all applications running on the system to have access to a large source of entropy of decent quality, in terms of randomness.

The true random numbers generated by the PUF module will have excellent unpredictability properties, verified by NIST/DIEHARD test suites. They will be used directly or indirectly, through special key generation or system entropy increase, by all other system modules in an effort to increase the security of the entire system.

Homomorphic Encryption Component. Homomorphic encryption (HE) is a recent cryptographic method allowing to perform computations directly on encrypted data, without the need of decrypting it. As such, the encryption schemes possessing homomorphic properties can be very useful to construct privacy-preserving protocols, in which the confidential data remains secured not only during the exchange and the storage, but also for the processing. The Fully Homomorphic Encryption (FHE) schemes are capable to perform additions and multiplications over homomorphically encrypted data (ciphertexts), which correspond to addition and, respectively, multiplication operations over the clear text messages (plaintexts). Therefore, since any function can be expressed as a

combination of additions and multiplications, FHE cryptosystems could compute, in theory, any arbitrary function. The first barrier to the adoption of FHE cryptosystems in real-world applications remains the computational overhead induced by the actual execution on homomorphically encrypted data. However, making use of recent dedicated compilation and parallelism techniques, it is possible to mitigate the performances overhead for a series of real, yet lightweight, applications. CEA crypto-compiler and run-time environment Cingulata[6] (previously known in the research field as Armadillo) allows to easily make the connection between the algorithms written in a high-level programming language and the low-level execution environment required for homomorphically encrypted data and, thanks to dedicated optimization and parallelism techniques, it achieves acceptable performance and security levels. For the KONFIDO project, the HE component used for protecting the exchange and the processing over sensitive patient data provides services at NI level, while for the NCP it is based on a new and ameliorated version of Cingulata. A first step towards its improvement consists in the release of Cingulata in an open source mode. In the context of KONFIDO, another amelioration is the design of a generic interface for different FHE cryptosystems and its support in Cingulata.

SIEM System. The KONFIDO SIEM will extend some existing SIEM solutions [3,4], and customize them based on the specific requirements of a federated environment compliant to the OpenNCP model. The KONFIDO SIEM will be able to analyse information and events collected using a holistic approach at the different levels of the monitored system to discover possible ongoing attacks, or anomalous situations. Considering the high number and heterogeneity of events to be collected and the specific solutions adopted for security provisioning, the development of a SIEM solution customized for such a deployment is required. In particular, the SIEM solution will be able:

- To treat homomorphically encrypted data: The use of homomorphic encrypted data allows for processing of sensitive information without disclosing their content with respect to the privacy requirement of the information;
- To communicate with secure enclaves: The communication capabilities with secure enclaves allows the KONFIDO SIEM to acquire data from a trusted entity in different formats, i.e. homomorphical encrypted data in case of sensitive information, plain data in the other cases;
- To deal with the federated deployment characteristic of OpenNCP-compliant scenarios and, thus, to support a distributed analysis of high volumes of data;
- To provide encrypted output using a PUF base encryption technique: The capability to provide an encrypted output based on PUF technologies allows the SIEM to disseminate sensitive monitoring results readable only to authorized entities.

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

Applying SIEM solutions to a federated eHealth system, such as the one addressed by the KONFIDO project, poses a number of challenges and requires the development of ad-hoc solutions. First of all, the lack of an individual owner of the overall infrastructure requires that the KONFIDO solution must be opportunely thought. The solution that will be implemented to overcome this problem is that each NI had a dedicated SIEM and each SIEM is interconnected with other ones to exchange security metrics via a secure publish subscribe communication channel. The KONFIDO SIEM will be designed to use both misuse-based approaches and anomaly-based ones. The designed algorithms will include both automatic anomaly detection methods, able to distinguish between normal and abnormal operations, and visual analytics methods, able to visually depict characteristics that assist the human operator to discover attacks and their causes (e.g. which users initiated an attack). In particular, the KONFIDO SIEM will be integrated with a Visual Analytics Module for analysing large amounts of data, containing multiple types of information, and detecting anomalies, utilizing both automatic anomaly detection algorithms, such as Local Outlier Factor and Bayesian Robust Principal Component Analysis [7], and visual analytics methods, such as k-partite graphs and multi-objective visualizations.

Blockchain Based Auditing System. The blockchain-based auditing mechanism developed in the framework of KONFIDO is a legally binding system that allows to prove that eHealth data have been requested by a legitimate entity and whether they have been provided or not. The main scenario includes the NCP of one country that requests eHealth data for a patient from the NCP of another country; in this case, both countries need to keep an unforgeable copy of the transaction, in order to be able to prove that the other NCP has requested and/or received the data. To solve this issue, we employ a blockchain (i.e., a distributed data structure) that links each block to its predecessor via cryptography. The OpenNCP node generally interacts with 2 different types of counterparts: the national infrastructure (to retrieve patient data from the national healthcare system) or another OpenNCP node (to retrieve patient eHealth data from another country). Each event of this type is stored as a log file and OpenNCP provides a web-based interface to view registered events and critical logs. In order to capture, filter, timestamp and encrypt the most critical logs that refer to cross-border data exchange between two NCP nodes in different countries, we will adapt the SmartLog log management system. The encrypted log files will then be stored on the KONFIDO distributed ledger. Given the fact that only authorised nodes will participate in the KONFIDO blockchain, we will employ a permissioned blockchain, where an access control mechanism will define who can join the system. The KONFIDO blockchain-based auditing mechanism will interact with the SIEM system to report any abnormal activity on the blockchain and the TEE to perform encryption of log files that contain sensitive information.

eIDAS Based Authentication System. OpenNCP will be extended to provide eIDAS-compliant authentication for its users. eIDAS-compliant authentication will take two different forms, considering the two different kinds of users in the system:

a Healthcare providers, like physicians and pharmacists, that must access the system with a strong digital identity, issued by their country of residence;
b Patients, that could access the system using an eIDAS cross-border authentication.

For each one of the three piloting countries, at least one authentication scheme will be supported. The deployment of the eIDAS Nodes for each of the eIDAS-participating countries is still at the beginning, so a sketchy eIDAS Node to manage the authentication requests for patients from the three piloting countries will be developed. This node will be based on the CEF eID sample implementation of the eIDAS Node, that is freely available to be customized. OpenNCP authentication takes place in the Portal component, which is a Liferay Community Edition application server. The Liferay authentication process is based on a modular and extensible approach, that shows how it is possible to have different authenticators. As such, two different authenticators will be implemented: one that authenticates locally, for healthcare providers, and one that authenticates with a remote eIDAS Node.

3.1 KONFIDO Deployment Architecture

Considering the OpenNCP scenario and the relative vulnerability assessment, the deployment architecture and distribution of the KONFIDO toolbox is presented in Fig. 3. The KONFIDO toolbox is deployed in all actors of the scenario with varying functionalities depending on the actions to be taken and on the hardware available. In particular:

– In each NCP, the entire KONFIDO solutions will be deployed. A TEE will be used to secure all actions needed to achieve a secure patient summary exchange; a PUF component will be deployed and integrated to achieve an unclonable key generator that can be used to generate keys, certificates and to secure the communication channels; an eIDAS service will be used to improve the actors authentication; the Auditing Services will be used to be compliant with log management/storing regulations; a HE technique will be used to allow the data processing for example of the PS without having to use the relative plain text.
– In each NI, a light version of the KONFIDO toolbox will be installed. The minimum set of KONFIDO solutions that must be installed is composed by the TEE. The TEE is needed to secure the transmission of the patient summary. Other tools are optional, in particular for the PUF component

(considering that an additional hardware is needed), its installation is required only on the corresponding NCP. The NCP will provide the PUF services to the NI via specific APIs offered by the TEE.
– In each terminal device, a KONFIDO client can be installed to allow a secure communication with the NI (optional).

Considering the high number of heterogeneous devices that can be involved in the OpenNCP scenario, the specific solutions adopted for security provisioning and their hardware requirements, KONFIDO will provide different communication channels to cover all possible situations:

– TEE communication channel: It is a trusted channel established using remote attestation between TEE based on Intel SGX technology. This communication channel allows the data exchange between SGX enclaves using PUF technologies for the keys used during the remote attestation.
– SSL communication channel between SGX-based TEE and other TEEs: It is a secure communication channel (SSL) to allow the communications between TEEs based on different technologies like Intel SGX and ARM Trust Zone (ARM TZ).
– HE+SSL communication channel: It is a homomorphic encrypted SSL communication channel to be used when TEE technologies are not available (for example in mobile devices or in NCP without TEE support).
– SSL communication channel: It is a standard communication channel used only for local data exchange like the communication between the PUF hardware and the TEE.
– OpenNCP communication channel: It is the standard OpenNCP communication channel.

Furthermore, in order to protect the OpenNCP infrastructure from distributed attacks (e.g. DDoS), a SIEM solution is needed. Considering the management/hosting issues and national regulations coming from a centralized SIEM, only a distributed solution is applicable: each NCP will have its SIEM that looks at corresponding NI and that is interconnected with other SIEMs to exchange security metrics via a publish-subscribe communication channel (Fig. 3). Two specialized TEE data hooks will be available for the SIEM, one providing plain data, and the other providing homomorphic encrypted data. The second one is needed to allow the data processing of sensitive data (respecting the privacy requirement) in terms of data threshold comparison, structure coherence and so on without access to the relative plain text.

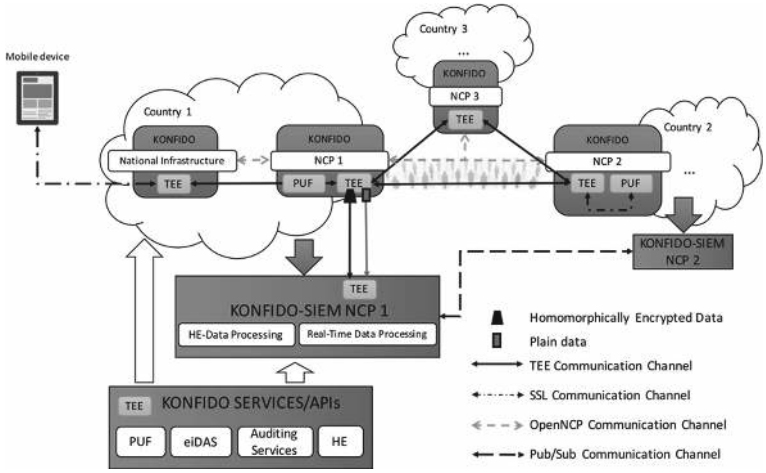

Fig. 3. KONFIDO architecture

4 An Agent-Based View of KONFIDO

The KONFIDO architecture can also be viewed as a system of interacting agents as shown schematically in Fig. 4, and in this section we describe a generic KONFIDO interface template, structured as a multi-agent Agent System (AS). This AS would be resident at each individual national or regional access point. Each AS can communicate with other similar ASs in the same or in different countries or regions, i.e. at the same local site or at remote sites, via a system such as OpenNCP. The ASs can also communicate directly with each other through the Internet. Each AS will be composed of several specialized agents (SA):

- Within the AS, the SAs can communicate with each other;
- One of these SAs is designed to communicate with the local NI;
- Other SAs are specialized in communicating with other SAs at other national access points, and one can imagine that within an AS there would be a distinct SA that is designed specifically to communicate with the SA at each specific country, and the agents can learn and adapt individually to their specific environment [9].

For each of the SA's, an automaton-like input-state-output graph specifies and describes its interaction with messages that enter the SA and which are aimed in particular at this SA, and with other agents outside and inside this particular SA. This graph represents states as nodes, and each distinct input is represented by an arc leading into another node. An input-state pair will then produce a new state (the next state) and an output.

Within each AS, there would be at least one SA which is specialized for security surveillance and reaction (i.e. the Security Surveillance Agent SSA):

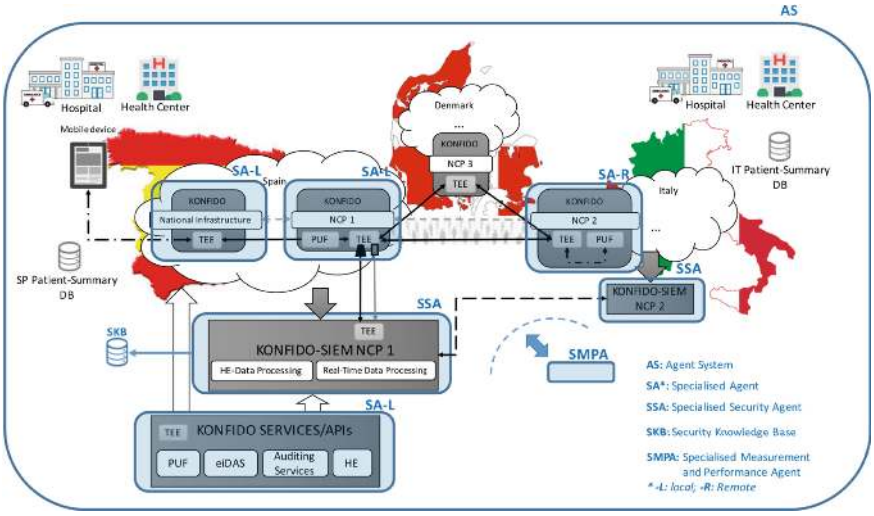

Fig. 4. The KONFIDO architecture as a system of interacting agents

- We can imagine that different SSAs can be specialised in keeping track of specific communications with the national health infrastructure, or the various communications that are being conducted.
- In addition, a Security Knowledge Base (SKB) which is local to each AS will store security related data that is relevant to that AS.

4.1 Advantages of the Multi-agent System Architecture

The AS architecture has several advantages over other approaches:

- It allows the designer to introduce new functionalities by introducing new SAs;
- This architecture allows for negotiations and economic exchanges between agents, that can offer means for distributed decision making;
- It simplifies the documentation since each AS with its collection of SAs follows the same standard template. Each AS, and each SA, is designed starting from the same core template and code, which should be portable between different countries, regions and access points;
- Code and agents can be shared as needed across multiple countries and access points;
- It allows for the separate concurrent execution of the SA within the same AS, so that we can benefit from parallelism to reduce execution times and also to limit the sequential dependence between different SAs;
- Each SA can be separately stopped and restarted as needed, or deleted, independently of the other SAs. Each individual agent can use its own access controls and attack detection [12] and we can monitor energy and resource usage for each agent separately [8];

– The automaton-theoretic representation proposed for each SA allows the input sequence, i.e. the sequences of messages that are directed to any specific SA, to be processed using standard parsing and interpretation algorithms both off-line, for instance during system development, or when one simulates a given AS to test and evaluate its operation. The same is true for the output message sequences.

Some of these advantages also relate directly to security:

– This also allows us to design the security surveillance for each SA based on standard parsing and formal language interpretation techniques which are 'real-time algorithms' for finite-state automata, and are also real-time for extensions such as push-down automata.
– Specifically, the output sequences from some remote SA, which arrive to a given SA at another location, can also be monitored for compliance with regard to the remote SA's finite-state-machine specification, and likewise the local SA's state and output behaviour can be monitored for compliance to its own specifications.

The AS, can thus comprise a Knowledge Base which includes the automaton specification of each of the SA that it contains, as well as those with which may be remotely located and with which it exchanges message sequences.

4.2 The Specialised Security Agents (SSA)

SSA are simply SAs in a given AS that are in charge of monitoring security and taking decisions that result from this monitoring activity. One of the roles of the SSA's in a given location's AS can be to test the arriving input sequences for compliance with the security requirements and as a way to detect unusual, unexpected or unspecified behaviours. Similarly, once a SSA has accepted an input sequence begin sent by some remote SA-R to a local SA-L as being valid, it can verify the behaviour of the receiving local SA-L with respect that SA-L's specification, in order to detect unusual behaviours. A SSA can similarly have the role of monitoring the output sequences of some local SA-L with respect to the input sequences it receives.

The output of this analysis, such as the type and number of correct or incorrect message sequences, e.g. where correctness can be viewed as recognition by the parsing algorithm, can be fed into a learning type algorithm which is used to detect threats, and threat levels, and also provide data to the local Security Knowledge Base (SKB) which is resident in each AS.

The SSA will have the ability to provide threat assessments and will be able to modify its perceived risk levels for different SAs or for different current (open) or past sessions.

Certain SSA will be considered to have higher priority, and they will be called SSA-H agents. They will be able only to trigger specific reactions such as blocking certain agents, re-starting agents that appear to be compromised, and blocking certain communication ports. We note that an SSA-H will have the

ability to call upon certain operating level procedures, contrary to the other SAs which operate at the level of the AS rather than at the level of the underlying software infrastructure.

4.3 Specialised Measurement and Performance Agents (SMPA)

Of course, once the system operates effectively and in a secure manner, it is also necessary that it operates promptly so that delays and congestion are managed as effectively as possible without undue delays and bottlenecks are avoided. Thus we would expect that each AS will typically contain at least one agent, the SMPA, that will measure relevant quantities such as the delay for the execution of requests, the throughput in number of requests processed per unit time, volumes of data transferred, the levels of transmission errors and repetitions, and possibly also data regarding the congestion or load of the physical infrastructure.

Such data can be used to report on end user satisfaction, but we can imagine that it can also be used to adaptively manage the infrastructure and the different SAs, including to prioritise or defer certain requests, so that overall system performance is optimised.

5 Conclusions

In this paper, we presented the KONFIDO approach for secure cross-border health-care data exchange across Europe. KONFIDO aims to deliver a secure and trust toolbox for enabling seamless interoperable cooperation of underlying medical services provided by numerous eHealth applications. Such cooperation requires a high level of security and also an high level of modularity to overcome the heterogeneity of the involved devices. This paper discussed the proposal architecture that will be implemented in the 36-month EU-funded KONFIDO project. In particular, we presented the overall KONFIDO architecture following a bottom-up approach. We started from a description of the reference scenario in the context of the eHealth data exchange provided by OpenNCP platform as outcome of the epSOS project. We presented the KONFIDO components and how these are combined in a holistic approach aiming at improving the security of OpenNCP eHealth data exchange. The main advantage of the KONFIDO solution is that it is designed and implemented as a toolbox composed by different services and tools the combination of which can be used to address a wide range of possible eHealth scenarios (not only the ones related to OpenNCP) and to solve many vulnerabilities in the exchange and processing of health data.

Acknowledgments. The research leading to these results has received funding from the European Union's (EU) Horizon 2020 research and innovation programme under grant agreement N727528 (Action title: KONFIDO - Secure and Trusted Paradigm for Interoperable eHealth Services, Acronym: KONFIDO). 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. Akriotou, M., Mesaritakis, C., Grivas, E., Chaintoutis, C., Fragkos, A., Syvridis, D.: Random number generation from a secure photonic physical unclonable hardware module. In: Gelenbe, E., et al. (eds.) Euro-CYBERSEC 2018. CCIS, vol. 821, pp. 28–37 (2018)
2. Castaldo, L., Cinque, V.: Blockchain based logging for cross-border exchange of ehealth data. In: Gelenbe, E., et al. (eds.) Euro-CYBERSEC 2018. CCIS, vol. 821, pp. 46–56 (2018)
3. Coppolino, L., D'Antonio, S., Formicola, V., Romano, L.: Integration of a system for critical infrastructure protection with the OSSIM SIEM platform: a dam case study. In: Flammini, F., Bologna, S., Vittorini, V. (eds.) SAFECOMP 2011. LNCS, vol. 6894, pp. 199–212. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-24270-0_15
4. Coppolino, L., D'Antonio, S., Formicola, V., Romano, L.: Enhancing SIEM technology to protect critical infrastructures. In: Hämmerli, B.M., Kalstad Svendsen, N., Lopez, J. (eds.) CRITIS 2012. LNCS, vol. 7722, pp. 10–21. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-41485-5_2
5. Coppolino, L., D'Antonio, S., Romano, L., Staffa, M.: KONFIDO project: a secure infrastructure increasing interoperability on a systemic level among eHealth services across Europe. In: Preceedings of ITASEC 2017, 20 January 2017, Venice, Italy (2017)
6. Faiella, G., Komnios, I., Voss-Knude, M., Cano, I., Duquenoy, P., Nalin, M., Baroni, I., Matrisciani, F., Clemente, F.: Building an ethical framework for cross-border applications: the KONFIDO project. In: Gelenbe, E., et al. (eds.) Euro-CYBERSEC 2018. CCIS, vol. 821, pp. 38–45 (2018)
7. Fan, J., Vercauteren, F.: Somewhat practical fully homomorphic encryption. IACR Cryptology ePrint Archive 2012, 144 (2012). http://dblp.uni-trier.de/db/journals/iacr/iacr2012.html#FanV12, informal publication
8. Gelenbe, E., Caseau, Y.: The impact of information technology on energy consumption and carbon emissions. Ubiquity **2015**(June), 1 (2015)
9. Gelenbe, E., Seref, E., Xu, Z.: Simulation with learning agents. Proc. IEEE **89**(2), 148–157 (2001)
10. Herder, C., Yu, M.D.M., Koushanfar, F., Devadas, S.: Physical unclonable functions and applications: a tutorial. Proc. IEEE **102**(8), 1126–1141 (2014)
11. Natsiavas, P., Kakalou, C., Votis, K., Tzovaras, D., Maglaveras, D., Koutkias, V.: User requirements elicitation towards a secure and interoperable solution for health data exchange. In: Gelenbe, E., Campegiani, P., Czachorski, T., Katsikas, S., Komnios, I., Romano, L., Tzovaras, D., (eds.) Proceedings of the 2018 ISCIS Security Workshop, Imperial College London. Springer, Heidelberg (2018)
12. Oke, G., Loukas, G., Gelenbe, E.: Detecting denial of service attacks with Bayesian classifiers and the random neural network. In: IEEE International Fuzzy Systems Conference, FUZZ-IEEE 2007, pp. 1–6. IEEE (2007)
13. Rasmussen, M., et al.: Gap analysis for information security in interoperable solutions at a systemic level: the KONFIDO approach. In: IFMBE Proceedings of the International Conference on Biomedical and Health Informaticsn, Greece, 18–21 November. Springer, Heidelberg (2017, in press)
14. Staffa, M., Sgaglione, L., Mazzeo, G., Coppolino, L., D'Antonio, S., Romano, L., Gelenbe, E., Stan, O., Carpov, S., Grivas, E., Campegiani, P., Castaldo, L., Votis, K., Koutkias, V., Komnios, I.: An openNCP-based solution for secure

eHealth data exchange. J. Netw. Comput. Appl. **116**, 65–85 (2018). https://doi.org/10.1016/j.jnca.2018.05.012. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85048715942&doi=10.1016%2fj.jnca.2018.05.012&partnerID=40&md5=81c9e20e7d35684f36599f4d8163bf98