SoftwareX 24 (2023) 101522

Contents lists available at ScienceDirect

SoftwareX

journal homepage: www.elsevier.com/locate/softx

Original software publication

ALIIAS: Anonymization/Pseudonymization with LimeSurvey integration and II-factor Authentication for Scientific research

Robert Englert [a,*], Manfred Schedlowski [b], Harald Engler [b], Winfried Rief [c], Christian Büchel [d], Ulrike Bingel [e], Tamas Spisak [a]

[a] Institute for Diagnostic and Interventional Radiology and Neuroradiology, University Hospital Essen, Essen, Germany
[b] Institute of Medical Psychology and Behavioral Immunobiology, Center for Translational Neuro- and Behavioral Sciences, University Hospital Essen, University of Duisburg–Essen, Essen, Germany
[c] Division of Clinical Psychology, Philipps-University Marburg, Marburg, Germany
[d] Affective Neuroscience Group, Department of Systems Neuroscience, University Medical Center Hamburg-Eppendorf, Hamburg, Germany
[e] Department of Neurology, Center for Translational Neuro- and Behavioural Sciences, University Medicine Essen, Essen, Germany

ARTICLE INFO

Article history:
Received 15 February 2022
Received in revised form 17 July 2023
Accepted 6 September 2023

Dataset link: https://github.com/pni-lab/ALIIAS

Keywords:
Pseudonymization
Software
Two-factor authentication
Encryption
LimeSurvey
Healthcare

ABSTRACT

As open science principles continue to gain traction, striking a balance between patient privacy and data accessibility has become more crucial in medical research than ever before. Encryption-based pseudonymization is a powerful tool to ensure compliance with data protection regulations from both local institutional guidelines and broader regional regulations, such as the General Data Protection Regulation of the European Union. Employing this type of pseudonymization protects the privacy and security of research participants, and allows researchers to effortlessly comply with data security regulations. The pseudonymization workflow however, can vary significantly across research projects, limiting the usability of supporting software tools. Here we present ALIIAS, a customizable pseudonymization framework that allows easy and flexible deployment of custom pseudonymization software, dedicated to the specific ethical and experimental requirements of individual research projects. Features include compatibility with hardware security tokens paired with two-factor authentication, integration to the survey web application LimeSurvey, as well as custom-format pseudonyms and automatic barcode generation. Collectively, these features make ALIIAS suitable for integration into various research infrastructures and lower the initial barrier to incorporating cutting-edge encryption-based pseudonymization in translational and clinical research practices.

Code metadata

Current code version	*0.9.0*
Permanent link to code/repository used for this code version	https://github.com/ElsevierSoftwareX/SOFTX-D-22-00043
Permanent link to reproducible capsule	*N/A*
Legal code license	*GPL-3.0*
Code versioning system used	*git*
Software code languages, tools and services used	*python*
Compilation requirements, operating environments and dependencies	*OpenSC (optional)*
If available, link to developer documentation/manual	https://github.com/pni-lab/ALIIAS/tree/master/docs
Support email for questions	robert.englert@uk-essen.de

1. Motivation and significance

Technological advancements are revolutionizing every aspect of our world, permeating through our private and professional lives, and transforming how we perceive and interact with the

* Corresponding author.
E-mail address: robert.englert@uk-essen.de (Robert Englert).

https://doi.org/10.1016/j.softx.2023.101522

world around us. However digital transformation also creates increasingly important challenges on the safeguarding of data and privacy, scientific research is not an exception. Data driven and artificial intelligence-based approaches are on the forefront of various research disciplines, which pose significant challenges regarding data protection. Especially in the medical sciences, data sensitivity can range from simple personal information to genetic information or brain scans of the data subject[1] (i.e., patient/study participant). This is profoundly sensitive data and its protection from unauthorized access or misuse is of the utmost importance.

In many cases data controllers[2] (i.e., researchers) are not only responsible for the collection and analyzation of the data, but the burden of data protection often falls on them individually. Managing data protection solutions that are both safe and sustainable can often pose a severe challenge, as they require expertise and resources that may not be readily available. To alleviate this burden, it is crucial to establish systems and frameworks that allow individual researchers to effortlessly meet data external regulations and guidelines, to be able to focus their resources on core research activities. Collaborative support systems can ensure good scientific practice that does not compromise on privacy and integrity.

Significant progress in privacy and data protection has been achieved in various areas, such as the implementation of security systems based on blockchain technology [2] or pseudonymization of vehicular data in smart city concepts [3]. In medical sciences, the data that is gathered can be highly sensitive and could – in a worst-case scenario – lead to forms of discrimination in many aspects of the personal and professional life of the affected patients [4–6]. With the advent of Open Science, the amount of publicly available datasets has increased drastically and the need for strong privacy protection of human research datasets is more important than ever before [7–9]. For medical research in humans, irreversible anonymization of the data is often not sufficient; as data must remain attributable to the participants retroactively, for instance in the case of incidental findings. This can be achieved by *pseudonymization*, the processing of personal data to de-associate it from experimental data, but in a way that the link between the data and the participant's identity can be re-established by (and only by) an authorized actor. While not a new process, pseudonymization came into the spotlight in 2018 with the enforcement of the General Data Protection Regulation (GDPR, Rec. 28) [10,11]. Pseudonymization often emerges as a significant challenge in current scientific practice, but it should not solely be seen as a burden put on the researchers, but rather as an opportunity to easily meet these data-protection obligations.

The simplest pseudonymization techniques, like using a sequential counter or a random number, become popular due to their easy implementation, but they require the researchers to continuously edit the "pseudonymization secret", which in this case is a mapping (e.g., a tabular-format file) between pseudonyms and personal data. The centralized nature of this type of pseudonymization secret increases vulnerability to adversary attacks and poses problems for multi-center studies where the secret gets updated in parallel [1]. Message Authentication Code (MAC) or encryption-based solutions provide a state-of-the-art alternative to these techniques, with better scalability and higher safety [12]. However, these solutions are harder to implement as they are typically designed around specific workflows and do not necessarily generalize to more complex scenarios. Available software solutions also commonly rely on involving a Trusted Third Party (TTP) for the separation of responsibilities [13], which increases the level of security, but at the cost of rising logistics of the pseudonymization pipeline and the effort needed to establish and maintain it in the strict IT infrastructure of a research institution. Established solutions with elaborate authentication systems are often very complex on the architectural side and may be hard to implement in clinical research settings [14,15]. Approaches designed around smartphone applications allow for a decentralized pseudonymization, with a focus on a patient-centric system [16]. As expressed by the European Union for Cyber Security (ENISA) [1], there is no one-size-fits-all pseudonymization technique and a high level of competence is needed to reduce threats by adapting the pseudonymization procedure to different scenarios. Accordingly, pseudonymization often emerges as a significant challenge in current scientific practice. Therefore, instead of aiming at developing a one-size-fits-all software tool, we propose an open-source framework that allows the fast deployment of project dedicated, self-contained pseudonymization software applications.

Our framework is called "ALIIAS: Anonymization/Pseudonymization with LimeSurvey integration and two-factor Authentication for Scientific research". ALIIAS eliminates the need for TTPs through a hardware security module based dual-encryption design and offers a highly customizable, decentralized pseudonymization workflow that can be integrated into a wide variety of research settings. We describe the software architecture of ALIIAS as well as a detailed description of its functionalities. Afterwards we present an example use-case for the ALIIAS framework, followed by a discussion of the possible impact of this project and a conclusion with an outlook to future advancements.

2. Software description

The core functionality of the ALIIAS framework is to deploy custom software applications for pseudonymization, dedicated to meet the requirements of the specific project. The pseudonymization process is based on an encryption-based protocol that can be used in single- or multi-center studies in a decentralized way, without the need for a TTP. The pseudonymization software is centered around a so-called dual encryption scheme, where the pseudonymization secret (i.e. the key needed to pseudonymize and reidentify the participants, "inner encryption") is itself encrypted, with a dedicated hardware module ("outer encryption"). The dual encryption scheme is implemented in python and extended with two other modules: a flask application that hosts a local webserver and employs an internet browser as user interface and a "LimeSurvey controller" module, to communicate with a LimeSurvey web application instance over the internet (optional). To ensure seamless integration of the ALIIAS-based pseudonymization tools with a wide variety of research settings, customizability is a key requirement. ALIIAS provides a range of selectable and personalized functionalities, including but not limited to two-factor authentication and hardware security tokens, as well as the ability to create custom short-form pseudonyms. Furthermore, ALIIAS seamlessly integrates with the widely used survey assessment tool, LimeSurvey [17]. An overview of the core components of the ALIIAS methodology can be found in Fig. 1, the technical details are outlined in the following sections.

Application customization can occur during the deployment process and can range from making changes to a straightforward, easily understandable configuration file to enhancing or altering the default software functionality by modifying the source code. As a result, in case of simpler research projects with limited

[1] "**Data subject** is a natural person whose personal data are processed and may be subject to pseudonymization. The term individual is also used in the text to refer to a data subject. Moreover, the term user is utilized in the same sense, especially when discussing online/mobile systems and services" [1].

[2] "**Data controller** is the entity that determines the purposes and means of the processing of personal data (article 4(7) GDPR). The data controller is responsible for the data processing and may employ pseudonymization as a technical measure for the protection of personal data" [1].

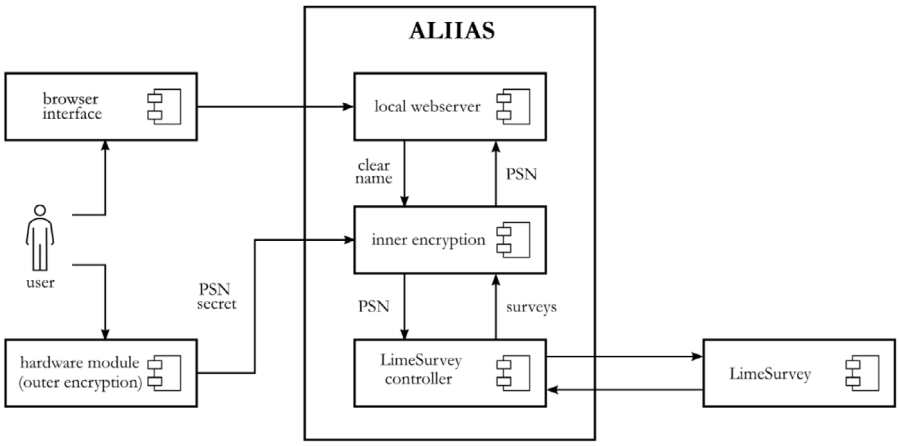

Fig. 1. The ALIIAS architecture is centered around a dual encryption scheme for generating the pseudonyms (see Section 2.1 for details). A local webserver provides a browser-based user interface and an optional LimeSurvey interface is provided.

customization needs, ALIIAS-based end-user applications may be deployed by the researcher. On the other hand, IT-professionals working on more complex multi-site projects have the opportunity for deep-customization, allowing seamless integration with a wide variety of research settings.

2.1. Software architecture

Dual Encryption scheme with support for hardware security modules

ALIIAS builds on encryption to create pseudonyms, as the algorithms are designed to be robust against adversarial attacks and are computationally highly efficient (typical running time < 1 ms). This also reduces the pseudonymization secret to a single point: the encryption key, which streamlines the management and protection of the pseudonymization process. ALIIAS can be used in two ways, meeting different levels of safety at the data controller's research infrastructure. In single-center situations, where strict safety requirements of the system hosting the ALIIAS-based end-user application can be ensured ALIIAS can be utilized in its "safe-host mode". In this mode, the secret used for pseudonymization is stored in an unprotected format, specifically in a configuration file, on the secure host computer. However, as the safety of the hosting system is often hard to guarantee, especially in multi-center studies with host computers that are in shared use, ALIIAS can be used in "hardware security mode". In this case, the pseudonymization secret is protected by a hardware security module (HSM) [18], employing the so-called "dual-encryption" scheme (Fig. 2).

In both modes, an encryption key P is used to generate the pseudonym C from the participants personal information X *(by default: first and last name, mother's maiden name, place and date of birth)* with an arbitrary deterministic encryption algorithm Φ_P(Eq. (1)).

$$C = \Phi_P(X) \tag{1}$$

The encryption key P will therefore be referred to as the "pseudonymization key". P is generated upon the process of deploying a project-dedicated end-user application. In "safe-host mode", P is simply stored in a configuration file, to be copied to the host computer. In "hardware security mode", P is instantly encrypted with another, asymmetric cryptographic algorithm Φ_T at deployment time with the public key of an asymmetric keypair T_{pub} *(Eq. (2)).*

$$Q = \Phi_{Tpub}(P) \tag{2}$$

Consequently, access to the pseudonymization secret will only be possible through decryption (Eq. (3)) with the private key T_{priv}.

$$P = \Phi^{-1}_{Tpriv}(Q) \tag{3}$$

Importantly, T_{priv} is generated and stored on an HSM token. In this case, it is guaranteed that T_{priv} never leaves the token and the decryption procedure $\Phi^{-1}_{Tpriv}(Q)$ can only take place on the cryptographic hardware module of the token. Therefore, in "hardware security mode", the safety of the pseudonymization secret can be guaranteed simply by preventing unauthorized access to the HSM token. Both pseudonymization and reidentification requires, in this case, access to both the (pin-code protected) HSM token and the host computer.

Recovery of the participant information X happens simply by decrypting the pseudonym C using Φ_P^{-1} (Eq. (4)).

$$X = \Phi_P^{-1}(C) \tag{4}$$

Pseudonymization protocol

ALIIAS employs a pseudonymization protocol that guarantees user authentication and safeguards against man-in-the-middle attacks. This protocol prevents any unauthorized alteration of the pseudonymization key on the host machine after deployment. The pseudonymization workflow, specifically the separation of duties between the software and the hardware token (if in use), are detailed in Fig. 3.

The protocol starts with plugging in the HSM token into the USB-port of the host computer and starting the executable file of the end-user application. If the two-factor authentication is activated, the user will be prompted for the user pin of the security token. The hardware security token then decrypts the handler file, which reveals the pseudonymization key to the software. Next, the pseudonymization key is used to decrypt a verification phrase that has been set up and encrypted with the pseudonymization key during software deployment and supplied in an encrypted form with the end-user application. The user must confirm this verification phrase to continue. An invalid phrase indicates that the pseudonymization key has been corrupted since deployment (which might be a consequence e.g., of a man-in-the-middle attack, changing the handler or the executable file on the host computer). If LimeSurvey integration is enabled, the user can use his/her credentials to log in to LimeSurvey through the browser UI. Up to this step, the protocols for pseudonymization and re-identification are identical but diverge for the remaining steps.

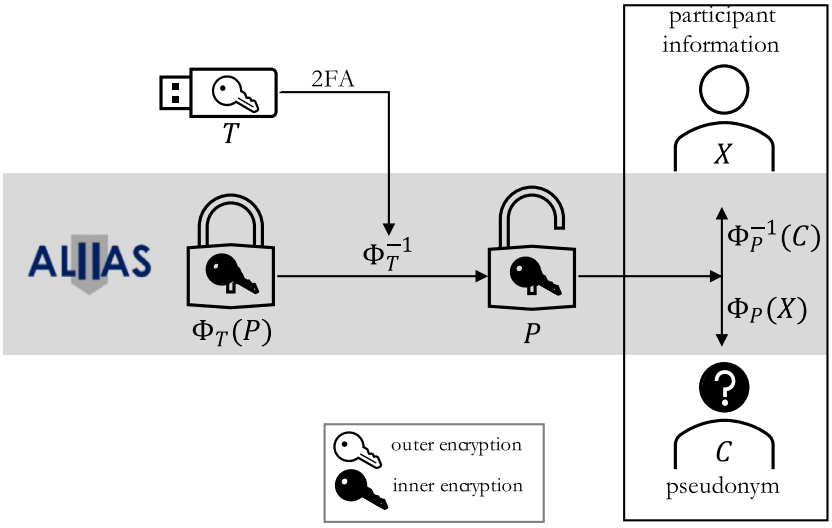

Fig. 2. Dual-encryption, the core concept of the pseudonymization workflow of ALIIAS. The pseudonymization key P is shipped in an encrypted form alongside the pseudonymization application, but can only be accessed through a pin-lockable security token T.

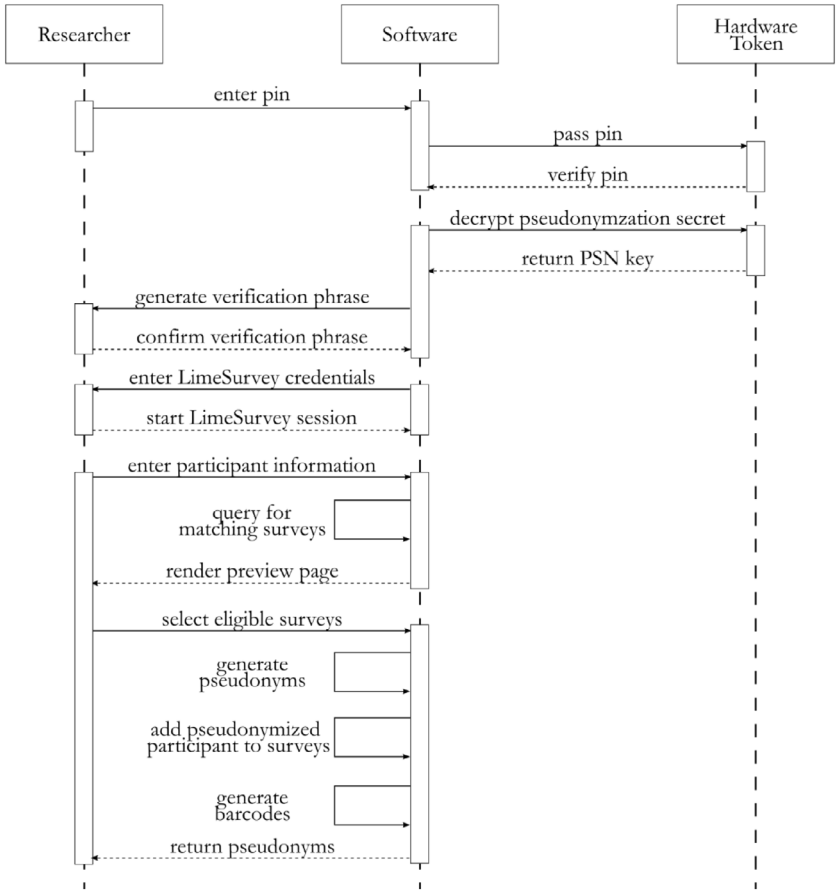

Fig. 3. UML sequence diagram of the pseudonymization process, which highlights the distribution of responsibilities among the researcher, the software and the hardware token (with all possible features enabled).

For pseudonymization, the researcher can now enter the participants personal information into the predefined fields in the user interface. After confirming, the user is directed to a preview screen where the given inputs can be reviewed and corrected if necessary. If the LimeSurvey integration is activated, the user can select the surveys to which the participant should be added (with his or her pseudonym). At this stage, the user can then advance to the pseudonym by clicking the corresponding button, at which point the software generates long and short forms of pseudonym based on the pseudonymization key, and it automatically adds the participant to the previously selected surveys and generates the invitation links for the questionnaires. If barcode generation is enabled, ALIIAS also generates and displays the barcode representation of the pseudonym.

For reidentification, instead of entering the personal information of the participant, the researcher enters the long-form pseudonym into a dedicated tab in the UI. The pseudonym is then reidentified using the pseudonymization key, which reveals the participants personal information.

Implementation details and deployment process

ALIIAS is mainly written in Python 3 and builds upon the vast open-source ecosystem of Python whenever possible. The framework relies on the python package 'pyinstaller ', to build and deploy project-dedicated end-user pseudonymization tools quickly and effortlessly. The default encryption scheme is a combination of a RSA and an AES encryption, as they have both been proven highly reliable in a wide array of applications. Flask was chosen as the backend for the local webserver, as it allows a lightweight Python solution, and the browser-based user interface enables the possibilities to deploy pseudonymization software within a local network. ALIIAS was optimized for a Microsoft Windows system but can also be deployed for MacOS. During deployment, all files needed for the end-user application, are packaged inside of a single, portable executable file, except the two configuration files (settings.conf, handler.txt), which allow customizing several aspects of the software, from logging and LimeSurvey server data to custom pseudonym character base and barcode generation. Before deployment, it is possible to customize the GUI (e.g., adding a project-specific logo) by editing a single css file (second-level customization). The source code was designed so that advanced users can relatively easily extend the framework with an alternative encryption algorithm (default: AES-SIV [19]) or modify the default pseudonymization protocol.

The setup of HSM tokens (in case "hardware security mode" is activated during deployment) is independent of the executable software and requires running a set of python command line scripts supplied with ALIIAS. Therefore, additional tokens can be added at any time even if the software is already deployed. In the first step, the token must be initialized. Two-factor authentication can be activated by setting up the "user" pin on the HSM module. In this case, the module becomes inaccessible without this pin and the user will have to provide the pin upon each startup of the end-user application. After the initialization, the (T_{priv}, T_{pub}) key-pair is generated on the token. With the token generated, the pseudonymization key is encrypted and stored in the *handler* file, which is shipped alongside the application. The handler file can manage multiple tokens and can be adjusted dynamically to add or remove any hardware keys.

Viable deployment structures

The decentralized pseudonymization workflow of ALIIAS suits a wide range of research scenarios, from single-site projects with one pseudonymization key and one (Fig. 4 A) or more (Fig. 4B) HSM tokens, to multi-center research consortia using separate pseudonymization keys per site (Fig. 4C) and multiple tokens per project (e.g. mixing B and C on Fig. 4). ALIIAS provides a highly scalable pseudonymization solution, even if ethical and privacy requirements are different across projects (e.g., if reidentification must only be within project). Pseudonymization keys, and hardware security tokens can dynamically added/removed to the deployed pseudonymization workflow.

2.2. Software functionalities

- **Encryption-based pseudonymization in a decentralized way**: implemented with the python encryption package PyCryptodome, see Section 2.1 for details.
- **Maximal safety with Hardware Security Module**: support for USB hardware security tokens that can be accessed through the OpenSC smart card python module [20]. This feature is currently tested with Nitrokey HSM2 security tokens (Nitrokey GmbH, Teltow, Germany) [21] .

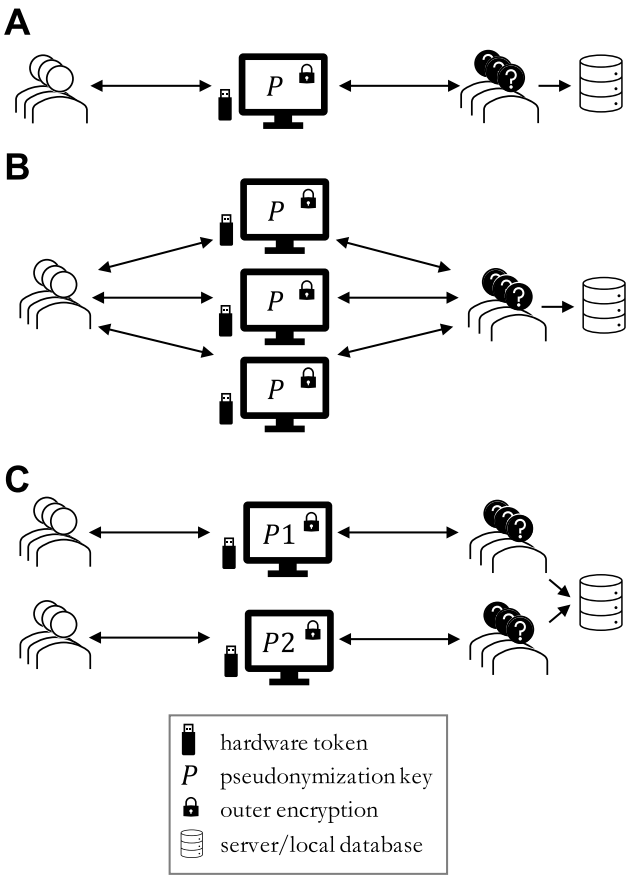

Fig. 4. Different use case scenarios for the integration of ALIIAS: **A** uses a single instance of the software to generate pseudonyms, **B** deploys multiple instances of ALIIAS based on one identical pseudonymization key and multiple security tokens. Configuration **C** deploys with different pseudonymization keys to comply with different privacy/ethical requirements of different experimental centers.

- **Custom pseudonym representations:** the character set used for the pseudonym can be customized to match the project-specific requirements. The default custom character base includes the numbers 1–9 and the letters a-z, excluding 'i', 'l' and 'o' to avoid clerical errors when using the pseudonym. As the full pseudonym may be impractical to use due to its length, it can optionally be hashed into an irreversible short-ID. The hash algorithm is customizable, although – depending on the choice of the pseudonym encryption method – simply truncating the Long-ID usually provides an already sufficient hashing performance, see Section 3 for details.
- **Barcodes** ALIIAS provides the option to automatically generate customizable barcodes (via 'python-barcode') with the creation of new pseudonyms. Size and type of barcodes is customizable (default type: 'code128').
- **Graphical User Interface:** the GUI is hosted by a local flask webserver which can be accessed through any regular web browser. The user interface is designed using HTML and Jinja and aims to streamline the pseudonymization and reidentification process to make it as accessible and as intuitive as possible.
- **LimeSurvey integration:** ALIIAS provides optional integration to the open-source survey web application LimeSurvey [14] via its RCP API. After logging in into LimeSurvey through the user interface, the user can add new participants to specific surveys via the newly generated pseudonym and list the surveys the given participant has already been assigned to.

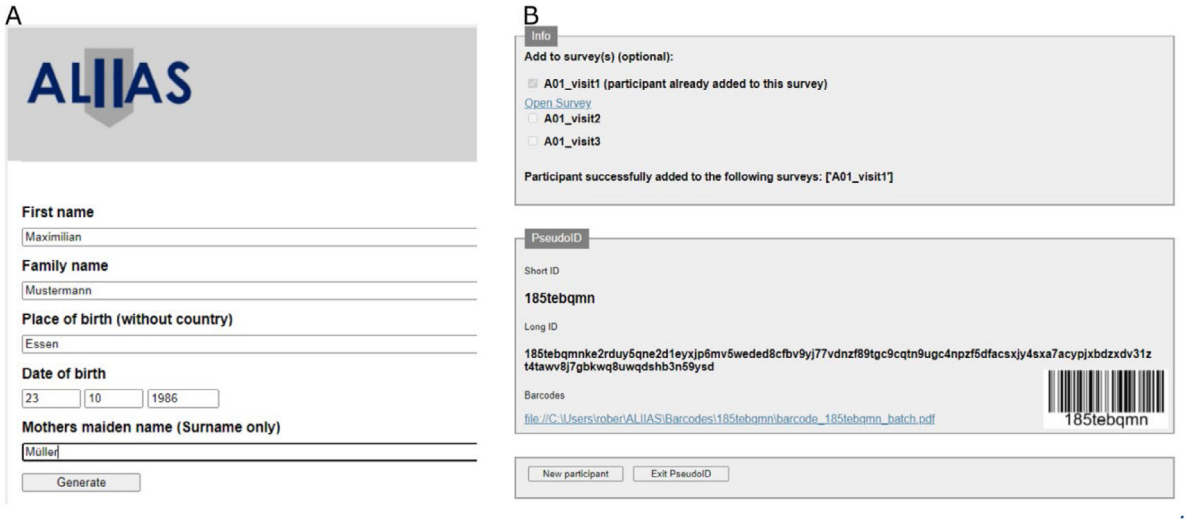

Fig. 5. Screenshots of the example application deployed with ALIIAS, during inputting personal data (A) and displaying pseudonyms (B).

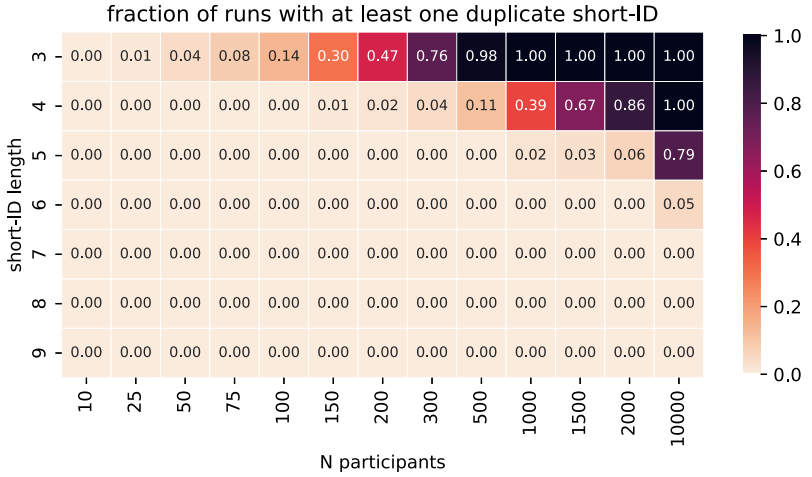

Fig. 6. Permutation testing results for possible duplicate Short-IDs. The fraction of duplicate runs (out of 100000) is shown for Short-ID length over number of participants.

3. Illustrative example

We introduce a working example of a pseudonymization software deployed with ALIIAS (Fig. 5), which can be downloaded from the corresponding GitHub repository along with an extensive user manual (https://github.com/pni-lab/ALIIAS/releases). The example application has been deployed in "safe-host mode", with a default pseudonymization key and can be tested without HSM token. Therefore, in the form it is downloaded from the repository, the example application serves solely demonstrational purposes. Nevertheless, by editing the configuration file and, optionally, providing a handler file that has been properly set-up with HSM tokens, the example application becomes safely deployable with real participant data. The example application is linked to a LimeSurvey server that can be used for testing the software. Login credentials are provided at the GitHub repository.

In the example application, short-IDs are generated by simply taking the first 8 characters of the pseudonym. This choice was based on simulations (study size: N=10000, participant data based on a database of common german names, cities as place of birth and a mean age of 30, with standard deviation of 10 years), that confirmed that the probability for duplicate short-IDs is extremely low in this case (Fig. 6).

The pseudonymization is based on AES-SIV encryption (32 bytes key length), which derives the initialization vector for the encryption from the actual plaintext, making the encryption deterministic. The default encryption used for the hardware security module (which is deactivated in the demo version), is an RSA encryption with 2048 Bit.

4. Impact

ALIIAS allows creating dedicated, encryption-based pseudonymization tools for human research and thereby makes advanced pseudonymization techniques available in a wide variety of research settings. Encryption-based pseudonymization, as implemented in ALIIAS, ensures long-term re-identifiability of

pseudonymized data, increases the safety of the pseudonymization secret and simplifies public data sharing.

ALIIAS has been successfully used to deploy a pseudonymization tool for the Collaborative Research Center TRR289 "Treatment expectation" [22,23]. The deployed software tools handle a total of 14 HSM tokens and generate unique pseudonyms for 12 sub-projects at three universities (University Hospital Essen, Medical University Hamburg-Eppendorf, University of Marburg) and has already been used to pseudonymize thousands of participants. First experiences clearly demonstrate that with ALIIAS, encryption-based pseudonymization can be seamlessly integrated into existing complex, multi-site research workflows, resulting in a safe and easy-to-use alternative to previously used approaches, like sequential numbering. In the next phase of development, we will build on experiences made within the Collaborative Research Center TRR289 to equip ALIIAS with additional interfaces (e.g., support for different hardware keys and other survey engines) to make it more accessible for the general research community. Adaptation of ALIIAS by the community will be supported by a detailed on-line documentation and dedicated hands-on workshops targeting multiple levels of users, with the aim of turning ALIIAS into an open-source community effort. We will aim to deliver the ALIIAS framework to smartphones and tablets in the future, with an additional focus on use-cases outside of medical research".

5. Conclusions

Pseudonymization can be a powerful tool to meet data protection guidelines, in order to protect both the data subject and the data controller. We aim to provide a solution that maximizes the levels of security of the data subject's data, while not introducing a Trusted Third Party. We also aim to provide a pseudonymization, that can replace the common practice of manual pseudonymization and offer a lightweight alternative to highly complex pseudonymization systems. With ALIIAS, we present a customizable pseudonymization framework that is accessible for researchers of varying disciplines. ALIIAS allows easy and flexible deployment of pseudonymization software that is dedicated to the special requirements of a given research project, while allowing to adjust key aspects of the software to comply with varying ethical and experimental requirements. Through the incorporation of hardware security tokens, the software can be deployed securely and independently to a wide variety of research infrastructures, which greatly decreases the initial threshold for establishing a state-of-the art, encryption-based pseudonymization solution into an existing workflow.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The entire code is accessible on https://github.com/pni-lab/ALIIAS.

Acknowledgments

This research was supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation): TRR 289 Treatment Expectation - Projektnummer 422744262.

References

[1] Recommendations on shaping technology according to GDPR provisions - An overview on data pseudonymisation. ENISA; 2023, https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions. (Accessed 04 July 2023).
[2] Grover B, Kushwaha DK. Authorization and privacy preservation in cloud-based distributed ehr system using blockchain technology and anonymous digital ring signature. Health Serv Outcomes Res Methodol 2023;23(2):227–40. http://dx.doi.org/10.1007/s10742-022-00281-z.
[3] Bouchelaghem S, Omar M. Secure and efficient pseudonymization for privacy-preserving vehicular communications in smart cities. Comput Electr Eng 2020;82:106557. http://dx.doi.org/10.1016/j.compeleceng.2020.106557.
[4] Horvitz E, Mulligan D. Data, privacy, and the greater good. Science 2015;349(6245):253–5. http://dx.doi.org/10.1126/science.aac4520.
[5] Heurix J, Neubauer T. Privacy-Preserving storage and access of medical data through pseudonymization and encryption. 2011, p. 197. http://dx.doi.org/10.1007/978-3-642-22890-2_16.
[6] Paul M, Maglaras L, Ferrag MA, Almomani I. Digitization of healthcare sector: A study on privacy and security concerns. ICT Express 2023. http://dx.doi.org/10.1016/j.icte.2023.02.007.
[7] Dennis S, et al. Privacy versus open science. Behav Res Methods 2019;51(4):1839–48. http://dx.doi.org/10.3758/s13428-019-01259-5.
[8] Kiourtis A, et al. Electronic health records at People's hands across Europe: The InteropEHRate protocols. Stud Health Technol Inf 2022;299:145–50. http://dx.doi.org/10.3233/SHTI220973.
[9] Ko H. Pseudonymization of healthcare data in South Korea. Nature Med 2022;28(1):15–6. http://dx.doi.org/10.1038/s41591-021-01580-7.
[10] Bolognini L, Bistolfi C. Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation. Comput Law Secur Rev 2017;33(2):171–81. http://dx.doi.org/10.1016/j.clsr.2016.11.002.
[11] Gruschka N, Mavroeidis V, Vishi K, Jensen M. Privacy issues and data protection in big data: A case study analysis under GDPR. In: 2018 IEEE international conference on big data. 2018, p. 5027–33. http://dx.doi.org/10.1109/BigData.2018.8622621.
[12] Noumeir R, Lemay A, Lina J-M. Pseudonymization of radiology data for research purposes. J Digit Imag 2007;20(3):284–95. http://dx.doi.org/10.1007/s10278-006-1051-4.
[13] Neubauer T, Heurix J. A methodology for the pseudonymization of medical data. Int J Med Inf 2011;80(3):190–204. http://dx.doi.org/10.1016/j.ijmedinf.2010.10.016.
[14] Aamot H, Kohl CD, Richter D, Knaup-Gregori P. Pseudonymization of patient identifiers for translational research. BMC Med Inform Decis Mak 2013;13(1):75. http://dx.doi.org/10.1186/1472-6947-13-75.
[15] Lablans M, Borg A, Ückert F. A restful interface to pseudonymization services in modern web applications. BMC Med Inform Decis Mak 2015;15(1):2. http://dx.doi.org/10.1186/s12911-014-0123-5.
[16] Dimopoulou S, Symvoulidis C, Koutsoukos K, Kiourtis A, Mavrogiorgou A, Kyriazis D. Mobile anonymization and pseudonymization of structured health data for research. In: 2022 Seventh international conference on mobile and secure services. 2022, p. 1–6. http://dx.doi.org/10.1109/MobiSecServ50855.2022.9727206.
[17] Klieve H, Beamish W, Bryer F, Rebollo R, Perrett H, Muyzenberg JVD. Accessing practitioner expertise through online survey tool LimeSurvey. 2010, [Online]. Available: https://www.semanticscholar.org/paper/Accessing-Practitioner-Expertise-Through-Online-Klieve-Beamish/79605c7285ac29095652d3afba8ada7ca6af3f89. (Accessed 04 Jul 2023).
[18] Wolf M, Gendrullis T. Design, implementation, and evaluation of a vehicular hardware security module. In: Kim H, editor. Information security and cryptology. Lecture notes in computer science, vol. 7259, Berlin, Heidelberg: Springer; 2012, p. 302–18. http://dx.doi.org/10.1007/978-3-642-31912-9_20.
[19] Harkins D. Synthetic initialization vector (SIV) authenticated encryption using the advanced encryption standard (AES). 2008.
[20] Talamo M, Galinium M, Schunck CH, Arcieri F. Secure messaging implementation in OpenSC. J Inf Secur 2012;03(04). http://dx.doi.org/10.4236/jis.2012.34032, Art. (04).
[21] Nitrokey. 2023, https://www.nitrokey.com/startseite. (Accessed 04 July 2023).
[22] SFB treatment expectation, TRR 289. 2023, https://treatment-expectation.de/. (Accessed 04 July 2023).
[23] Meizner C, et al. Disentangling pharmacological and expectation effects in antidepressant discontinuation among patients with fully remitted major depressive disorder: Study protocol of a randomized, open-hidden discontinuation trial. BMC Psychiatry 2023;23(1):457. http://dx.doi.org/10.1186/s12888-023-04941-3.

DOI: 10.1016/j.softx.2023.101522
URN: urn:nbn:de:hbz:465-20250107-132107-7