Blockchain-Based Logging for the Cross-Border Exchange of eHealth Data in Europe

Luigi Castaldo(✉) and Vincenzo Cinque

Bit4id S.r.l., via Diocleziano 107, 80125 Naples, Italy
{lca,vci}@bit4id.com
http://www.bit4id.com

Abstract. On an EU level, the topic of electronic health data is a high priority. Many projects have been developed to realise a standard health data format to share information on a regional, national or EU level. All the projects favour and contribute to the development and improvement of the prerequisites for intra- and cross-border patient mobility. This work presents a new approach for the implementation of disruptive logging: an audit mechanism for cross-border exchange of eHealth data on OpenNCP, providing traceability and liability support within the OpenNCP infrastructure. Relevant parties could be legally obliged to keep a log of all privacy-critical operations performed by OpenNCP users.

Keywords: Cyberecurity · E-Health · Blockchain · Logging

1 Introduction

In the last few years, the number of people travelling across Europe for leisure, business or study purposes has been constantly increasing. In addition, the right of European Union (EU) citizens to seek healthcare in other European countries creates a strong demand for the cross-border exchange of health data. On an EU level, the topic of electronic health data is a high priority. Several projects have been developed to realise a standard health data format to share information on a regional, national or EU level.

With the advent of digital technology and with an increasing number of countries in Europe shifting their priorities towards digital health care, a secure, standard method for exchanging data among member states is needed. Electronic data does not flow freely between most of the EU countries due to a number of barriers, such as a lack of awareness, trust and legal clarity. This has led to the need for increased security implementations, resulting in improved user acceptance of such applications and thus to large-scale adoption of these technologies and to full exploitation of their advantages. Electronic health record (EHR) systems must assure a high level of protection to maintain the confidentiality of patients' data [12].

© The Author(s) 2018
E. Gelenbe et al. (Eds.): Euro-CYBERSEC 2018, CCIS 821, pp. 46–56, 2018.
https://doi.org/10.1007/978-3-319-95189-8_5

The EU is very active in the development of possible solutions, and several projects have been funded by EU's Horizon 2020 programme. For instance, the KONFIDO [11,17] project is developing a federated architecture, using privacy through design principles. It will enable the secure exchange, processing and storage of health-related data. KONFIDO will make cross-border interoperation of eHealth services provided by individual countries more secure, while allowing each participating entity to enforce specific policies for protection and control of personal health related data.

While some past and current projects have delivered important results, a sound holistic approach to the issue of digital security in eHealth is still a faraway target.

In this work, we present a secure audit mechanism based on blockchain technology. We first provide a general overview of the current situation regarding eHealth data exchange in Europe. Second, we introduce the OpenNCP software, mainly focusing on the log flows inside the platform. We continue with a description of the presented solution, detailing the interaction between the proposed components. Finally, we give our conclusions.

2 eHealth Data Exchange in Europe

Moving toward eHealth is a key goal of the EU. Many health and IT policy documents emphasise the benefits of (and barriers to) pursuing the digital agenda. In 2004, the European Commission initiated its first eHealth Action Plan, requesting a commitment from Member States to work together on eHealth. Over the last decade, progress toward eHealth within the 27 EU Member States has been inconsistent [6,9]. The academic literature has primarily focused on issues related to the adoption and diffusion of specific eHealth technologies, such as EHRs, health information exchanges (HIEs), and telemedicine, along with their various benefits and barriers [5].

To increase the efficiency of patient care delivery, healthcare parties must be able to access and exchange patient information independent of their organisational and technological particularities. The European Commission is taking a first step in this direction by defining guidelines for defining and sharing patient summaries across Europe. The European Patient Summary (EPS) [15] is an interoperability infrastructure intended to address this challenge by managing and exchanging patient summaries across European healthcare networks. From a technical perspective, the realisation of the EPS demands powerful middleware technology that guarantees ubiquitous access to distributed and multi-faceted data as well as scalability, persistency and interoperability.

One of the most relevant efforts has been the epSOS [7] Project, aiming at designing, building and evaluating an e-Health framework and ICT infrastructure to allow patient data to be securely exchanged among different European healthcare systems. The epSOS project 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 and ePrescription/eDispensing, between European healthcare systems. The cross-border services are handled by clinical gateways called National Contact Points (NCP) [14].

epSOS introduced a full set of specifications and operational aspects to define an interoperability framework that builds on widely accepted standards, such as Health Level 7 (HL7). epSOS also provided a reference implementation which was changed to an open-source community implementation, OpenNCP [10].

3 OpenNCP

OpenNCP [8] solves the problem of securely exchanging documents for care provisioning abroad, maintaining the clinical/legal value of the original documents. OpenNCP is meant to establish shared eHealth practices with respect to patient data exchange across European member countries. Besides supporting the correct flow of data, the goal of OpenNCP is to ensure the respect of security, legal and interoperability requirements. OpenNCP provides a number of interoperable services, which enable national and regional eHealth platforms to establish cross-border health information networks. Although OpenNCP offers a secure solution to transfer eHealth data across the EU, there is still room for improvements from a security point of view. A key concern is the implementation of a secure and unforgeable audit system.

3.1 Logflow

An OpenNCP node generally interacts with two different types of counterparts: a national infrastructure, to retrieve patients' data from the national healthcare system, and another OpenNCP node, to retrieve patient's health data from another country. This section mainly focuses on identifying the log flows inside OpenNCP, in particular for all the scenarios requiring health data exchange between two different countries. An OpenNCP node interacts externally towards another NCP node for these purposes [16]: (a) Exchange of ePrescription (eP), Patient Summary (PS) and eDispense documents; (b) Patient identification.

Audit Manager. The current implementation of OpenNCP uses an internal component, based on OpenATNA [1], to implement the Audit Trail objectives. This component provides interfaces for the Audit Trail Service, acting as service point to keep track of events to be logged. The Audit Manager has a built-in feature to assure that all the audit messages are sent to OpenATNA and persisted in the database. If something goes wrong while attempting to send an audit message to OpenATNA, the message is stored on the file-system for later handling.

Patient Identification. The workflow between two countries during the identification of a patient in a foreign country (B) and his or her home country (A) can be summarised as follows: the Audit Manager on node B keeps track of the

request sent by country B. The same occurs in country A when the message arrives. When country A responds to the request, a new record is created in the Audit Manager and persisted in the database. The same happens in B when the response arrives.

Data Exchange (PS and EP) and Notifications. If a patient has been already identified, a healthcare professional (HP) can query the system to retrieve his or her patient summary and/or prescriptions. Each component performing an operation, in both countries, either going on the National Infrastructure or forwarding to an external NCP node, saves an audit trail in the DB by means of the Audit Manager.

4 Architecture

This work proposes a new architecture to overcome the issues related to the standard logging mechanisms within OpenNCP. It provides traceability and liability through an unforgeable log management system based on blockchain. The aim of this study is to create an architectural model of a centralised blockchain-based solution extending Bit4id's SmartLog [2] platform.

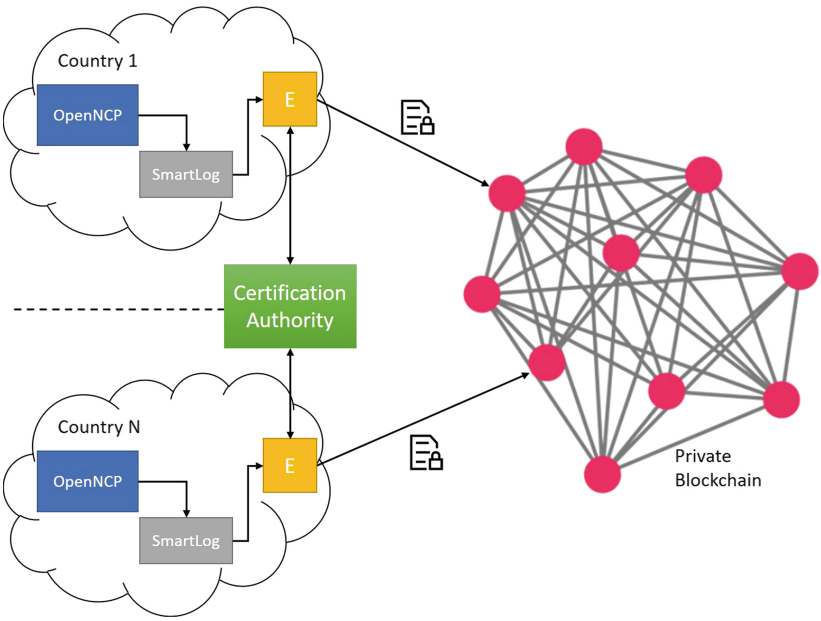

Fig. 1. Log management system architecture.

The proposed architecture is based on three modules (Fig. 1):

- SmartLog: it is able to ensure the origin and integrity of system logs and certain time evidence of log generation (by time-stamping) along with the standard filtering features provided by the most common logging management systems;
- Encryption module (E): all the logs must be properly encrypted before saving them on the blockchain. The encryption is needed for two main reasons: (a) making logs accessible only to the countries involved in the transactions; (b) purging all the logs after a certain amount of time, according to specific regulations;
- Blockchain: it grants distributed access to data, while making information unforgeable and undeletable.

The proposed approach requires deployment of the new modules in each OpenNCP node. For every country, the new logging system requires that a SmartLog and an encryption module directly connected to the OpenNCP node be in use, and a node belonging to a private blockchain must safely store the logs. The Certification Authority, depicted in Fig. 1, is part of the defined encryption mechanism, but it does not need to be deployed in every country. A single element is enough to support the entire architecture (Fig. 2).

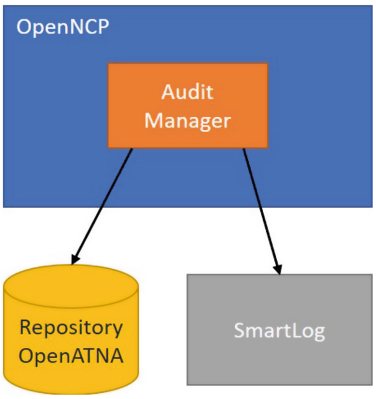

Fig. 2. SmartLog integration.

4.1 SmartLog

SmartLog is a client-server system for log message management, ensuring system log origin, certain time evidence of log generation (by time-stamping), integrity of each message and confidentiality. SmartLog makes it possible to perform efficient and centralised management of the log files. The solution is not invasive and is completely decoupled from pre-existent hardware/software architectures. Moreover, it does not require any intervention on the current OpenNCP architecture or development of an integration module. The product is able to replace

the OpenATNA repository used by the platform. In our work, SmartLog receives the logs directly from the Audit Manager, which can be achieved by changing a few parameters in the OpenNCP settings configuration.

SmartLog is based on four main components (Fig. 3):

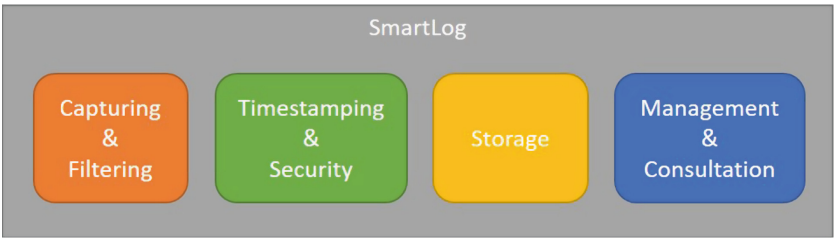

Fig. 3. SmartLog components.

- Capturing and filtering: SmartLog is able to safely acquire and transfer all messages generated by the monitored systems. Any type of event can be enriched and transformed;
- Timestamping and security: the platform generates a timestamp for each log message to ensure a trusted and certain time reference for the log and to level out the time formats (often disparate) between the different systems;
- Storage: SmartLog comes with an internal storage mechanism hosting all the collected logs, without allowing access to the data except for authorised personnel. This work focuses on extending this functionality, storing selected logs directly on a private blockchain through the use of the encryption module described in the next section. This mechanism will be applied only to logs regarding critical operations within OpenNCP;
- Management and consultation: log consultation and management is exclusively available to authorised personnel.

When SmartLog completes its processing on the received logs, it has two possible choices: storing the logs in internal secure storage or, in case the logs referring to ehealth data exchange between two countries, forwarding them to the encryption module for the next steps.

4.2 Encryption Mechanism

Once the critical logs have been filtered and processed by SmartLog, they are ready to be securely stored on the blockchain to make them unforgeable and undeletable. At this point, another problem arises. When something is stored on a blockchain, even a private blockchain, the information becomes accessible to everyone connected to the distributed ledger. In case of eHealth, most often, exchanged data contains patients' sensitive information, and so it cannot be

openly exposed to everyone in the system. According to EU regulations, only the entities involved in a transaction should have access to the audit logs of the transaction. Moreover, old logs must be purged after a certain amount of time.

The regulation requirements are partially conflicting with the immutability and undeletable nature of the auditing mechanism and the blockchain technology. For this reason, a specific encryption mechanism has been defined in this work. This mechanism is required to ensure that data are only accessible to the parties involved. An approach with a combination of symmetric and asymmetric encryption enables data sharing between selected entities and yields good performance for the auditing system [13].

Symmetric Encryption. Symmetric encryption mechanisms considerably reduce encryption complexity. Following this method, data are encrypted and decrypted by splitting them into a form of blocks. In its simplest mode, it is possible to split plain text into blocks, which are then fed into the cipher system to produce blocks of cipher text. By handling only small chunks of data, symmetric encryption algorithms yield good performance. The biggest problem with symmetric key encryption is finding a safe way to exchange the ciphering key with the other parties involved in the communication [18].

Asymmetric Encryption. Asymmetric cryptography, also known as public key cryptography, uses public and private keys to encrypt and decrypt data. For asymmetric encryption to deliver confidentiality, integrity, authenticity and non-repudiability, users and systems need to be certain that a public key is authentic, that it belongs to the person or entity claimed and that it has not been tampered with or replaced by a malicious third party. There is no perfect solution to this public key authentication problem. A public key infrastructure (PKI), where trusted certificate authorities certify ownership of key pairs and certificates, is the most common approach.

The encryption module, by design, generates a new key-pair and the corresponding Certificate Signing Request (CSR) every year. The CSR is later submitted to the trusted internal Certification Authority (CA). Upon receiving the CSR, the CA validates the request and responds with a CA Certificate. When the certificate expires, the module takes care of deleting the key-pair associated to it and generates a new one to request a new certificate.

When the encryption module of an OpenNCP node receives a new log from SmartLog, it converts it in the encrypted format depicted in Fig. 4. The encryption process can be summarised as follows:

1. The encryption module extracts meta-data from the log, such as source country, destination country and performed operation. The meta-data are not encrypted and are used to index the messages in the blockchain for future retrieval;
2. Module (E) generates a random symmetric key (K) that is used to encrypt the audit log (M): $[SE(M, K)]$;

3. The key is later encrypted using the asymmetric encryption. The module encrypts the key (K) two times. The first encryption is performed using the public key P_{send} of the source country $[AE(K, P_{send})]$, the second using the public key P_{recv} of the destination country $[AE(K, P_{recv})]$. The public keys are always retrieved from the CA, which is the only trusted entity to retrieve public keys;
4. The fully encrypted log is sent to the blockchain to be permanently stored;
5. The module destroys the symmetric key, which from that point on is only available in the message on the blockchain.

Metadata	Enc. Key	Message
Sender	$AE(K, P_{send})$	$SE(M, K)$ where: M = message K = symmetric key
Receiver		
Operation	$AE(K, P_{recv})$	
Index Keys		

Fig. 4. Encrypted log structure.

The encryption mechanism described above makes the data stored on the blockchain only accessible to entitled parties. Only the involved parties can access the logs using their private key, if it has not already expired. If one of the countries (A) involved in a transaction needs to get access to a log, it can retrieve the log from the blockchain. The log can only be decrypted in the encryption module, which owns the private key of the country. The private key PR_A is used to decrypt the symmetric key (K) saved in the message, which in turn is used to decrypt the real log. This process safeguards users' privacy and enables the single actors to decrypt the messages on their own in case of disputes. Moreover, changing the encryption key-pairs every year and forcing the deletion of the previous ones for every Member State makes it impossible to decrypt old logs, in accordance with the specific regulations.

4.3 Blockchain

Blockchain is a decentralised transaction and data management technology developed first for Bitcoin cryptocurrency. The interest in Blockchain technology has been increasing since the idea was coined in 2008. The reason for the interest in Blockchain is its central attributes, which provide security, anonymity and data integrity and immutability without any third-party organisation in control of the transactions, and therefore it creates interesting research areas, especially from the perspective of technical challenges and limitations [3].

All the participants are equipotent and equally privileged, and the operational principles of the decentralised database are mutually decided. Blockchain

protocols thus ensure that transactions on a blockchain are valid and never recorded to the shared repository more than once, enabling people to coordinate individual transactions in a decentralised manner without the need to rely on a trusted authority to verify and clear all transactions.

After a block has been added to the blockchain, it can no longer be deleted or changed, and the transactions it contains can be accessed and verified by everyone on the network.

Multiple distributed ledger solutions have been evaluated to best fit the flexibility, security and performance prerequisites needed for the proposed approach. Considering the generic purpose of the platform, we decided to use MultiChain [4]. It is an open source technology allowing the implementation of a private blockchain and providing low overhead for the transactions handling.

The MultiChain technology is a platform that helps users to establish a certain private Blockchain. It solves the related problems of mining, privacy and openness via integrated management of user permissions.

Once a blockchain is private, problems relating to scaling are easily resolved, as the chain's participants can control the maximum block size. In addition, as a closed system, the blockchain will only contain transactions which are of interest to those participants.

Privileges. In MultiChain, all privileges are granted and revoked using network transactions containing special metadata. The miner of the first 'genesis' block automatically receives all privileges, including administrator rights to manage the privileges of other users. This administrator grants privileges to other users in transactions whose outputs contain those users' addresses along with metadata denoting the privileges conferred. When changing the administration and mining privileges of other users, an additional constraint is introduced, in which a minimum proportion of the existing administrators must vote to make a change.

Mining. By restricting mining to a set of identifiable entities, MultiChain resolves the dilemma posed by private blockchains, in which one participant can monopolise the mining process. The solution lies in a constraint on the number of blocks which may be created by the same miner within a given window. MultiChain implements this scheme using a parameter called mining diversity.

General Data Storage. MultiChain streams enable a blockchain to be used as a general purpose append-only database. A MultiChain blockchain can contain any number of streams, where the data published in every stream are stored by every node.

5 Conclusions

In this paper, we presented a method for utilising blockchain technology to provide tamper-proof audit logs for cross-border exchange of eHealth data

in Europe. Blockchain security properties can guarantee off-the-shelf non-repudiation and integrity for logs without extra efforts. MultiChain technology, without relying on the proof-of-work mechanism, does not suffer from the limitations imposed by the Bitcoin technology regarding the number of transactions, block size and cost per transaction. This approach provides an easy to integrate solution for current OpenNCP issues by providing traceability and liability support within its infrastructure. Our work combines secure storing mechanisms with fine-grained privacy controls in one component, without requiring significant changes to the OpenNCP architecture.

References

1. Openatna. Technical report, MOSS & University of Cardiff (2018). https://ec.europa.eu/cefdigital/code/projects/EHNCP/repos/ehealth/browse/openatna
2. Bit4id: Smartlog (2018). https://www.bit4id.com/en/secure-log-management/
3. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J., Felten, E.: Research perspectives and challenges for bitcoin and cryptocurrencies. In: IEEE Security and Privacy, March 2015. https://eprint.iacr.org/2015/261.pdf
4. CoinSciences: Multichain (2018). https://www.multichain.com/
5. Currie, W., Seddon, J.: A cross-national analysis of ehealth in the European union: some policy and research directions. Inf. Manag. **51**(6), 783–797 (2014)
6. Dobrev, A., Jones, T., Stroetmann, V., Stroetmann, K., Vatter, Y., Peng, K.: Interoperable ehealth is worth it-securing benefits from electronic health records and eprescribing. Bonn/Brussels: European Commission on Information Safety and Media (2010)
7. EpSOS-Project: About epsos (2018). http://www.epsos.eu/home/about-epsos.html
8. EpSOS-Project: Openncp (2018). https://openncp.atlassian.net/wiki/spaces/ncp
9. European-Commission: E-health-making healthcare better for european citizens: An action plan for a european e-health area (2004)
10. Fonseca, M., Karkaletsis, K., Cruz, I., Berler, A., Oliveira, I.: OpenNCP: a novel framework to foster cross-border e-health services. In: MIE, pp. 617–621 (2015)
11. KONFIDO-Project: About konfido (2018). http://www.konfido-project.eu/konfido/content/what-konfido-project-about
12. Krummenacher, R., Simperl, E., Cerizza, D., Valle, E.D., Nixon, L., Foxvog, D.: Enabling the European patient summary through triplespaces. Comput. Methods Programs Biomed. **95**(2), S33–S43 (2009)
13. Kumar, Y., Munjal, R., Sharma, H.: Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures. Int. J. Comput. Sci. Manag. Stud. **11**(3) (2011)
14. Moharra, M.: Almazán, C., Decool, M., Nilsson, A., Allegretti, N., Seven, M.: Implementation of a cross-border health service: physician and pharmacists' opinions from the epSOS project. Fam. Practice **32**(5), 564–567 (2015)
15. Olsson, S., Lymberis, A., Whitehouse, D.: European commission activities in ehealth. Int. J. Circumpolar Health **63**(4), 310–316 (2004)
16. Ruestchmann, P., de Béjarry, G.: Final epSOS system technical specification. Deliverable D3.3.2, ASIP SANTE, April 2010

17. Staffa, M., Coppolino, L., Sgaglione, L., Gelenbe, E., Komnios, I., Grivas, E., Stan, O., Castaldo, L.: Konfido: An openNCP-based secure ehealth data exchange system. In: Gelenbe, E. et al. (eds.) Euro-CYBERSEC 2018. CCIS, vol. 821, pp. 11–27. Springer, Heidelberg (2018)
18. Thakur, J., Kumar, N.: DES, AES and Blowfish: symmetric key cryptography algorithms simulation based performance analysis. Int. J. Emerg. Technol. Adv. Eng. **1**(2), 6–12 (2011)

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.