ICT for Health Science Research
A. Shabo (Shvo) et al. (Eds.)

doi:10.3233/978-1-61499-959-1-110

Privacy by Design for Integrated Case and Care Management: Receiver-Oriented Encryption in STROKE OWL

Timo MICHELSEN[a,1], Christian LINS[a], Stefan GUDENKAUF[b], Andreas HEIN[c], Christian LÜPKES[a]
[a] *OFFIS – Institute for Information Technology, Div. Health, Oldenburg, Germany*
[b] *University of Applied Sciences and Arts Hannover, Hannover, Germany*
[c] *Carl von Ossietzky University Oldenburg, Dep. Health Services Research, Oldenburg, Germany*

Abstract. Research into new forms of care for complex chronic diseases requires substantial efforts in the collection, storage, and analysis of medical data. Additionally, providing practical support for those who coordinate the actual care management process within a diversified network of regional service providers is also necessary. For instance, for stroke units, rehabilitation partners, ambulatory actors, as well as health insurance funds. In this paper, we propose the concept of comprehensive and practical receiver-oriented encryption (ROE) as a guiding principle for such data-intensive, research-oriented case management systems, and illustrate our concept with the example of the IT infrastructure of the project STROKE OWL.

Keywords. Case Management, Data Management, Privacy by Design, Asymmetric encryption, Pseudonymization, Anonymization

1. Introduction

Case management is designed to empower social and health professionals to coordinate aid efforts under complex conditions and to use existing institutional resources in the community or field of work. The aim is to organize, control, and evaluate a system of cooperation that is geared to the concrete needs for support of the person, and in which the respective person is directly involved. This is addressed by optimizing assistance in a specific case (*care management*), and by optimizing support around responsibility (*systems management*). The transition from systems management to care management is seamless [1]. The cross-sectoral organized care management of complex chronic diseases is of interest in integrated case and care management, here using the example of strokes in the pilot region Ostwestfalen-Lippe (STROKE OWL) [2]: The project aims at a comprehensive implementation of cross-sector care management for patients after a stroke. The actual care management process is carried out by so-called *stroke pilots*, who accompany patients in coordinating their lives after the stroke incident. In a population-oriented approach, the complete care path is integrated, i.e. the formation and

[1] Corresponding Author, Timo Michelsen, OFFIS – Institute for Information Technology, Escherweg 2, 26121 Oldenburg, Germany; E-mail: timo.michelsen@offis.de

coordination of a network of regional service providers consisting of stroke units, rehabilitation partners, and ambulatory actors, as well as health insurance funds.

The mere number and diversity of individual actors place high demands on the IT infrastructure of such projects about the collection, provision, and evaluation of data, especially concerning security and privacy. Fortunately, there are guidelines that provide a sound overview of the requirements for such systems (*what should be implemented*), such as the TMF Guidelines to privacy in medical research projects [3], and the individual aspects of secure implementation are well known for decades: authentication mechanisms [4], authorization restrictions [5] and encryption techniques [6]. However, there is often a lack of consistent concepts on *how to implement* these requirements. In line with the overall demand for Privacy by Design [7], we propose the model of comprehensive receiver-oriented encryption (ROE), which we illustrate using the example of the IT infrastructure of the STROKE OWL.

In the following Section 2, we give an overview of the state of the art. Section 3 describes ROE in more detail, followed by an overview of STROKE OWL, in which ROE is implemented (Section 4). Concept and Implementation were preceded by a requirements analysis, which is based on the TMF Guidelines regarding the general infrastructure, and on extensive stakeholder workshops regarding the logical data model. Finally, we discuss lessons learned and conclude our approach in Section 5.

2. State of the art

Medical research projects cannot succeed without the collection, long-term storage, and analysis of medical data. Accordingly, the importance of data protection and data security is growing. The TMF guidelines for data protection in medical research projects provide a quality-assured framework as orientation for organizational and technical implementations [3]. Furthermore, in the context of strict data protection laws in the EU [8], requirements that arise from the principle of Privacy by Design are more relevant than ever [7].

An example for IT-based epidemiological research is the analysis of cancer data, which adopted a combination of data warehouse systems to provide epidemiologists an integrated view on population-based cancer data confined to a specific region, and appropriate user-friendly specialist tools to enable their analysis [9]. Guaranteeing security and privacy play a superordinate role here. Contrary to case management, however, there is no direct interaction with patients. Reporting procedures are carried out by authorities and other organizations without a treatment context. Also, the downstream interpretation of the data is population-based rather than cohort-based, and the separation of the system into a trust center and a central registry is a given, the latter having access to all data in a protected environment.

Case management also plays an increasingly important part beyond the healthcare system [10], e.g. the adoption of case management in business process management [11]. In this context, case management software systems (CMS) are discussed as *standard software solutions*. In addition to healthcare, other specialist domains targeted are social work and health insurance funds [12]. Examples of such CMS are the web-based CaseNet (www.diartis.ch) and e-Case (infogate.ch). CMS research points out emerging trends of IT-based case management in general: increased adoption of mobile technologies, enhanced collaboration capabilities, increased use of business intelligence methods, and continuous improvements in the reporting and scheduling of activities [13].

3. Concept of ROE

We use the following terminology to describe ROE: a *user* (e.g., doctor or case manager) is a data provider, which handles data of multiple persons (e.g., patients) and their person data in a direct treatment context. We assume that the user has a letter of agreement from each person. *Personal data* is a combination of sensitive data (name, address, etc.) and domain-specific data (e.g., cross-sectoral medical data from doctors) from a person. All personal data combined is *primary data.* A *recipient* is an actor, person, or institution, which has a reasonable demand on (parts of) primary data (so-called *recipient-specific data packages*). *Secondary data* are additional data (connected to primary data in some way), mainly send by third parties (e.g., health insurance funds).

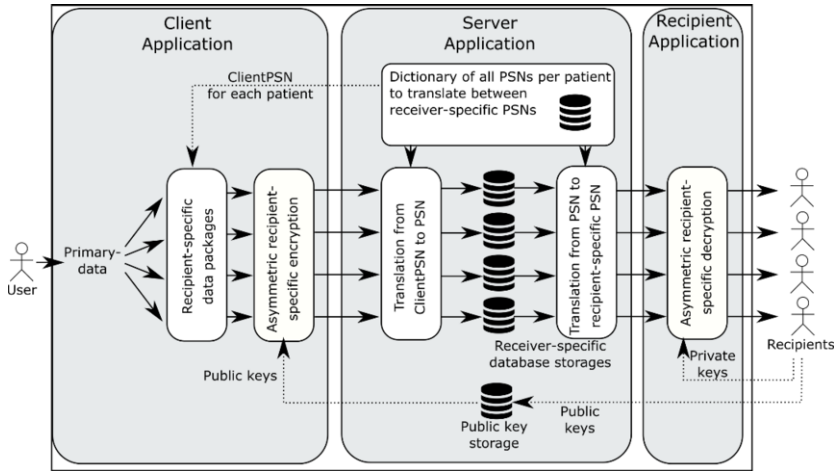

Figure 1. Overview of ROE.

To secure data privacy and security, ROE combines and adapts two existing methods: asymmetric cryptography and pseudonymization. The software architecture is divided into three conceptual parts: client application, server application, and recipient application (see Figure 1).

3.1. Asymmetric encryption and decryption

In a client application (e.g., mobile app, web-portal), the user gathers primary data. As the primary data source, it is the only application which has a reason to access, edit, and delete all primary data. It splits the personal data into recipient-oriented data packages. These packages are encrypted asymmetrically with the individual public keys provided by the trustworthy server application. Since each recipient provides its public key for encryption, it is not possible to the recipient to access data packages of other recipients.

The server application stores the encrypted data packages in individual databases. When one user requests its encrypted data, the server application provides it to a recipient application (e.g., dedicated web portal), where the data is decrypted with the private key of the respective recipient. Asymmetric encryption and decryption are done in the client application and recipient application respectively. Therefore, the server application (and its operator) has no access to any data.

3.2. Pseudonymization

One focus of ROE is to distribute the encrypted data packages while avoiding the possibility for the recipients to merge the decrypted packages again (e.g. to re-identify the person). The idea is to send each recipient a different pseudonym (PSN) for the same person data (*recipient-oriented PSNs, ROPSN)*. Therefore, each recipient and each client application has its domain of ROPSN. And vice versa, each person data has a collection of different ROPSN. Depending on the receiver, a data package of one person is annotated with the corresponding ROPSN. In doing so, it is not possible to merge the data packages from one person since they have different ROPSN.

In the server application, a *central PSN* is generated for each person, too. This PSN is solely used to (1) store the encrypted data packages in a consistent way and (2) to translate between different ROPSN when needed (so-called *identity management*).

4. Implementation in STROKE OWL

To realize ROE (and privacy-by-design) in STROKE OWL, we defined delivery schedules, users and recipients. We specified their data needs, and the data formats of primary data, secondary data, and receiver-oriented data packages. It required extensive communication with all stakeholders to understand fully how ROE can be implemented.

The implementation considers the following recipients: (a) two study nurses, who send paper-based questionnaires to patients and need access to sensible address data (with a specialized recipient application for secured access), (b) seven health insurance funds, which provide secondary data, measure the potential cost of such integrated case-and-care management, and require the insurance numbers of the patients, (c) the University of Bielefeld as an academic partner, which evaluates the primary outcome of reduction of recurrent strokes with medical data (e.g., diagnosis, assessments) of anonymized patients, and (d) stroke pilots who enter primary data into a specialized mobile client application.

Each recipient has ROPSNs and key-pairs for encryption and decryption. Furthermore, the University of Bielefeld uses its ROPSN to associate questionnaire results with corresponding medical data without being able to identify the patient itself (therefore, patients are anonymized from their point-of-view).

5. Lessons learned and conclusion

During development, a strictly defensive approach in programming, implementation, testing, deployment, and maintenance was crucial. The resulting implementation of ROE in STROKE OWL shows the feasibility of the approach, fulfilling the critical need for privacy and security in healthcare systems. Operators are never able to access domain-specific (encrypted) data because client applications send only encrypted recipient-oriented data packages. At the same time, each recipient can only access the data necessary to perform their activities. By using ROPSN as an aspect of ROE, the receivers cannot merge their data packages.

However, one drawback is extensive communication among recipients before data processing can start. Operators, developers, and the server application have no possibility to correct already encrypted and stored data. Additionally, changes in data formats are

costly because data cannot be decrypted by operators and developers to apply those changes. At worst, data packages must be created again from primary data.

Nevertheless, we showed the feasibility of ROE at the example of the STROKE OWL implementation and will further refine the concept in future work. For instance, we currently focus on enhancing privacy-preserving data migration between patient-trusted persons. We would also welcome a future adaptation of ROE in related areas.

Acknowledgments

This work was funded by the Federal Joint Committee German Innovation Fund (Innovationsausschuss des Gemeinsamen Bundesausschuss) within the joint research project STROKE OWL (grant no. 01NVF17025).

References

[1] DGCC, Offizielle Definition der DGCC 2012, https://www.dgcc.de/case-management/ (last visit at 21th January 2019).
[2] Stiftung Deutscher Schlaganfallhilfe (SDSH), STROKE OWL Project Website, https://stroke-owl.de/de/startseite/ (last visit at 21th January 2019).
[3] Pommerening, K., Drepper, J., Helbing, K., Ganslandt, T., *Leitfaden zum Datenschutz in medizinischen Forschungsprojekten: Generische Lösungen der TMF 2.0*., MWV Medizinisch Wissenschaftliche Verlagsgesellschaft mbH & Co. KG, Berlin, 2014.
[4] Debiao, H., Jianhua, C. & Rui, Z., A More Secure Authentication Scheme for Telecare Medicine Information Systems, *J Med Syst* **36** (2012), 1989-1995.
[5] Vawdrey, D. K., Sundelin, T. L., Seamons, K. E., & Knutson, C. D., Trust negotiation for authentication and authorization in healthcare information systems, *Proceedings of the 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (IEEE Cat. No.03CH37439)*, (2014), 1406–1409.
[6] Benaloh, J., Chase, M., Horvitz, E., Lauter, K., Patient controlled encryption: ensuring privacy of electronic medical records, *Proceedings of the 2009 ACM workshop on Cloud computing security* (2009), 103-114.
[7] Schaar, P., Privacy by Design, *Identity in the Information Society*, *3*(2) (2010), 267–274.
[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://data.europa.eu/eli/reg/2016/679/2016-05-04 (last visit at 21th January 2019).
[9] Korfkamp, D., Gudenkauf, S., Rohde, M., Sirri, E., Kieschke, J., Blohm, K., Appelrath, H.-J., Opening up Data Analysis for Medical Health Services: Data Integration and Analysis in Cancer Registries with CARESS, *Transactions on Large-Scale Data- and Knowledge-Centered Systems XXVI: Special Issue on Data Warehousing and Knowledge Discovery* (2016), 89–107.
[10] Swenson, K., *Mastering The Unpredictable: How Adaptive Case Management Will Revolutionize The Way That Knowledge Workers Get Things Done*, Meghan-Kiffer Press, 2010.
[11] van der Aalst, W.M., Weske, M., Grünbauer, D., Case handling: a new paradigm for business process support, *Data & Knowledge Engineering* **53**, 129–162, 2005.
[12] Kie, T., Monzer, M., Case Management und Soziale Dienste, Evers, A., Heinze, R.G. (eds.) *Handbuch Soziale Dienste*, 499–515, VS Verlag für Sozialwissenschaften (2011).
[13] Koehler, J., Hofstetter, J., Woodtly, R., Capabilities and Levels of Maturity in IT-Based Case Management, A. Barros, A. Gal, & E. Kindler (Eds.), *Business Process Management,* Heidelberg: Springer-Verlag, Berlin, 2012.