Decision-based Data Distribution (D³): Enabling Users to Minimize Data Propagation in Privacy-sensitive Scenarios

Sebastian Linsner
PEASEC, TU Darmstadt
Darmstadt, Germany
linsner@peasec.tu-darmstadt.de

Kilian Demuth
PEASEC, TU Darmstadt
Darmstadt, Germany
demuth@peasec.tu-darmstadt.de

Marc Fischlin
Cryptoplexity, TU Darmstadt
Darmstadt, Germany
marc.fischlin@tu-darmstadt.de

Christian Reuter
PEASEC, TU Darmstadt
Darmstadt, Germany
reuter@peasec.tu-darmstadt.de

ABSTRACT

In many scenarios, users have to communicate sensitive data with third parties such as doctors, lawyers, insurance companies, social workers, or online shops. Handing over personal data is necessary to use those services, but delegating tasks to increase efficiency still poses the risk that personal data might be leaked. To minimize this risk and further enhance the privacy of users, we propose an interaction concept that uses layered encryption of messages to provide a trade-off between privacy and usability. Users can choose which data is additionally encrypted in an inner layer, e.g. only for the eyes of their doctor, and which data is available in an outer (encrypted or unencrypted) layer for all staff members. Another benefit is the hiding of sensitive data from package inspection or crawling algorithms via emails, while less critical parts can still be processed by these systems via the partial access. To investigate this concept, we derive relevant use cases for form-based communication via email from a quantitative pre-study with 1011 participants, showing that general practitioners are the most suitable use case. We developed demonstrators for this use case and evaluated them in a qualitative study with 42 participants. Our results show that the possibility of minimizing the propagation of sensitive data through additional encryption is highly appreciated and the usage of form-based communication is a promising approach for digital transformation.

KEYWORDS

user-centered design, usable privacy, layered encryption, qualitative study

1 INTRODUCTION

In December 2022, Google announced it would integrate client-side encryption in its mail clients for enterprise workspace and educational customers. While this clearly advances end-to-end security for users, it also comes with a downside, as Google notes on its support page[1]: "Client-side encrypted files and emails aren't scanned for phishing and malware, because Google's servers don't have access to the content." Hence, while users gain confidentiality through the established end-to-end encryption, they also degrade their own security by precluding Google from scanning for malicious emails.

The trade-off between confidentiality and accessibility is not new, and has been discussed extensively in many facets before [6, 27, 82]. The reasons for giving access to protected communication, where today this protection is either accomplished via plain encryption or by secure channels like TLS, may be conflicting security desires [22]. The end-users may wish for malware protection or intrusion detection, as in the Google example above, or may have other, more subtle reasons like caching or compression for performance [54].

Arguably, the most visible example where confidentiality and accessibility clash is lawful interception. Recently, the most prominent case may have been the efforts of major providers to integrate detection mechanisms for illicit content, such as child sexual abuse material (CSAM) [66]. This includes Apple's NeuralHash, Microsoft's PhotoDNA, and Facebook's PDQ, which scan for suspicious image or video material at the client side and report potential cases to the providers. Beyond the political dimension, it turns out that the approaches behind the deployed perceptual hash functions, which should tolerate small changes in the images, are all cryptographically weak [40, 61] and thus do not provide the required level of effectiveness.

From a technical viewpoint, the situation in the area of intrusion detection and malware protection for encrypted data looks much better than for perceptual hashing. Initially, the most common solution for intrusion detection was to give the firewall access to the shared key so that the system could access the protected data in clear form. Alternatively, but effectively identical, the middlebox may securely connect to each end-user and relay the data. In recent years, researchers have developed improved solutions for this problem, aiming to re-establish privacy for the users and their data while maintaining a minimal level of accessibility for the detection systems. Examples are the Blindbox protocol [71], the recently proposed concept of zero-knowledge middleboxes (ZKMB) [35, 83], and multi-context TLS [53]. Roughly, these approaches encrypt

Proceedings on Privacy Enhancing Technologies 2024(4), 185–208

https://doi.org/10.56553/popets-2024-0113

[1] https://support.google.com/a/answer/10741897?hl=en, accessed August 21st, 2023.

communication with a secure end-to-end mechanism but also provide additional information to the detection system, enabling it to check for malicious content.

Another recent proposal is to use stealth key exchange and channels in TLS 1.3 [29], where the sender determines to which partial content the detection system has access, and which part should be kept confidential. The solution relies on the ability to generate a second shared key in the key establishment of TLS "for free". Consequently, one key can be shared with the middlebox, and the other is only known to the end-users. The sender can then decide which data should be encrypted additionally under the extra key and thus remain hidden from the middlebox. The middlebox only gets access to the other data. We note that outsiders do not have access to either kind of data. Therefore, in contrast to Blindbox and ZKMB, the approach reveals partial information to the detection system but is faster and easier to integrate into existing network protocols. In the context of this paper, we use the term partially-accessible encryption to describe the utilization of layered encryption to hide sensitive information from recipients without the second shared key.

Given that we now have the technical possibilities to select a continuous balance between confidentiality and accessibility in encrypted communication, the question remains what the users want and if they would be willing to adopt such a system. Therefore, our research question to investigate possibilities, trade-offs, and pitfalls for layered encryption in real-world scenarios is:

> **'How do users perceive the possibilities of partially-accessible encryption in everyday scenarios?'**

In order to answer this question, we first conducted a representative quantitative study in Germany with 1011 participants to find out which communication is especially perceived as sensitive by users and, therefore, appropriate for an idea like ours. We found the communication with doctors and lawyers to be particularly sensitive and chose the former for the implementation of demonstrators. We opted for two demonstrators to investigate the so-called control paradox, a phenomenon described in the literature that leads to increased data disclosure when granting more control over the disclosure to the users [13] [9]. Therefore, we built two different versions of a contact form which can be used to request a prescription or a referral from a doctor. In one version, the user can decide which information is visible only to the doctor. In the other version, all information is visible to the entire medical office, with the exception of one text field in which the user can write information that can only be seen by the doctor. These two demonstrators were finally evaluated in a qualitative study with 42 participants. We found that around 74% of users preferred the version where they can decide which information is visible only to the doctor and appreciated the freedom of choice granting them sovereignty over their data. The participants highly appreciated the easy-to-use concept of partially-accessible encryption and were curious about a real-world adoption since our concept would reduce physical and social barriers to seeking help and would make interaction with doctors easier. Furthermore, the majority of the participants appreciated the feeling of control over their own data.

2 RELATED WORK

As this paper covers multiple research areas, related works to the presented concept feature discussions about secure communication of sensitive data in general, (partially-)accessible as well as usable encryption. Lastly, the discussion about the control paradox has to be considered for this study and is therefore outlined.

2.1 Sensitive and Secure Communication

The research on secure communication with professions where sensitive data needs to be transmitted has widely differing approaches.

Lerner et al. [49] specifically targeted the communication of sensitive data via email and introduced an email client to facilitate email encryption. Another very widespread approach to secure communication is the use of blockchain, e.g., to store and share electronic medical records securely [24]. Li et al. [50] used blockchain technology to propose a scheme for evidence management to achieve witness privacy. Zheng et al. [84] used blockchain for secure communication of medical insurance claims to ensure privacy and legitimacy. Yadav et al. [81] similarly addressed the problem of privacy-preserving insurance registration with blockchain and smart contracts. A different approach to secure communication, only prevalent in the e-commerce domain, was the use of quantum security. Most recently, the work of Thapliyal and Pathak [75] presented four different quantum protocols to guarantee security in online shopping, building upon approaches by Chou et al. [16] and Huang et al. [38].

2.2 Partially-Accessible Encryption

Governmental organizations argue the importance of so-called lawful interception, usually with the need to fight crime or for reasons of national security ("going dark"). However, beyond the political dimension of this, the examples of client-side scanning for illicit material, as in the case of NeuralHash, PhotoDNA, and PDQ, show that the technical solutions in this area are far from mature [40, 61]. The European Union is currently discussing similar measures under the term "chat control". The EU proposal has received a lot of criticism regarding data protection, and its lawfulness is highly disputed, even within the EU [76].

The possibility of middleboxes being able to access encrypted data legitimately has a long history. It is based on the observation that it may be in the interest of users (e.g., when protecting them from malicious attachments or when compressing data to save resources) or in the interest of the party running the detection system (e.g., a company trying to prevent attacks on their system) [23]. We focus here on cases where the user can decide whether to use these measures or not. In the widely deployed TLS protocol, granting the middlebox access is possible via the usage of static Diffie-Hellman keys (or, in earlier versions of TLS, also for RSA keys). In this case, the middlebox would be able to decrypt the secured communication data. Unfortunately, this approach with static keys infringes on the notion of forward security, that past sessions should still be protected if the adversary gets access to static private keys. Yet, Green et al. [34], for instance, describe such a TLS 1.3 variant with static keys. Another widely used option is to let the middlebox break up end-to-end encryption. That is, the middlebox establishes a secure connection with one user and another one with the other

user, re-encrypting data when routed through the middlebox. This is, for example, the path middlebox-aware TLS (maTLS) takes [48]. In addition to the loss of end-to-end security, these proxy solutions introduce other risks, such as insufficient certificate validation [21].

As mentioned in the introduction, the shortcomings of the above approaches lead researchers to develop advanced methods such as Blindbox [71], ZKMB [35, 83], multi-context TLS [53], and stealth key exchange for TLS 1.3 [29]. However, Fischlin [29] was able to integrate the key exchange into TLS 1.3 without modifying the network layer of the original protocol, although lacking in flexibility and security compared to Blindbox and ZKMB. The idea by Fischlin [29] of sanitizable channels to allow for a middlebox to alter parts of the payload builds on the concept of sanitizable signatures [5], sanitizable signcryption [28] and access control encryption [20, 31, 43, 79]. Fischlin [29], however, applies this concept to symmetric-key cryptography in real-world channel protocols, which had not been covered before.

There are some methods that follow a similar objective as this paper, namely, structured encryption and, more specifically, searchable encryption and variants of both. They describe ways to store data and perform actions, e.g. by searching through it via an untrusted server, while the server cannot learn any information about the data [4, 12, 25, 41, 42, 44, 72, 74]. Most research, however, sees the use case for this in the storage of large databases [46], wherein the storing and accessing of data is done by the same person [3, 11, 33, 52, 58], contrary to the approach presented here.

Finally, layered encryption is also used in onion routing protocols, especially Tor [26]. There, the goal is to hide path information from the onion routers and outsiders. This is accomplished with an overlay network, whereas the other aforementioned solutions for detection systems usually try to stay close to the original network infrastructure. Ideally, the content in onion routing protocols is still end-to-end encrypted and only available to the intended recipient.

2.3 Usability of Encryption

There has been a general discussion about the security usability trade-off for some time. Some authors agree that there is a clear trade-off between security and usability [1, 14, 45] and try to mitigate the effect in differing ways, trying to aid practitioners [2, 8]. Others see the current discussion as less expedient and point out that a more fine-grained assessment of a possible security usability trade-off is necessary. They state that uncertainty about factors leading to the problem and the methods used to research the suggested dichotomy are insufficient for a clear statement [68, 69]. Some, on the other hand, claim to have found ways to diminish the caused harm [51, 55]. To consider a possible trade-off, this work follows the proposal of Alsuhibany [1] to analyze the usability of a new security feature precisely. Other studies have focused more on concrete practice examples regarding the usability of encryption tools and mechanisms. Since Whitten and Tygar [80] has shown that the usability of PGP 5.0 was insufficient, there has been a discussion about usable email encryption. Multiple papers showed similar results to Whitten and Tygar [80] by conducting user studies on usable email encryption by means of PGP clients, stating that users would be frustrated or unable to successfully use these or giving recommendations for future improvement [7, 64, 67, 70, 77]. Borradaile et al. [10], on the other hand, were able to show that if the motivation was high enough, over 50% of study participants would continue to use PGP for secure email communication after a short training period. Since the end of 2022, Google has been offering the possibility of email encryption to selected customers (Enterprise Plus, Education Standard, and Education Plus) in the browser-based mail client. The confidential mode introduced previously in 2018, although perceived by users to use end-to-end encryption, did not offer this service [62]. The new client-side encryption (CSE) from 2022, essentially represents an end-to-end encryption and allows users to control the key management. Because this hinders Google servers from accessing the email content after encryption, emails can no longer be checked for malicious content.

2.4 Control Paradox

Literature often shows that it is important to give users control over their data [19]. Other than by technology, the use of data can also be controlled by laws or policies which need to adapt to the rapidly changing technology [47]. In contrast, recent literature shows the existence of the so-called 'control paradox': Brandimarte et al. [13] and Boer et al. [9] showed that users reveal more personal information when given more control about their shared personal information, which in turn leads to a higher risk of identifiability. However, Colnago et al. [18] warn that self-assessments by study participants about their privacy concerns and behavior can be misleading and that respective privacy measures are often taken more regularly than participants think. Additionally, concerns about security and privacy vary widely among individuals and particular risk scenarios [18, 32, 63]. Therefore, we can also examine the control paradox and observe which information is published when users receive control over the disclosure of their personal information.

2.5 Research Gap

As discussed, allowing users to encrypt their communication can increase their security and privacy, but this requires some effort. This is the reason for lacking adoption of encryption tools such as PGP. Another usability-related problem is that users can make poor privacy decisions because of the negative effects of information overflow or the control paradox. Even if those problems are overcome, the user has to deal with the trade-off between privacy and usability. As the Google CSE debate shows: better encryption can diminish the possibility of malware checks. Furthermore, encrypted content is not available for search operations in the mailbox.

To combat these problems, we propose the usage of partially-accessible encrypted messages. The users are enabled to define which information is protected with additional encryption and which information is transmitted 'normally' (either unprotected or still encrypted but for a broader audience). This way, we reduce the cost of the privacy-usability trade-off and allow search operations on the accessible part of the message. By freedom of choice, users can opt not to use the feature if they do not want to invest time and thought for additional protection. On the other hand, users with a strong preference for privacy can fully customize the message to meet their desired level of protection. Enabling users to act without enforcing it makes this system viable for a variety

of target groups. For this purpose, we provide a concept for the use of partially-accessible encrypted messages in an everyday use case (see Section 4) derived from a representative pre-study (see Section 3). To investigate the usability of such a system as well as the effects of the control paradox, we implement demonstrators for a qualitative study (see Section 5). An overview of the applied methods can be found in Appendix A.4.

3 QUANTITATIVE PRE-STUDY

In order to find suitable use cases for our study, we conducted a quantitative pre-study. This was considered necessary to ensure that the design and the use case were suitable for German participants. Literature shows that Germans differ from other European (and non-European) citizens with regard to risk culture and attitude towards authorities [65]. For a detailed discussion of these regional differences, see Section 6.4. Furthermore, the recent pandemic accelerated the adoption of digital tools for work and social life. Therefore, reliable data for an appropriate use case for our interaction concept is needed.

3.1 Methodology

While the personal data collected was limited to age, gender, education, income, and state, participants were transparently informed about the goals of the study and then asked for their informed consent to participate. For the inquiry, we selected GapFish (Berlin) as an ISO-certified panel provider, which ensures panel and data quality, representativeness for the German population, security, and survey quality within their panel of 500,000 active participants. After transmitting the final questionnaire, GapFish programmed and hosted the online survey. Once final quality checks, a soft launch, and mutual agreement were achieved, they invited participants from their panel to take part in the survey in April 2023 (N=1,011, t: 1 min. per question). The sample comprised 1011 persons living in Germany, of which 517 identified as female, 493 as male, and one as diverse. The age of the participants was distributed in a broad range: 8% were between 18 and 24, 15% between 25 and 34, 15% between 35 and 44, 16% between 45 and 54, 19% between 55 and 64 and 28% were 65 or older. The participants' monthly income was distributed as follows: 18% had an income lower than €1500, the income of 27% was between €1500 and €2600, that of 35% was between €2600 and €4500, and 19% had an income above €4500. 26% of our participants had at least a general high school leaving certificate (German average 28.6%), 5.49% had a former GDR general education certificate (German average 6,5%), 30.56% had an intermediate school-leaving certificate (German average 23.5%), 35.5% had college/university entrance qualification (German average 33.5%), and 16.29% had studied at a university or college (German average 17.3%). The values for the German average were taken from the federal office for statistics (Statistisches Bundesamt)[2]. For the sake of research economics we chose to participate in a joint survey with other researchers of our department (18 items total). We are aware that this might affect the answers of the participants, but since we are using this pre-study only for choosing a use case, the validity of our main evaluation (see Section 5) is not affected.

[2]https://www.destatis.de/EN/Themes/Society-Environment/Education-Research-Culture/Educational-Level/Tables/educational-attainment-population-germany.html

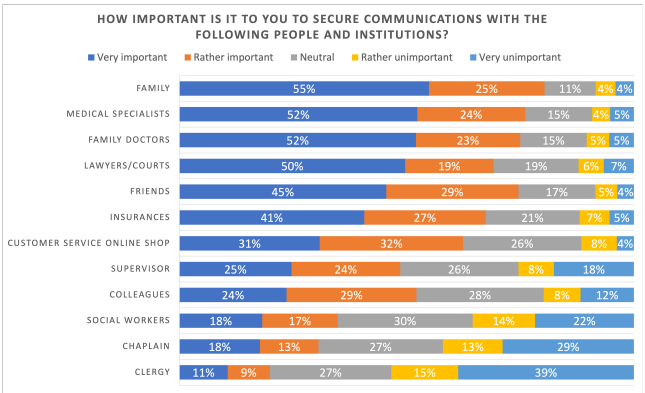

Figure 1: Results of the first item of our pre-study

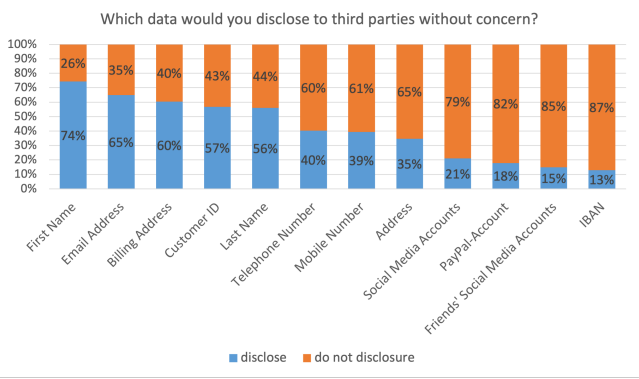

Figure 2: Results of the second item of our pre-study

3.2 Items and Results

To find out which communication is particularly sensitive for users, we posed the following questions in the survey:

3.2.1 Use Case. To find the most suitable use case for our concept, we designed the first item: "How important is it to you to have a secure line of communication with the following people and institutions?" The users could answer this question by rating the importance on a 5-Point-Likert-Scale ranging from very important to very unimportant. The following communication partners were surveyed: clergy, chaplains, social workers, colleagues, supervisors, customer service from online shops, insurance companies, friends, lawyers/courts, general practitioners, medical specialists, and family members. Not all of those are relevant for our use case, but it would be a bias to nudge the participants toward a desired result. Therefore, we include typical groups and persons that the participants are familiar with. For our use case, we will pick the highest-rated of the use cases that work for communication via an online form. The results for the first item can be seen in Figure 1.

The communication most worthy of protection is the communication with family members, followed by communication with medical specialists, family doctors, and lawyers. Also worthy of protection, but not as sensitive, is the communications with friends, insurance companies, and customer service from online shops. The

communication least worthy of protection is the one with supervisors, colleagues, social workers, chaplains, or the clergy. For our experimental form-based communication approach, it would have been difficult to build a demonstrator for communication with family and friends. Furthermore, it is unlikely that family members would communicate via an online form for matters of their daily life. Therefore, the remaining appropriate use cases were: medical specialists, general practitioners, and lawyers. Since we were planning to advertise our main study at the university, we chose general practitioners because it was to be expected that the participants attending our study would be most familiar with this use case.

3.2.2 Sensitive Data. To further investigate which type of data is most sensitive to users in communication with these actors, we designed the second item: "Which data would you disclose to third parties without concern?" The answers were "disclose" and "do not disclose" for the following data: First name, last name, address, email address, billing address, Customer ID (at customer support), telephone number, mobile number, IBAN, PayPal account, social media accounts, social media accounts of friends (advertise friends to get a bonus). The results are displayed in Figure 2.

4 THE D³ INTERACTION CONCEPT

As related work has shown, there are several approaches to enhance the confidentiality and security of C2B communication. In this paper, we focus on the approach of Fischlin [29] since it offers additional features such as deniability of usage. The sTeaLS protocol [29], as explained in the introduction, allows the generation of two keys in a single connection. One key is shared between the endpoints and the detection system, representing a regular TLS channel with full access for the detection system to the data. The other key, called the stealth key, is exclusively shared between the endpoints. The former key protects the so-called TLS channel, whereas the latter key secures the so-called stealth channel within the TLS channel via pre-encryption of the sensitive data. This two-key approach enables the user to decide which parts of the encrypted data should be shared exclusively with the receiver and which parts may be accessible by the detection system and potentially administrative personnel. This allows for an interesting new perspective: Instead of communication with a faceless organization, the communication is now directly related to another person inside the organization. The person receiving the message is not someone who randomly got assigned to the task but is addressed directly. We call our interaction concept "Decision-based Data Distribution (D³)". Note that outsiders do not have access to any transmitted data. The concept is illustrated in Figure 3.

The described approach is independent of the use case. However, our study will focus on one particular use case derived from the pre-study (see Section 3). Our design comprises an online form, a key wallet, and TLS connections for data transfer. After the initial contact via the online form, the correspondence is via email, in which the form structure is still represented. We assume that the 'final' implementation consists of an application similar to a mail client or an add-on for an existing mail client which contains the users' key wallet and has an authentication mechanism to identify the user in the decryption process. Furthermore, we assume that everything is implemented correctly and keys are stored securely. The receiving party provides an online form (e.g., on their website) with input fields for necessary information needed to fulfill a service. The users fill in the required information and define which information should be considered sensitive and, therefore, which information should be sent over the stealth channel. After submission, the structure and content of these forms are converted into a structured data format such as HTML, XML, JSON, or similar. Sensitive data, which is marked for stealth communication, is marked as 'secret' in the data structure. Furthermore, the sTeaLS protocol is initiated, and the TLS and stealth keys are computed. The sTeaLS key is added to the user's and recipient's key wallet. All 'secret' data is encrypted with the stealth key. After encryption, 'CONFIDENTIAL' is added to the result as a flag for regular TLS decryption. Additionally, if a 'secret' field is empty, it is filled with the string 'no input', which is then encrypted with the stealth key to provide indistinguishability if secret data was submitted or not. The transmission itself is similar to regular TLS. On the receiving side, the form is displayed, and if the viewer possesses the stealth key, the secret information is decrypted and displayed because the flag 'CONFIDENTIAL' is revealed in decryption. Otherwise, the message 'access denied' is shown in the secret sections of the form. An optional feature is the highlighting of the confidential content for the recipient. This serves two purposes: (1) the recipient is aware of which information should be treated with care to protect the sender, and (2) the recipient knows which content was not checked by the firewall and, therefore, should be treated carefully, since it may contain malicious links or other forms of social engineering. To utilize the full potential of the stealth channels, the recipient's response is also partially encrypted. Therefore, information that was considered sensitive by the initial sender and marked as confidential is not sent in plain text in the recipient's response. The partially encrypted mail ensures that the sensitive information is not leaked by unauthorized access to the sender's computer (e.g., by persons in the same household). Due to the form-based communication, the confidential fields can be hidden by default. The same mechanism that prevents other people on the receiver's side from viewing confidential data prevents users of the sender's computer from viewing it. To view the encrypted parts of the emails, the user has to be authorized by the client that hosts the key wallet. Then, the user can manually decrypt the confidential fields. The purpose of this is that sensitive information is never stored persistently on the computer and is only temporarily available to be displayed.

Please note that this concept relies on compliance by the involved parties, like most other security- and privacy-critical applications that involve human beings. Circumventing mechanisms or sharing credentials render those concepts useless. Therefore, we propose this concept for companies and individuals that want to provide increased privacy for their customers or clients. Especially for jobs that fall under the obligation to secrecy, like the medical confidentiality of doctors, the secrecy of confession for religious matters, or the professional discretion of lawyers.

5 QUALITATIVE EVALUATION

We built and evaluated demonstrators to gain user feedback on our interaction concept. The results are used to evaluate the practicability and to enhance our concept. A qualitative approach was chosen

to allow us to watch the participants interact with our demonstrators and gain first-hand impressions. Furthermore, the qualitative evaluation provided us with in-depth feedback and discussions of our concept.

5.1 Methodology

5.1.1 Participants. The participants were hired from the university environment. We advertised the study in lectures and via a mailing list for people interested in our user studies. We recruited 42 participants in total, 10 of whom identified as female and 32 as male. The participants' ages ranged from 17 to 42, with a median of 22.5 and a standard derivation of 4.61. Before conducting our study, we obtained ethical approval for our study from the ethics committee at our university. This ensures that we adhere to the university's ethical guidelines regarding study design, data storage, and processing. Accordingly, every participant signed an informed consent form describing the procedure of the study, the data storage, and processing. Every participant was compensated with €20 for participating in the study and informed that they could leave the study at any point without having to provide a reason. We removed the pseudonyms of the participants from results that cover sensitive use cases to enhance the anonymity of the participants.

5.1.2 Materials. We decided to use mock-ups for our study because they are lightweight to implement, easy to adjust, and are not dependent on an internet connection. As explained in our concept (see Section 4), we assume that technical preconditions are given since those are out of the scope of this paper (e.g., wallets to store keys). For our main purpose, the user study that investigates whether people perceive the benefits of partial encryption when communicating with doctors, it is not necessary to implement a mail client, a secure key storage, and an administrative software for a doctor's computer. We can simulate all of these using interactive mock-ups without creating dependencies and possible bugs that would interfere with our study. Therefore, we created interactive demonstrators using Axure[3], which offer the participants of our study the possibility to experience our concept from the sender's and recipient's view. We chose to build two different demonstrators because we wanted the users to choose themselves which information should be protected. However, literature highlights the control paradox: users tend to reveal more personal data when they have more control over it. To investigate this, we propose two different versions for our demonstrator (see Figure 4 and 5):

(1) One version has no option for partial encryption besides one single text area that is, by default, encrypted with the sTeaLS key. This is the baseline version for the control paradox since no customization is allowed. For brevity, we refer to this version as the **non-customizable version** (see Figure 4 in Appendix A.6).

Each demonstrator consists of three views: (a) the online form, (b) the doctor's view, and (c) the answer email. We decided to include all three views in the demonstrators to give the participants of our study an overview of the effects of the privacy features.

The first view consists of three parts: A part for the patients' information to identify them, an information text, and the message to the doctor. The first part comprises several input fields to fill in general information, like insurance ID, name, or address. Furthermore, the patients can choose which doctor they would like to send the form to. This is important since many medical offices are shared by multiple doctors. For our concept, it is necessary to specify which doctor is the recipient of the form in order to initiate the sTeaLs protocol with the corresponding doctor. The second part explains the functionality of the form to the users and the implications of the layered-encryption. We chose not to place this text at the top but over the part that it is relevant for. This choice was made due to the design principle of proximity. The third part consists of the two text areas that define which information is considered sensitive and will be encrypted using the sTeaLS key and which information is transmitted via regular TLS. The only choice that is available in this version is the choice of which information is put in which text area. This is the control group to investigate the control paradox.

The second view is designed for the doctor: The structure is the same as the online form, but the first part with the patient's information is not editable and the second text area is highlighted in red as a warning for the doctor. This serves two reasons: first, the doctor is reminded that the data contained in this text area is meant to be treated with care since it is considered sensitive by the patient. Secondly, due to the additional encryption, the firewall does not scan the content. In our scenario, we assume that cross-site scripting is prevented by technical means, but there remains the risk that social engineering, such as phishing, is used by a malicious user. The red highlighting should alert the doctors to be careful when interacting with this data (e.g., clicking on links in this text area). Additionally, a warning text is displayed over the text area: 'Content not checked. Handle with care'. A possible phishing attack could be the following text: 'I got injured and took a photo of the wound. I attached the picture with the following link <URL>. Please tell me if I should go to the hospital with it.'

The third view resembles the answer email from the doctor to the patient. It also resembles the structure of the online form but without the information text. Furthermore, the partial encryption feature is simulated: the second text area is hidden behind a button with 'Decrypt and show', which is hidden when clicked. This simulated the following aspect of the concept: The second text area (containing the sensitive data) is removed from the email if the user is not logged in to the key wallet. If the user is authenticated, a 'decrypt and show' button is displayed instead of the text area. If the user clicks on it, the sensitive data is decrypted temporarily and displayed. This feature ensures that the data marked as sensitive is never stored in plain text on the patient's computer.

Although this demonstrator is just a mock-up, we implemented some quality-of-life features: The input fields of the three views are interconnected so that the user's inputs are also put in the corresponding input fields of the other views. In the case of the second view, the doctor's answers were updated only in the third view (answer email) and not in the first view (online form). Furthermore, to increase accessibility, users can use the Tab-key to switch between the input fields in the correct order.

(2) The second version allows the users to specify which part of the form should be sent via the stealth channel. Each input field has a corresponding checkbox that marks this field as confidential. Therefore, the users can fully customize their level of protection.

[3] https://www.axure.com/

This is the experimental version since it comes back to the problem of our research gap: Which trade-off between confidentiality and usability (possibility of keyword search) do users make? This version is referred to as the **customizable version** (see Figure 5).

The customizable version is quite similar to the non-customizable version, but does not have the second text area for the sensitive information. Instead, each input field has a corresponding check box to mark it as sensitive. The information text is at the top to introduce the privacy mechanism first and explain the implications of layered encryption. For further convenience, we added an option to receive the requested receipt or referral letter via mail. Other quality-of-life features were a mark-all option for the check-boxes, and we simulated an adaptive form by making it responsive based on the choice of the users' request. In the doctor's view, all input fields marked as sensitive are highlighted in red. Furthermore, an information text indicates that the highlighted information was not checked by the firewall. The third view resembles the answer email. Similar to the non-customizable version, the input fields marked as sensitive are not visible if the user is not authenticated. Our demonstrator covers the case that the user is authenticated and hides the sensitive (encrypted) information behind a button ('decrypt and show'). After clicking it, the button becomes invisible, simulating the process of temporarily decrypting the data and rendering it into the form. Because of the limited space in the input fields for the house number and postcode, the button just states 'show'.

In both versions, we did not make any required fields since we wanted all data to be considered equally and avoid suggestive biases. This way, we can examine which data is considered sensitive by the participants of our study. During the interviews, we used questionnaires on a self-hosted instance of LimeSurvey[4] to get demographic information and some quantitative feedback. In order to test the usability of the demonstrators, we used the short version of the user experience questionnaire (UEQ-S)[5] for both demonstrators.

5.1.3 Procedure. Each session consisted of several parts which were completed by a single participant in about 30 to 50 minutes. The interview guideline can be found in the Appendix A.3.

First, we had a briefing, and the participant signed the informed consent form. The form was sent to the participants prior to the study in order to allow them to read it without the context of the study setting, which would make it harder for them to refuse participation. After studying the hard copy of the informed consent form and signing it, the first questionnaire was filled out to collect demographic information about the participants, investigating their privacy knowledge using the Online Privacy Literacy Scale (OPLIS)[6]. Since OPLIS provides a norm table for the whole population, we decided to classify the participants into three groups, i.e., low, medium, and high privacy literacy. The thresholds were set to divide the population so that each group represents around a third of the demographic spectrum, according to OPLIS. In our sample, seven participants were classified as having low privacy literacy, 13 as having medium privacy literacy, and 22 were classified as having high privacy literacy. This means that we have a bias towards users with a higher privacy literacy. Nevertheless, as described in section 5.3, privacy literacy does not have an impact on the version of our demonstrator which is preferred by the participants. Additionally, we included the items from the quantitative study for comparison.

The second part of the study was the hands-on experiment. Since we had two demonstrators, this part consisted of two rounds: We alternated the order in which the participants encountered the two versions with each session to avoid sequence effects: Participants with an odd participant-number (P1, P3, P5, etc.) encountered the non-customizable version first and the customizable version in the second round. Participants with an even participant-number (P2, P4, P6, etc.) encountered the customizable version first and the non-customizable-version second. Every participant was asked to interact with both demonstrators and fill them out in a way that would make sense to them. This means that the participants were not required to fill out the form using their data, such as their real addresses, but fill in data that was plausible to them in such a scenario since we were investigating the three different views for each demonstrator and the data should be recognized in the other views. The scenario was to order a receipt for medicine or a letter of referral to another doctor via the online form. After filling out the forms and checking the views for the doctor and the response email, the UEQ-S questionnaire was filled out, and the process was repeated for the other demonstrator.

After finishing the tasks with the demonstrators, the participants filled out a questionnaire which compared both versions. The participants had to choose which version they preferred and explain their choice in a few words. Furthermore, users should rate whether they would use such a tool in real life on a 5-point-Likert-scale (Would definitively use - Would definitively not use). During the evaluation, we used the Think-Aloud-Method [56] and recorded the audio.

As a final part, we had a discussion with the participants. For this, we prepared guiding questions which can be found in the Appendix A.3, investigating aspects they (dis-)liked and reflecting on their behavior during the experiment.

5.2 Data Analysis

In our data analysis, we followed the first six steps of the model of Olson et al. [57] for applying the Constant Comparative Method (CCM), a special form of grounded theory. The authors claim that their improved model increases the credibility of CCM. Furthermore, we chose this method because it allows for iterative development. The audio data was transcribed, and the questionnaires were converted into tables. After the (1) initial sighting of the material, interesting quotes and important topics were gathered and clustered. Based on this, (2) a codebook was developed, which can be found in Appendix A.8. Utilizing this codebook, two researchers analyzed the material independently (3), marking which participant contributed to which code. One researcher listened to the audio recordings and analyzed the open questions from the questionnaire, comparing both demonstrators, while the other read transcripts of the audio recordings. Comparing the coding (4) showed that for 40% of the codes, the coders had identical results; for the other 60% of the codes, the error rate varied between eight and 82% (mean: 18%), indicating that participants brought up further topics in the questionnaire. Afterward, inconsistencies were discussed (5), specifying the code book's criteria for applying codes (6). Analyzing the

[4]https://www.limesurvey.org/
[5]https://www.ueq-online.org/
[6]https://oplis.de/index_eng.html

coded data, we found that after participant P34, no new topics were brought up, and we assumed that saturation had been reached [15]. The analysis was done in German since most interviews were conducted in German (one participant preferred to answer in English). The finished results and the quotes for the result section were then translated into English as literally as possible. Afterward, some phrases were polished during proofreading to avoid confusion.

5.3 Results

5.3.1 Preferred Version. After the participants tried both versions of the demonstrator, they were asked which version they preferred. 31 participants stated that they preferred the customizable version, and 11 preferred the non-customizable version. Since we alternated the versions so that one-half of the participants started with the customizable version and the other half started with the non-customizable version, we examined whether a sequence effect occurred. We can deny this because 71.43% of those who started with the customizable version liked it most (15 of 21), and 76.19% of those who started with the non-customizable version also liked the customizable version most (16 of 21). We also examined whether privacy literacy influenced the participants' preferences. We can also deny this bias: Of the participants with low privacy literacy, 71% preferred the customizable version; of the participants with medium privacy literacy, 69% preferred the customizable version; and of the participants with high privacy literacy, 77% preferred the customizable version.

The participants stated a variety of reasons why they preferred one version over the other: One participant who preferred the non-customizable version stated, that it could confuse the user to decide for every input field whether it should be only visible for the doctor, which leads to an overhead that costs the user more time (P33). P22 stated that the customizable version could lead to miscommunication. This is a concern which was shared by P27, who stated the possibility to 'miss-click': "The checkboxes are intuitive, but you could confuse the rows and check the wrong box." Furthermore, the non-customizable version would provide a more strict separation between the sensitive and the non-sensitive data. This was also pointed out by P11: "You notice that the fields are clearly separated. This gives me the feeling that it is secure. For people who are not familiar with technology such a feeling could be more important than the technology itself." The possibility of usage errors was pointed out by P8, who preferred the non-customizable version because it was "easy to use", a sentiment that was shared by four other participants (P13, P17, P28, and P30). Additionally, P31 stated that the customizable version would be inefficient: "It is inconvenient that you have to click every single thing". P17 further stated that the information that could be marked sensitive in the customizable version would be relevant for other staff members and not only for the doctor. This was a point of criticism that other participants shared.P2 pointed out that the personal information was needed to identify them more easily, and the only relevant information worth protecting would be the reason why the patient needed the doctor's help. The non-customizable version would offer the possibility to do so. P3 argued similarly that staff members need information such as the address to support the doctor efficiently. If everything could be hidden from them, efficiency would suffer. Furthermore, independently of their preference, P11, P14, P19, P21, P24, P25, and P28 pointed out that hiding data from staff members would lead to administrative problems. The efficiency of the work processes was also a concern for those who preferred the customizable version, which affected their choice during the interaction with the demonstrators (see Section 5.3.3).

The participants who preferred the customizable version did so because of usability, perceived security, and the ability to customize and control their interaction with the doctor. For example, P20 described the customizable version as "easy and clear. The ability to select single elements works fast and is intuitive". P20 continued with the complaint that the two different text areas were cumbersome since the user had to write two texts and was prone to reveal information without intending to do so if the concept was misunderstood. That the two inputs from the non-customizable version are cumbersome was shared by P5, P9, and P38, who described the customizable version as less "redundant". P21 proposed an approach with two text areas for the patient's message but for another use case: The form should provide the possibility to write a message to the doctor and a second one to the other staff to enhance the performance for each request. P14 reported that the customizable version had better usability. P14 praised the better guidance of the user and that it was intuitive, which information was considered sensitive, a fact that was also brought up by P37. P42 added that the fact that the checkboxes allowed a decision close to the corresponding information was a great benefit. The ability to protect all personal data was important to P40 and P29, who stated an increased feeling of security. P13 added: "It's all health information, it's all sensitive in some way." P26 had the impression that it was less likely to unintentionally reveal data in the customizable version compared to the non-customizable version due to the fine-granular customization. P36 added that this ability to encrypt everything enhances the feeling of privacy. Overall, empowering users to decide the level of protection for their data was the most important factor as to why participants preferred the customizable version. In particular, P6 had the feeling of having more freedom to choose over his data and further stated that "all data that I do not encrypt, I chose not to encrypt". This was confirmed by P15, stating, "You can decide yourself which data should be protected". P18 also favored this choice: "I think I like the [customizable version], because at least there I had a choice which information I want to share". This self-controlled disclosure of data was also perceived as part of sovereignty over one's data. P24 expressed a similar aspect: By being able to customize the visibility of her data she can match her personal preference of what is considered sensitive. This was confirmed by P41, who stated that "the decision is taken away" from her in the non-customizable version. The trade-off between privacy and usability was brought up by P19: "In this [customizable version] I have more options to define what should be treated confidentially. This leads to a slight overhead (just some clicks), which is not a hindrance for me."

5.3.2 Usability of the Demonstrators. We used the UEQ-S to evaluate the usability of our two demonstrators. With this measure, we wanted to verify that lacking usability had no influence on our qualitative results. The usability scores in Table 5 attest to excellent usability according to UEQ-S (values higher than 4.5) and show

that the demonstrators were designed well enough not to pose a bias to the investigation of the privacy paradox. This is supported by statements from the participants as well: For example, P18 said: "I think I like the [customizable version] because at least there I had a choice which information I want to share. Other than that, I think both are almost the same". In general, the feedback of the participants focused on the two different options to apply layered encryption and protect their data. This may be due to the fact that we transparently communicated that the demonstrators were mock-ups or that the look and feel of the Axure assets emphasized that it is not ready to use. Feedback on the rest of the forms was limited to aspects like the wish for colored forms or a date picker to specify the date of birth. The latter was not included in the demonstrators because no such option was available in the mock-up tool.

5.3.3 Which data is considered sensitive? An overview of how the participants selected the data can be found in Table 1. Please note that 5 participants were removed from this overview because they stated that they did not set the check-boxes like they would in real life but randomly to see the effects on the other views. They still provided valuable feedback on the demonstrators and the use case, which is why they were only excluded from this analysis.

The information that was considered sensitive by most of the participants was the actual medicine or the type of doctor they wanted to be referred to. Interestingly, these were exactly those fields that correspond to the text areas in the non-customizable version. However, despite the seeming indifference between the two versions with this configuration, the participants preferred the sovereignty over their data in the customizable version (see 5.3.1). Some participants considered the town they live in as less sensitive than the street they live in since this information could be used more effectively to find them in real life. During the evaluation of the demonstrator, many participants stated that they suspected that some of their personal data would be necessary to process their request in the doctor's office. Therefore, many of them did not protect their personal information, fearing that their request might not be processed due to missing data. This is, in part, the fault of our design choices: We did not want to make 'required fields' in the form because we wanted to investigate which data is considered sensitive. Highlighting some of it as required would be a bias.

The choice of which data should be considered sensitive was also addressed in the discussion. For example, P12 reported that a female friend voiced her last name and date of birth in a medical office, which is a common practice at the registration desk. Someone who happened to be there too, was able to find her on social media with this little data. P12 was afraid that someone with more resources could do even more than that. Another concern was raised by P15: By disclosing personal data, it becomes more likely that someone could attempt identity theft to gain even more private data. P26 stated that he would provide more information (by not selecting the checkbox) if he knew which information was used for which purpose and therefore, could evaluate how he can support the processing of his request by revealing information without risking the negative effects of the disclosure. P34 was also concerned about the extra work for the staff: He would always encrypt the data because it would not make sense to him otherwise: If non-sensitive information is not encrypted, that means that all encrypted data is sensitive data, making the communication suspicious. He assumed that many people would use the encryption if available, creating more work for doctors, which could become a problem in Germany. This assumption is confirmed by P36 who stated that she would always encrypt every possible information if this did not increase the time for processing her request too much. Other participants also stated the trade-off between more disclosure and faster processing of their requests (P18, P32, P42). Another fear was revealed by P21 and P35: they were afraid that their request could not be processed properly due to missing data.

Another interesting aspect was brought up by P13, who stated that personal experience would highly impact the choice of protected data and that people who experienced negative consequences of lacking privacy would act more sensible in this regard. P14 also mentioned the connection between personal experience with privacy and behavior in relation to privacy: "A person who never bothered with data protection or their personal data might get incentivized [by the customization option] to think about what data should be protected. This might raise awareness in society".

For further insights into the consistency of privacy behavior, we correlated the answers from the questionnaire ("Which data would you disclose to third parties without concern?') to the choices in the demonstrator for the four items first name, last name, address, and insurance number (the latter correlated to the item "Customer ID"). We found that seven participants encrypted their first name despite claiming to disclose it ("over-encrypted"), and two participants did not encrypt it despite claiming not to disclose it in the questionnaire ("under-encrypted"), leading to a total discrepancy of 24%. Four participants "over-encrypted" and 14 "under-encrypted" their last name (discrepancy 48%). In the context of their address, one "over-encrypted" and 22 "under-encrypted" (discrepancy 62%). Finally, six participants "over-encrypted" and four "under-encrypted" their insurance numbers (discrepancy 27%). These discrepancies might result from the use case of our evaluation: In the pre-study, we did not provide a special context on purpose, but in the evaluation of the demonstrators the participants were confronted with the context of a medical office. We confirmed this by reviewing the audio recordings from the experiment: While filling out the forms, the participants did not only consider their personal preferences, but the workflow of a medical office. Therefore, they hesitated to encrypt information that they thought was necessary to identify them as a patient and to process the request (P19, P28, P35, P42). P6 considered the encryption as a measure to direct the data to different addressees: "Information such as addresses is not interesting for the doctor, but the assistants". Similarly, P2, P5, P21, P25, and P34 did not encrypt some of the data to minimize the effort for the doctor and the assistants. Not having all available information or forcing the doctors to do administrative tasks like sending a letter themselves was not deemed justifiable in that use case (P25. P28. P34). This explains the over- and under-encryption from our correlation: Last names are under-encrypted to identify the patient. In Germany, when entering a medical office, patients state their names and "verify" their identity by stating their date of birth. This is not a security feature but is intended to ensure that the correct patient data is used and that mistakes due to common names are avoided (e.g., identify the correct John Smith). The first names are not so essential for this process since the last name and birth date

Table 1: Protected fields in the customizable version (•) vs. the unprotected fields (empty).

Field	P1	P3	P5	P6	P7	P8	P9	P10	P12	P13	P14	P15	P16	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28	P29	P30	P31	P32	P34	P35	P36	P37	P38	P39	P40	P41	P42
Insurance Number	•						•								•	•	•			•	•	•	•				•		•		•		•				
Last Name	•						•		•			•				•						•					•		•		•						•
First Name	•						•		•			•				•	•					•					•		•		•		•		•	•	•
Street and House Number	•				•		•		•			•		•		•				•		•					•		•		•		•		•		•
Town and Postcode	•				•		•							•		•				•		•					•		•		•						•
Date of Birth	•				•		•		•					•		•	•		•			•					•		•		•		•			•	•
Type of Request	•			•		•	•			•	•		•		•		•			•		•	•				•	•		•	•						•
Receipt or Referral	•	•		•		•	•			•	•		•	•	•	•	•		•	•	•	•	•		•		•	•	•	•	•	•				•	•
Comment	•		•	•	•	•	•	•	•	•			•	•	•	•	•		•	•	•	•	•	•			•	•	•	•	•					•	•

are often sufficient for identification. Thus, the over-encryption can be explained. In some cases, the participants thought it would be sufficient to leave the insurance number unencrypted to identify them, resulting in under-encryption. The under-encryption of the addresses also originated from the use case: In order to send receipts, the staff members need to know the addresses. Therefore, many participants did not encrypt them on purpose to support the workflows of staff members.

5.3.4 Form-based Communication. In our study, we found that form-based communication is a promising approach. After the interaction with the demonstrators, the users were asked in the questionnaire if they would use such a form if it would be available in real life. The possible answer ranges were: 'definitely', 'likely yes', 'I don't know', 'likely no', 'definitely not'. Two participants voted for 'I don't know', while 13 voted for 'Likely yes' and 27 voted 'definitely'. Although this result may be affected by the acquiescence bias, we confirmed that the possibility of communicating via an online form was highly appreciated.

Reasons for that are not only our novel concept for partial encryption of sensitive data but also the ability to communicate with doctors more easily, reducing barriers to seeking help. The latter was confirmed by participants who stated that it was easier to formulate embarrassing or stigmatized topics in text than in a conversation in person or via telephone (e.g. P3, P5, and P27). Furthermore, P4, P12, P20, and P42 complained about the ability of bystanders to eavesdrop on telephone calls with the medical staff. In Germany, the calls are answered by staff at the registration desk, which makes it possible for other patients waiting in line to listen to the conversation. P20 stated: "It is uncomfortable when the staff talks loudly about you and others in the medical office can hear it. Even if it is nothing sensitive, like going to the dentist". In general, communication via telephone is perceived as cumbersome to some (P6, P13, P16, P31, P37) or even as reason for discomfort or fear to others (P4, P6, P10, P19, P20, P26, P30 P32). The more flexible way of communication via an online form was pointed out by twelve participants. Users do not have to wait (very long) for their calls to be answered or can send requests whenever they like without having to pay attention to the opening hours of the doctor's office, which is a major problem for people who have to work shifts that collide with those time slots. For example, P28 stated: "I am a student, and I am at the university all day. I can't go out and try calling the medical office a thousand times a day. An email or a form is easily done. Therefore, it makes a lot of sense [to use this way of communication]". Besides perceiving communication via telephone as cumbersome, eight participants mentioned telephone anxiety, which affected them or people they knew (P4, P6, P13, P16, P19, P20, P26, P30). On the other hand, some participants mentioned that they would still use the telephone for urgent cases (P9, P40).

5.3.5 Use Cases. We did not comment on the use cases mentioned by the participants or discuss whether they are hypothetical or based on their own experience since many of the use cases are very sensitive (e.g., depression or domestic violence), and we did not want to trigger traumas or embarrass the participants. Furthermore, we refrain from using the participant ID in this section to provide further anonymization. Instead, we will include just the number of participants who mentioned a certain topic for each topic.

We distinguished the use cases mentioned by the participants in two scenarios: First, we investigated for which use case participants consider it important that the answer email is partially encrypted so that people in their surroundings cannot see the data they marked as sensible, even in the case of "shoulder surfing":

One of the most mentioned reasons for this scenario was getting a severe or lethal diagnosis and trying to comprehend and process this information by themselves before anyone else finds out. Furthermore, the participants wanted to decide for themselves when (or whether) the diagnosis would be disclosed to others (12). One category in this section can be summarized as "housing situation": Participants reported many use cases where it is important to have strong privacy features at home. The reasons ranged from "mistrust at home" (4) over living in shared flats (8) to having a divorce but still living together (1). Four participants even mentioned domestic violence. Regarding the housing situation, participants mentioned the parent-child relationship: Three participants did not want to disclose the parents' diagnoses to their children to prevent them from worrying. On the other hand, children should be protected from parental surveillance (8). Furthermore, three participants mentioned the issue of females wanting to go to the gynecologist against their families' will. Another category is about intimate topics: Eleven participants stated intimate topics, in general, were confidential. Others were more precise and specifically addressed the topics of (unwanted) Pregnancy (6), abortions (3), or results from the urologist (6). Similarly, taboos or topics stigmatized by society were mentioned: Besides the general topic (13), the participants mentioned Sexual Transmittable Infections (STIs) (12), mental problems (e.g., depression) (9), drug abuse including alcohol (3), and help for suicidal people (1). Furthermore, the fear of discrimination was brought up: One participant said that any information that could prevent him from living his life as before if

it were to be leaked was worth protecting. Others reported more specific reasons for discrimination: LGBTQ topics (2) or (mental) disablement (1). Further use cases were the handling of legal documents (21) or communication with schools (3), as well as religious reasons (3). For example, women might not want to go to a male doctor due to religious beliefs, and professions like gynecology may be stigmatized by some beliefs.

Secondly, we investigated use cases for privacy towards other people in the doctor's office, achieved by the additional encryption: The reasons for privacy within the medical office are divided into two groups: The actual topic, why someone attends the medical office and social aspects. The topics that were considered most sensitive were intimate issues (8), mental problems (19), and embarrassing or stigmatized problems (17). The social aspects mostly cover the issue of rumors (3). For example, one participant stated that her grandfather did not want to go to the doctor because he feared potential rumors. Furthermore, having relatives or family members among the medical office's personnel was a concern for 19 participants. Eight participants also mentioned that living in a rural area is problematic: There are fewer doctors, and most people know each other, which makes it impossible to go to the doctor without anyone knowing it. A corresponding quote from a participant who lives in the city was: "If I know someone in the medical office and I do not trust them, I go to a different medical office".

On the other hand, participants explicitly stated that they have a general trust in medical staff (10). Reasons for this differed: Some personally trust the staff, others rely on the laws and regulations in Germany which enforce secrecy for medical data. Regarding their level of trust, some participants also differentiated between the doctor and the assistants. Furthermore, one participant even differentiated between the different staff members: She mentioned that at her gynecologist, there is always an assistant present. Therefore, she trusts those assistants for treatment more than those who are in charge of administrative tasks. A limitation of this system was mentioned by one participant who stated that frequently changing personnel among the staff would reduce trust.

5.4 Limitations

In our qualitative evaluation, we face the limitation that our sample consists of relatively young and well-educated participants. This makes our results less representative. To evaluate to which extent this bias affects our results, we compared our sample with the representative sample from the pre-study. For this reason, we included the questions from the quantitative survey in the questionnaires of our qualitative evaluation. By statistically assessing the difference between our qualitative sample and the representative sample, we can estimate to which degree the results can be generalized. We compared the following samples: **Sample A**: answers from the participants of our qualitative study (N=42); **Sample B1**: answers from the age group of 18-44 from the representative survey (N=378); **Sample C1**: answers from the representative survey that are not part of B1 (N=633); **Sample B2**: answers from the representative survey from the age group of 18-44 with a similar education level compared to sample A (N=222); **Sample C2**: answers from the representative survey that are not part of B2 (N=785). In samples B2 and C2, we exclude the answers of those who stated "other" when asked for their highest educational degree. We conducted a Mann-Whitney-U-Test to compare two samples at a time. For each item from each question we compared sample A to B1 and B2 in order to evaluate how the answers of our qualitative sample differ from the corresponding group in the representative sample. Additionally, we conducted the test for samples B1 vs. C1 and B2 vs. C2. This way, we could evaluate whether age (or age and educational level) had an impact on the answers to our questions. Furthermore, the sums of the answers were compared as well. This way, a Pearsons correlation efficient was determined as the effect size [30] and interpreted according to Cohen [17]. We specified p=.05 as the significance level ($|r| < 0.1$ = very weak; $0.1 < |r| < 0.3$ = weak; $0.3 < |r| < 0.5$ moderate; $|r| >= 0.5$ = strong). For the first question, all differences in the Mann-Whitney-U-Test were weak, very weak, or insignificant, with one exception: the difference between sample A and B2 was moderate for the item ''chaplain".

Furthermore, all effect sizes were negative, which means that A-samples indicated a higher importance than B-samples, which in turn indicated a higher importance than C-samples (higher because in the Rep study '1' stood for "very important" and '5' for "very unimportant"). For the second question, all differences were weak, very weak, or insignificant. Again, all (significant) effects were negative, which means that A-samples were more willing to share data than B-samples, which in turn were more willing than C-samples. However, if we sum up the answers to the questions on sharing data, we see that there is a moderate effect, which means that the A-sample was more willing to share data than the B-sample. To provide full transparency, we added a detailed table for all items in Appendix A.1. To summarize, we have limitations regarding the age and the education of the participants in the qualitative sample, but the differences do not render our qualitative results useless.

Another limitation is that some of our findings are not exclusively related to our concept. For example, providing an alternative to the telephone for communication with doctors can be achieved without the additional protection features. However, those findings are relevant for our paper since we propose a concept that increases privacy and security without the need for a trade-off. Therefore, the additional findings provide insights necessary for potential adoption into practice. Further limitations are the qualitative nature of our evaluation and the focus on the German population. Studies in different countries may yield different results (see Section 6.4).

6 DISCUSSION AND CONCLUSION

In this paper, we were able to shed the first light on our interaction concept D³. In the following, we will discuss topics that were brought up during the investigation of suitable use cases and evaluate our concept with the first iteration of demonstrators.

6.1 Evaluating the Control Paradox

In our study, we found that the majority of our participants preferred the customizable version. Since this was independent of the sequence they encountered the demonstrators and the privacy literacy of the participants, we conclude that the ability to customize their own privacy is important to users, confirming these claims in the literature [19]. Some participants reported personal experiences with negative consequences of data leakage and were eager

to encrypt all data, while others, who did not perceive the necessity of encrypting personal data still liked the possibility of doing so. Besides the fact that many customized the level of protection similar to the level of protection of the non-customizable version, the circumstances were different: The unprotected data is the same for both versions, but one version forces the disclosure of data to staff members and the other leaves the decision to the patient.

On the other hand, the statistical comparison to the representative sample showed that besides no significant difference in the answers of the questionnaire items, there was a tendency to disclose more data among our qualitative sample while claiming a higher importance of protection. This may be due to the sample size or a confirmation of the control paradox stated by Brandimarte et al. [13] and Boer et al. [9]. We can rule out the influence of the demonstrator design because the questions used for comparison were answered before the interaction with the demonstrators. In summary, the qualitative sample answered the questionnaire items similar to the representative sample, with a slight tendency to rate the protection of communication higher (item 1: "How important is it to you to secure communications with the following people and institutions?") and a slight tendency to protect less data assets (item 2: "Which data would you disclose to third parties without concern?"). Therefore, we can assume that the settings of the checkboxes would be similar for a larger sample. Considering the non-significant derivation, a more representative sample would possibly check some boxes more.

One of our participants gave a possible explanation for the control paradox: By granting the users the freedom to choose the level of protection they want, the disclosed data is voluntarily given away. Denying the users this choice makes them feel like the data is taken against their will, which results in the feeling that the company is the adversary. Withholding as much information as possible from them is like fighting back. This could be an explanation of the control paradox: If users have the power to decide, they can evaluate, based on individual information, whether it may be disclosed or not, which could result in them revealing more data due to a better feeling. However, if they are forced to give away data, they will try to withhold as much as possible.

6.2 Practical Relevance

In our study, we found several implications for the real-world adoption of our interaction concept. First, we confirmed that one barrier would be the potential increase in workload for doctors. This was the reason why we designed the concept to be voluntary. Forcing someone to use it who will circumvent the purpose of it due to lacking capacities would be fatal. Therefore, we recommend our system for doctors who have the capacity for an additional workload or those who wish to address a broader field of patients. Another target group for our concept are counseling agencies for sensitive use cases. Our participants reported some very critical use cases where it is crucial that patients can communicate securely and secretly. Examples of this are use cases in which people face repression from their surroundings, such as religious reasons, repressive families, or even domestic violence. Social workers who provide support in these situations could benefit from our system since it is suitable for covered communication due to the use of the sTeaLS protocol. Due to the fact that it is not distinguishable from the outside if a regular TLS handshake was conducted or the sTeaLS protocol was used, it is deniable that the second key exists. Therefore, steganographic methods can be applied to deny that a second key ever existed to adversaries who can monitor the network traffic.

Introducing our concept to the public would confront those people who are not concerned about privacy with a potentially undesired mechanism. However, our concept benefits all users, not only those who value privacy. For example, the use of form-based communication was perceived as a major improvement to the current situation. Due to lacking digitalization, the telephone is the only viable option for many patients. This perception of lacking digitalization is not limited to our sample, as a recent investigation shows [73]. The preference for the use of online forms was stated by many participants of our study. We presented research in the related work section that emphasizes the role of trade-offs between security and usability [1, 14, 45]. However, with our interaction concept D^3, we propose a solution that increases security while being more usable than the current status quo. This way, we tackle the challenge of the trade-off between confidentiality and usability by improving the usability of communication with doctors compared to the current situation while adding the option for additional encryption. Therefore, we do not need compromises but offer better usability with better confidentiality. Based on the enthusiasm of the participants for real-world adoption of our concept, we are confident that this technology can improve the lives of many people, especially of those who perceive the current best practice as a hindrance to getting help. By providing online forms as an alternative, people who cannot use the telephone due to their physical condition, time constraints, or telephone anxiety can easily contact a medical office while being able to customize the level of confidentiality. Therefore, benefits are provided even for those who do not value privacy-preserving communication.

6.3 Impact on the Iterative Design of the Interaction Concept

The qualitative study was the first step in the evaluation of our concept. Valuable feedback from the participants will be used to enhance the interaction concept even further. Many participants mentioned that they did not know which information was necessary for the rest of the staff to process the request. In the study setting, we abstained from using 'required fields' to avoid a bias in the selection of 'sensitive data' by the participants. In a real-world scenario, each medical office or company that would use our concept would have individual forms for their services suited for their work processes.

'Express forms' could be offered to address the concern of some participants that the partially encrypted data would lead to slower processing because only the doctors can see and process the data. By clearly informing the patient that those forms do not provide the partial encryption feature, the patients can decide whether faster processing is worth disclosing their data.

6.4 Transferability of Results

Our research focused on the German population. To evaluate whether our results are applicable to other countries, we investigated existing literature: Firstly, in studies comparing multiple countries,

Germany belongs to the countries with higher privacy and security concerns. Herbert et al. [37] investigate the misconceptions regarding security and privacy topics (12,351 participants in 12 countries: China, Germany, Great Britain, India, Israel, Italy, Mexico, Poland, Saudi Arabia, Sweden, the USA, and South Africa). In their survey, they found differences regarding security and privacy misconceptions between Western and non-Western countries. Germany, therefore, differs from non-Western countries but is similar to other Western countries. Prince et al. [60] investigate the level of privacy concerns of different European countries by surveying online privacy literacy. Using the Eurostat 443 dataset (n=26,526; 28 countries), they investigated the privacy concerns regarding access to their data, monitoring, and confidentiality. Compared to the reference country France, Germany belonged to the group of countries with higher privacy concerns (Ireland, United Kingdom, Denmark, Malta). On the contrary, there was also a group with fewer privacy concerns: Cyprus, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Slovakia, Bulgaria, and Croatia. Harbach et al. [36] investigated the smartphone locking behavior in eight countries (n = 8,286): Australia, Canada, Germany, Italy, Japan, Netherlands, United Kingdom, and the United States. The authors found that data protection was rated higher in Germany and Japan than in the US sample. Utz et al. [78] investigated the acceptance of contact tracing apps during the Covid-19 pandemic in Germany, USA, and China. The German and the US sample were hesitant towards contract tracing, while the Chinese sample was fonder of this concept. The authors assume that the familiarity with similar systems in China reduced the barriers for adoption. On the contrary, the German and US participants had greater concerns regarding governmental surveillance. Secondly, we looked into studies that make a direct comparison between Germany and another country: Ilhan and Fietkiewicz [39] investigate the difference between German and US users regarding their knowledge and behavior towards activity tracking. Surprisingly, the US sample was more likely to deactivate accounts or request the deletion of data than the German sample, although the German sample knew more often about the possibility of deleting the data. Further analysis showed that US users were more likely to inform themselves about the company, their reputations, and the Terms of Service, while the German sample was more likely to read the Data Privacy Policy. However, both samples had a similar rating of data sensitivity and concerns about data misuse. Pleger et al. [59] conducted a media analysis and survey with 1000 participants from Germany and the UK (500 from each country). While both populations state the importance of data protection and data security as well as have similar trust in the government, the UK citizens had a greater concern about disclosing personal data on the internet than the Germans (7.34 out of 10 vs. 7.09 out of 10). Similarly, the concerns for 'fraudulent use of data', 'data theft', 'identity theft', and 'electronic manipulations of elections' were slightly higher in the UK compared to Germany.

Non-Western societies, in particular, are different in their perception of security and privacy topics. On the other hand, Germany was relatively comparable to the UK and the US. Besides some differences of opinion on certain topics, all three countries are among those who value privacy and security highly. Another finding from the literature is the role of the state in the perception of societies. Reuter et al. [65] show that Germans trust the state and hold it responsible for emergency management, while this perception differs in other European countries. Therefore, the findings from our study are relevant to other countries as well. Nevertheless, before adopting our proposed interaction concept in other countries, further regional research is recommended.

6.5 Future Work

With this study, we confirmed that our interaction concept can address relevant use cases and provide benefits for civilians. After discovering several use cases (see section 5.3.5), a possible next step would be to conduct expert interviews with professions that are affected by these use cases and could benefit from our system. Furthermore, to allow easy adoption into practice, a form generator should be implemented to allow for an easy design of individual forms for each use case. Additionally, the backend implementation to host those forms should be made public (e.g. open source).

6.6 Conclusion

In this paper, we presented and evaluated an interaction concept to bring state-of-the-art cryptography into usage in everyday scenarios. By utilizing the sTeaLS protocol [29], users are provided with the possibility to add an additional layer of encryption for their data, which also provides protection from middleboxes. In this paper, we propose an interaction concept (D³) that utilizes this protocol for communication with specific recipients within a business or an organization, leaving the decision to the users which part of the message is additionally encrypted. To find the most relevant use cases for this partially-accessible encryption, we conducted a quantitative survey with 1011 participants representative of the German population for the criteria of age, gender, education, and income. After identifying the interaction with doctors as the most suitable use case, we investigated whether new privacy solutions for this use case are appreciated by end users, and further development in this area should be continued by conducting a qualitative evaluation with 42 participants. Enabling users to decide over their data by themselves and its protection is prone to the privacy paradox: The tendency to disclose more data if more control over it is granted. To investigate this, we decided to utilize two demonstrators. One with no customization features that offer a basic functionality and a version that allows a full customization of which part of the message is additionally encrypted. The results of our study show that the possibility of partial encryption is highly appreciated and could be beneficial for several critical use cases. One major theme among the participants was the sovereignty over their data. Even if they disclosed a lot of information, they appreciated that this was their own choice. This led to a preference for the customizable version over the non-customizable version in our study. Furthermore, besides the ability to utilize layered encryption, the possibility to communicate with doctors via an online form was perceived as an improvement to the current situation in Germany, where the telephone is often the only way to communicate with medical offices. Therefore, the proposed concept would reduce physical and social barriers to seeking help and combat the trade-off between confidentiality and usability by providing a custom level of protection while also offering better usability.

ACKNOWLEDGMENTS

This research work has been funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – SFB 1119 (CROSSING) – 236615297 and by the German Federal Ministry of Education and Research and the Hessian Ministry of Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

REFERENCES

[1] Suliman A. Alsuhibany. A proposed approach for handling the tradeoff between security, usability, and cost. In *2019 International Conference on Computer and Information Sciences (ICCIS)*, pages 1–6, 2019. doi: 10.1109/ICCISci.2019.8716447.

[2] Nampoina Andriamilanto and Tristan Allard. Brfast: A tool to select browser fingerprinting attributes for web authentication according to a usability-security trade-off. In *Companion Proceedings of the Web Conference 2021*, WWW '21, page 701–704, New York, NY, USA, 2021. Association for Computing Machinery. ISBN 9781450383134. doi: 10.1145/3442442.3458610. URL https://doi.org/10.1145/3442442.3458610.

[3] Gilad Asharov, Gil Segev, and Ido Shahaf. Tight tradeoffs in searchable symmetric encryption. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology – CRYPTO 2018*, pages 407–436, Cham, 2018. Springer International Publishing. ISBN 978-3-319-96884-1.

[4] Léonard Assouline and Brice Minaud. Weighted oblivious ram, with applications to searchable symmetric encryption. In *Advances in Cryptology – EUROCRYPT 2023: 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part I*, page 426–455, Berlin, Heidelberg, 2023. Springer-Verlag. ISBN 978-3-031-30544-3. doi: 10.1007/978-3-031-30545-0_15. URL https://doi.org/10.1007/978-3-031-30545-0_15.

[5] Giuseppe Ateniese, Daniel H. Chou, Breno de Medeiros, and Gene Tsudik. Sanitizable signatures. In Sabrina de Capitani di Vimercati, Paul Syverson, and Dieter Gollmann, editors, *Computer Security – ESORICS 2005*, pages 159–177, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg. ISBN 978-3-540-31981-8.

[6] Haleh Ayatollahi, PA Bath, and S Goodacre. Accessibility versus confidentiality of information in the emergency department. *Emergency Medicine Journal*, 26 (12):857–860, 2009.

[7] Wei Bai, Doowon Kim, Moses Namara, Yichen Qian, Patrick Gage Kelley, and Michelle L. Mazurek. Balancing security and usability in encrypted email. *IEEE Internet Computing*, 21(3):30–38, 2017. doi: 10.1109/MIC.2017.57.

[8] Noam Ben-Asher, Joachim Meyer, Yisrael Parmet, Sebastian Moeller, and Roman Englert. An experimental microworld for evaluating the tradeoffs between usability and security. In *Symposium on Usable Privacy and Security (SOUPS)*, 2010.

[9] Ivana De Boer, Eelco Herder, and Marc Van Lieshoud. The illusion of control in privacy trade-offs: Does familiarity play a role? In *Adjunct Proceedings of the 29th ACM Conference on User Modeling, Adaptation and Personalization*, pages 338–344. Association for Computing Machinery, Inc, 6 2021. ISBN 9781450383677. doi: 10.1145/3450614.3464471.

[10] Glencora Borradaile, Kelsy Kretschmer, Michele Gretes, and Alexandria LeClerc. The motivated can encrypt (even with pgp). *Proceedings on Privacy Enhancing Technologies*, 2021:49–69, 7 2021. doi: 10.2478/popets-2021-0037.

[11] Angèle Bossuat, Raphael Bost, Pierre-Alain Fouque, Brice Minaud, and Michael Reichle. Sse and ssd: Page-efficient searchable symmetric encryption. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – CRYPTO 2021*, pages 157–184, Cham, 2021. Springer International Publishing. ISBN 978-3-030-84252-9.

[12] Raphaël Bost, Brice Minaud, and Olga Ohrimenko. Forward and backward private searchable encryption from constrained cryptographic primitives. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, page 1465–1482, New York, NY, USA, 2017. Association for Computing Machinery. ISBN 9781450349468. doi: 10.1145/3133956.3133980. URL https://doi.org/10.1145/3133956.3133980.

[13] Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. Misplaced confidences: Privacy and the control paradox. *Social psychological and personality science*, 4(3):340–347, 2013.

[14] Christina Braz, Ahmed Seffah, and David M'Raihi. Designing a trade-off between usability and security: A metrics based-model. In Cécilia Baranauskas, Philippe Palanque, Julio Abascal, and Simone Diniz Junqueira Barbosa, editors, *Human-Computer Interaction – INTERACT 2007*, pages 114–126, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg. ISBN 978-3-540-74800-7.

[15] Kelly Caine. Local standards for sample size at chi. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, page 981–992, New York, NY, USA, 2016. Association for Computing Machinery. ISBN 9781450333627. doi: 10.1145/2858036.2858498. URL https://doi.org/10.1145/2858036.2858498.

[16] Yao-Hsin Chou, Fang-Jhu Lin, and Guo-Jyun Zeng. An efficient novel online shopping mechanism based on quantum communication. *Electronic Commerce Research*, 14:349–367, 12 2014. ISSN 15729362. doi: 10.1007/s10660-014-9143-6.

[17] Jacob Cohen. *Statistical power analysis for the behavioral sciences*. 1988. ISBN 9780203771587. doi: 0.4324/9780203771587.

[18] Jessica Colnago, Lorrie Cranor, and Alessandro Acquisti. Is there a reverse privacy paradox? an exploratory analysis of gaps between privacy perspectives and privacy-seeking behaviors. *Proceedings on Privacy Enhancing Technologies*, 2023:455–476, 1 2023. doi: 10.56553/popets-2023-0027.

[19] Mary J Culnan. " how did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use. *MIS quarterly*, pages 341–363, 1993.

[20] Ivan Damgård, Helene Haagh, and Claudio Orlandi. Access control encryption: Enforcing information flow with cryptography. In Martin Hirt and Adam Smith, editors, *Theory of Cryptography*, pages 547–576, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg. ISBN 978-3-662-53644-5.

[21] Xavier de Carné de Carnavalet and Mohammad Mannan. Killed by proxy: Analyzing client-end TLS interception software. In *NDSS*. The Internet Society, 2016.

[22] Xavier de Carné de Carnavalet and Paul C. van Oorschot. A survey and analysis of TLS interception mechanisms and motivations. *CoRR*, abs/2010.16388, 2020. URL https://arxiv.org/abs/2010.16388.

[23] Xavier de Carné de Carnavalet and Mohammad Mannan. Killed by proxy: Analyzing client-end tls interception software. In *Network and Distributed System Security Symposium*. Internet Society, 5 2017. doi: 10.14722/ndss.2016.23374.

[24] Marcela T. de Oliveira, Lucio H. A. Reis, Ricardo C. Carrano, Flavio L. Seixas, Debora C. M. Saade, Celio V. Albuquerque, Natalia C. Fernandes, Silvia D. Olabarriaga, Dianne S. V. Medeiros, and Diogo M. F. Mattos. Towards a blockchain-based secure electronic medical record for healthcare applications. In *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, pages 1–6, 2019. doi: 10.1109/ICC.2019.8761307.

[25] Ioannis Demertzis, Dimitrios Papadopoulos, and Charalampos Papamanthou. Searchable encryption with optimal locality: Achieving sublogarithmic read efficiency. In *Advances in Cryptology – CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part I*, page 371–406, Berlin, Heidelberg, 2018. Springer-Verlag. ISBN 978-3-319-96883-4. doi: 10.1007/978-3-319-96884-1_13. URL https://doi.org/10.1007/978-3-319-96884-1_13.

[26] Roger Dingledine, Nick Mathewson, and Paul F. Syverson. Tor: The second-generation onion router. In *USENIX Security Symposium*, pages 303–320. USENIX, 2004.

[27] George T Duncan, Thomas B Jabine, and Virginia A de Wolf. *Private lives and public policies: Confidentiality and accessibility of government statistics*. National Academy Press, 1993.

[28] Victoria Fehr and Marc Fischlin. Sanitizable signcryption: Sanitization over encrypted data (full version). *IACR Cryptol. ePrint Arch.*, 2015:765, 2015. URL https://api.semanticscholar.org/CorpusID:16085003.

[29] Marc Fischlin. Stealth key exchange and confined access to the record protocol data in tls 1.3. Cryptology ePrint Archive, Paper 2023/651, 2023. URL https://eprint.iacr.org/2023/651. to appear at CCS 2023.

[30] Catherine Fritz, Peter Morris, and Jennifer Richler. Effect size estimates: Current use, calculations, and interpretation. *Journal of experimental psychology. General*, 141:2–18, 08 2011. doi: 10.1037/a0024338.

[31] Georg Fuchsbauer, Romain Gay, Lucas Kowalczyk, and Claudio Orlandi. Access control encryption for equality, comparison, and more. In Serge Fehr, editor, *Public-Key Cryptography – PKC 2017*, pages 88–118, Berlin, Heidelberg, 2017. Springer Berlin Heidelberg. ISBN 978-3-662-54388-7.

[32] Nina Gerber, Benjamin Berens, and Melanie Volkamer. Investigating people's privacy risk perception. *Proceedings on Privacy Enhancing Technologies*, 2019: 267–288, 07 2019. doi: 10.2478/popets-2019-0047.

[33] Javad Ghareh Chamani, Dimitrios Papadopoulos, Charalampos Papamanthou, and Rasool Jalili. New constructions for forward and backward private symmetric searchable encryption. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, page 1038–1055, New York, NY, USA, 2018. Association for Computing Machinery. ISBN 9781450356930. doi: 10.1145/3243734.3243833. URL https://doi.org/10.1145/3243734.3243833.

[34] Matthew Green, Ralph Droms, Russ Housley, Paul Turner, and Steve Fenter. Data Center use of Static Diffie-Hellman in TLS 1.3. Internet-Draft draft-green-tls-static-dh-in-tls13-01, Internet Engineering Task Force, July 2017. URL https://datatracker.ietf.org/doc/html/draft-green-tls-static-dh-in-tls13-01. Work in Progress.

[35] Paul Grubbs, Arasu Arun, Ye Zhang, Joseph Bonneau, and Michael Walfish. Zero-knowledge middleboxes. In *USENIX Security Symposium*, pages 4255–4272. USENIX Association, 2022.

[36] Marian Harbach, Alexander De Luca, Nathan Malkin, and Serge Egelman. Keep on lockin'in the free world: A multi-national comparison of smartphone locking. In *Proceedings of the 2016 chi conference on human factors in computing systems*, pages 4823–4827, 2016.

[37] Franziska Herbert, Steffen Becker, Leonie Schaewitz, Jonas Hielscher, Marvin Kowalewski, Angela Sasse, Yasemin Acar, and Markus Dürmuth. A world full of privacy and security (mis) conceptions? findings of a representative survey in 12 countries. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–23, 2023.

[38] Wei Huang, Ying-Hui Yang, and Heng-Yue Jia. Cryptanalysis and improvement of a quantum communication-based online shopping mechanism. *Quantum Information Processing*, 14:2211–2225, 6 2015. ISSN 15700755. doi: 10.1007/s11128-015-0958-4.

[39] Aylin Ilhan and Kaja J Fietkiewicz. Data privacy-related behavior and concerns of activity tracking technology users from germany and the usa. *Aslib Journal of Information Management*, 73(2):180–200, 2021.

[40] Shubham Jain, Ana-Maria Cretu, and Yves-Alexandre de Montjoye. Adversarial detection avoidance attacks: Evaluating the robustness of perceptual hashing-based client-side scanning. In *USENIX Security Symposium*, pages 2317–2334. USENIX Association, 2022.

[41] Seny Kamara and Tarik Moataz. Boolean searchable symmetric encryption with worst-case sub-linear complexity. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology – EUROCRYPT 2017*, pages 94–124, Cham, 2017. Springer International Publishing. ISBN 978-3-319-56617-7.

[42] Kee Sung Kim, Minkyu Kim, Dongsoo Lee, Je Hong Park, and Woo-Hwan Kim. Forward secure dynamic searchable symmetric encryption with efficient updates. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, page 1449–1463, New York, NY, USA, 2017. Association for Computing Machinery. ISBN 9781450349468. doi: 10.1145/3133956.3133970. URL https://doi.org/10.1145/3133956.3133970.

[43] Sam Kim and David J. Wu. Access control encryption for general policies from standard assumptions. Cryptology ePrint Archive, Paper 2017/467, 2017. URL https://eprint.iacr.org/2017/467. https://eprint.iacr.org/2017/467.

[44] Evgenios M. Kornaropoulos, Nathaniel Moyer, Charalampos Papamanthou, and Alexandros Psomas. Leakage inversion: Towards quantifying privacy in searchable encryption. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, CCS '22, page 1829–1842, New York, NY, USA, 2022. Association for Computing Machinery. ISBN 9781450394505. doi: 10.1145/3548606.3560593. URL https://doi.org/10.1145/3548606.3560593.

[45] Oksana Kulyk, Stephan Neumann, Jurlind Budurushi, and Melanie Volkamer. Nothing comes for free: How much usability can you sacrifice for security? *IEEE Security & Privacy*, 15(3):24–29, 2017. doi: 10.1109/MSP.2017.70.

[46] Shangqi Lai, Sikhar Patranabis, Amin Sakzad, Joseph K. Liu, Debdeep Mukhopadhyay, Ron Steinfeld, Shi-Feng Sun, Dongxi Liu, and Cong Zuo. Result pattern hiding searchable encryption for conjunctive queries. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, page 745–762, New York, NY, USA, 2018. Association for Computing Machinery. ISBN 9781450356930. doi: 10.1145/3243734.3243753. URL https://doi.org/10.1145/3243734.3243753.

[47] Susan Landau. Control use of data to protect privacy. *Science*, 347(6221):504–506, 2015.

[48] Hyunwoo Lee, Zach Smith, Junghwan Lim, Gyeongjae Choi, Selin Chun, Taejoong Chung, and Ted Taekyoung Kwon. matls: How to make TLS middlebox-aware? In *NDSS*. The Internet Society, 2019.

[49] Ada Lerner, Eric Zeng, and Franziska Roesner. Confidante: Usable encrypted email: A case study with lawyers and journalists. In *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 385–400. Institute of Electrical and Electronics Engineers Inc., 6 2017. ISBN 9781509057610. doi: 10.1109/EuroSP.2017.41.

[50] Meng Li, Chhagan Lal, Mauro Conti, and Donghui Hu. Lechain: A blockchain-based lawful evidence management scheme for digital forensics. *Future Generation Computer Systems*, 115:406–420, 2 2021. ISSN 0167739X. doi: 10.1016/j.future.2020.09.038.

[51] Masaki Minami, Kuniyasu Suzaki, and Takashi Okumura. Security considered harmful a case study of tradeoff between security and usability. In *2011 IEEE Consumer Communications and Networking Conference (CCNC)*, pages 523–524, 2011. doi: 10.1109/CCNC.2011.5766529.

[52] Brice Minaud and Michael Reichle. Dynamic local searchable symmetric encryption. *CoRR*, abs/2201.05006, 2022. URL https://arxiv.org/abs/2201.05006.

[53] David Naylor, Kyle Schomp, Matteo Varvello, Ilias Leontiadis, Jeremy Blackburn, Diego R. López, Konstantina Papagiannaki, Pablo Rodríguez Rodríguez, and Peter Steenkiste. Multi-context TLS (mctls): Enabling secure in-network functionality in TLS. In *SIGCOMM*, pages 199–212. ACM, 2015.

[54] Jianting Ning, Xinyi Huang, Geong Sen Poh, Shengmin Xu, Jia-Chng Loh, Jian Weng, and Robert H Deng. Pine: Enabling privacy-preserving deep packet inspection on tls with rule-hiding and fast connection establishment. In *Computer Security–ESORICS 2020: 25th European Symposium on Research in Computer Security, ESORICS 2020, Guildford, UK, September 14–18, 2020, Proceedings, Part I 25*, pages 3–22. Springer, 2020.

[55] Francesco Di Nocera and Giorgia Tempestini. Getting rid of the usability/security trade-off: A behavioral approach. *Journal of Cybersecurity and Privacy*, 2:245–256, 3 2022. doi: 10.3390/jcp2020013.

[56] Erica L. Olmsted-Hawala, Elizabeth D. Murphy, Sam Hawala, and Kathleen T. Ashenfelter. Think-aloud protocols: a comparison of three think-aloud protocols for use in testing data-dissemination web sites for usability. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, page 2381–2390, New York, NY, USA, 2010. Association for Computing Machinery. ISBN 9781605589299. doi: 10.1145/1753326.1753685. URL https://doi.org/10.1145/1753326.1753685.

[57] Joel Olson, Chad McAllister, Lynn D Grinnell, Kimberly Gehrke Walters, and Frank Appunn. Applying constant comparative method with multiple investigators and inter-coder reliability. 2016.

[58] Sarvar Patel, Giuseppe Persiano, and Kevin Yeo. Lower bounds for encrypted multi-maps and searchable encryption in the leakage cell probe model. In Daniele Micciancio and Thomas Ristenpart, editors, *Advances in Cryptology – CRYPTO 2020*, pages 433–463, Cham, 2020. Springer International Publishing. ISBN 978-3-030-56784-2.

[59] Lyn E Pleger, Katharina Guirguis, and Alexander Mertes. Making public concerns tangible: An empirical study of german and uk citizens' perception of data protection and data security. *Computers in Human Behavior*, 122:106830, 2021.

[60] Christine Prince, Nessrine Omrani, Adnane Maalaoui, Marina Dabic, and Sascha Kraus. Are we living in surveillance societies and is privacy an illusion? an empirical study on privacy literacy and privacy concerns. *IEEE Transactions on Engineering Management*, 2021.

[61] Jonathan Prokos, Neil Fendley, Matthew Green, Roei Schuster, Eran Tromer, Tushar M. Jois, and Yinzhi Cao. Squint hard enough: Attacking perceptual hashing with adversarial machine learning. In *USENIX Security Symposium*. USENIX Association, 2023.

[62] Elham Al Qahtani, Yousra Javed, and Mohamed Shehab. User perceptions of gmail's confidential mode. *Proceedings on Privacy Enhancing Technologies*, 2022: 187–206, 1 2022. doi: 10.2478/popets-2022-0010.

[63] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. "warn them" or "just block them"?: Investigating privacy concerns among older and working age adults. *Proceedings on Privacy Enhancing Technologies*, 2021:27–47, 4 2021. doi: 10.2478/popets-2021-0016.

[64] Adrian Reuter, Ahmed Abdelmaksoud, Karima Boudaoud, and Marco Winckler. Usability of end-to-end encryption in e-mail communication. *Frontiers in Big Data*, 4, 7 2021. ISSN 2624909X. doi: 10.3389/fdata.2021.568284.

[65] Christian Reuter, Marc-André Kaufhold, Stefka Schmid, Thomas Spielhofer, and Anna Sophie Hahne. The Impact of Risk Cultures: Citizens' Perception of Social Media Use in Emergencies across Europe. *Technological Forecasting and Social Change (TFSC)*, 148(119724):1–17, 2019. doi: 10.1016/j.techfore.2019.119724. URL http://www.peasec.de/paper/2019/2019_ReuterKaufholdSchmidSpielhoferHahne_TheImpactofRiskCultures_TFSC.pdf.

[66] Tatiana Ringenberg and Lorraine Kisselburgh. A way forward: What we know (or not) about {CSAM} & privacy. 2022.

[67] Scott Ruoti, Jeff Andersen, Daniel Zappala, and Kent E. Seamons. Why johnny still, still can't encrypt: Evaluating the usability of a modern PGP client. *CoRR*, abs/1510.08555, 2015. URL http://arxiv.org/abs/1510.08555.

[68] M. Angela Sasse and Matthew Smith. The security-usability tradeoff myth [guest editors' introduction]. *IEEE Security & Privacy*, 14(5):11–13, 2016. doi: 10.1109/MSP.2016.102.

[69] M. Angela Sasse, Matthew Smith, Cormac Herley, Heather Lipford, and Kami Vaniea. Debunking security-usability tradeoff myths. *IEEE Security & Privacy*, 14 (5):33–39, 2016. doi: 10.1109/MSP.2016.110.

[70] Steve Sheng, Levi Broderick, Colleen Alison Koranda, and Jeremy J Hyland. Why johnny still can't encrypt: evaluating the usability of email encryption software. In *Symposium on usable privacy and security*, pages 3–4. ACM, 2006.

[71] Justine Sherry, Chang Lan, Raluca Ada Popa, and Sylvia Ratnasamy. Blindbox: Deep packet inspection over encrypted traffic. In Steve Uhlig, Olaf Maennel, Brad Karp, and Jitendra Padhye, editors, *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication, SIGCOMM 2015, London, United Kingdom, August 17-21, 2015*, pages 213–226. ACM, 2015. doi: 10.1145/2785956.2787502. URL https://doi.org/10.1145/2785956.2787502.

[72] Dawn Xiaoding Song, D. Wagner, and A. Perrig. Practical techniques for searches on encrypted data. In *Proceeding 2000 IEEE Symposium on Security and Privacy. S&P 2000*, pages 44–55, 2000. doi: 10.1109/SECPRI.2000.848445.

[73] Philipp Stachwitz and Jörg F Debatin. Digitalisierung im gesundheitswesen: heute und in zukunft. *Bundesgesundheitsblatt-Gesundheitsforschung-Gesundheitsschutz*, 66(2):105–113, 2023.

[74] Shi-Feng Sun, Xingliang Yuan, Joseph K. Liu, Ron Steinfeld, Amin Sakzad, Viet Vo, and Surya Nepal. Practical backward-secure searchable encryption from symmetric puncturable encryption. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, page 763–780. Association for Computing Machinery, 2018. ISBN 9781450356930.

[75] Kishore Thapliyal and Anirban Pathak. Quantum e-commerce: a comparative study of possible protocols for online shopping and other tasks related to e-commerce. *Quantum Information Processing*, 18, 6 2019. ISSN 15731332. doi: 10.1007/s11128-019-2309-3.

[76] The Guardian. Eu lawyers say plan to scan private messages for child abuse may be unlawful, May 2023. URL https://www.theguardian.com/world/2023/may/08/eu-lawyers-plan-to-scan-private-messages-child-abuse-may-be-unlawful-chat-controls-regulation. accessed August 21, 2023.

[77] Christian Tiefenau, Emanuel von Zezschwitz, Maximilian Häring, Katharina Krombholz, and Matthew Smith. A usability evaluation of let's encrypt and certbot: Usable security done right. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 1971–1988. Association for Computing Machinery, 11 2019. ISBN 9781450367479. doi: 10.1145/3319535.3363220.

[78] Christine Utz, Steffen Becker, Theodor Schnitzler, Florian M Farke, Franziska Herbert, Leonie Schaewitz, Martin Degeling, and Markus Dürmuth. Apps against the spread: Privacy implications and user acceptance of covid-19-related smartphone apps on three continents. In *Proceedings of the 2021 chi conference on human factors in computing systems*, pages 1–22, 2021.

[79] Xiuhua Wang and Sherman S. M. Chow. Cross-domain access control encryption: Arbitrary-policy, constant-size, efficient. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 748–761, 2021. doi: 10.1109/SP40001.2021.00023.

[80] Alma Whitten and J Doug Tygar. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *USENIX security symposium*, volume 348, pages 169–184, 1999.

[81] Amrendra Singh Yadav, Vincent Charles, Dharen Kumar Pandey, and Somya Gupta. Blockchain-based secure privacy-preserving vehicle accident and insurance registration. *Expert Systems with Applications*, 230, 11 2023. ISSN 09574174. doi: 10.1016/j.eswa.2023.120651.

[82] Elena Yanakieva, Michael Youssef, Ahmad Hussein Rezae, and Annette Bieniusa. On the impossibility of confidentiality, integrity and accessibility in highly-available file systems. In *Networked Systems: 9th International Conference, NETYS 2021, Virtual Event, May 19–21, 2021, Proceedings*, pages 3–18. Springer, 2021.

[83] Collin Zhang, Zachary DeStefano, Arasu Arun, Joseph Bonneau, Paul Grubbs, and Michael Walfish. Zombie: Middleboxes that don't snoop. *IACR Cryptol. ePrint Arch.*, page 1022, 2023.

[84] Houyu Zheng, Lin You, and Gengran Hu. A novel insurance claim blockchain scheme based on zero-knowledge proof technology. *Computer Communications*, 195:207–216, 11 2022. ISSN 1873703X. doi: 10.1016/j.comcom.2022.08.007.

A APPENDIX

A.1 Comparison of Samples

In the following we provide the detailed results of our comparison of the qualitative sample and the representative sample.

Item	Sample 1	Sample 2	Significance	Effect Size	Mann-Whitney-U
General practitioner	A (1.43)	B1 (1.99)	0.004	-0.13	5953.5 (weak)
	B1 (1.99)	C1 (1.83)	0.007	-0.08	108585.5 (very weak)
	A (1.43)	B2 (2.09)	0.001	-0.19	3261.5 (weak)
	B2 (2.09)	C2 (1.83)	0.001	-0.1	75306.5 (very weak)
Medical specialist	A (1.33)	B1 (1.88)	0.001	-0.14	5764.0 (weak)
	B1 (1.88)	C1 (1.85)	0.315	-0.02	115498.0 (insignificant)
	A (1.33)	B2 (1.99)	0.001	-0.2	3209.5 (weak)
	B2 (1.99)	C2 (1.82)	0.048	-0.05	80186.5 (very weak)
Lawyer/Court	A (1.1)	B1 (1.93)	0.0	-0.24	4574.0 (weak)
	B1 (1.93)	C1 (2.04)	0.29	-0.02	115223.5 (insignificant)
	A (1.1)	B2 (1.95)	0.0	-0.29	2716.0 (weak)
	B2 (1.95)	C2 (2.01)	0.443	-0.0	84407.5 (insignificant)
Chaplain	A (1.45)	B1 (2.76)	0.0	-0.29	3521.0 (weak)
	B1 (2.76)	C1 (3.51)	0.0	-0.25	84100.0 (weak)
	A (1.45)	B2 (2.91)	0.0	-0.38	1874.0 (moderate)
	B2 (2.91)	C2 (3.32)	0.0	-0.12	72843.0 (weak)
Insurance Company	A (1.6)	B1 (2.1)	0.006	-0.12	5981.0 (weak)
	B1 (2.1)	C1 (2.09)	0.848	0.03	118817.0 (insignificant)
	A (1.6)	B2 (2.21)	0.001	-0.19	3257.5 (weak)
	B2 (2.21)	C2 (2.06)	0.075	-0.05	80651.5 (insignificant)
Customer support (Online-Shop)	A (2.83)	B1 (2.4)	0.032	-0.09	6393.5 (very weak)
	B1 (2.4)	C1 (2.12)	0.0	-0.12	101856.5 (weak)
	A (2.83)	B2 (2.53)	0.164	-0.06	4051.0 (insignificant)
	B2 (2.53)	C2 (2.14)	0.0	-0.15	69695.5 (weak)
Clergy	A (2.34)	B1 (3.37)	0.0	-0.22	4432.5 (weak)
	B1 (3.37)	C1 (3.77)	0.0	-0.15	68691.5 (weak)
	A (2.34)	B2 (3.44)	0.0	-0.28	2497.5 (weak)
	B2 (3.44)	C2 (3.67)	0.017	-0.07	78358.5 (very weak)
Social worker	A (1.92)	B1 (2.69)	0.0	-0.16	5044.0 (weak)
	B1 (2.69)	C1 (3.25)	0.0	-0.19	92152.0 (weak)
	A (1.92)	B2 (2.83)	0.0	-0.24	2715.5 (weak)
	B2 (2.83)	C2 (3.11)	0.009	-0.07	77361.5 (very weak)
Supervisor	A (1.95)	B1 (2.21)	0.166	-0.05	6948.5 (insignificant)
	B1 (2.21)	C1 (2.99)	0.0	-0.25	83816.5 (weak)
	A (1.95)	B2 (2.24)	0.134	-0.07	4013.0 (insignificant)
	B2 (2.24)	C2 (2.83)	0.0	-0.16	67478.0 (waek)
Colleagues	A (2.24)	B1 (2.26)	0.94	0.08	7884.0 (insignificant)
	B1 (2.26)	C1 (2.74)	0.0	-0.16	96906.5 (weak)
	A (2.24)	B2 (2.32)	0.811	0.05	4558.0 (insignificant)
	B2 (2.32)	C2 (2.62)	0.007	-0.08	77064.0 (very weak)
Friends	A (1.83)	B1 (1.96)	0.825	0.05	7782.5 (insignificant)
	B1 (1.96)	C1 (1.9)	0.227	-0.02	114561.5 (insignificant)
	A (1.83)	B2 (2.2)	0.099	-0.08	3948.5 (insignificant)
	B2 (2.2)	C2 (1.84)	0.0	-0.14	70757.5 (weak)
Family	A (1.64)	B1 (1.88)	0.568	0.01	7546.0 (insignificant)
	B1 (1.88)	C1 (1.71)	0.027	-0.06	110667.5 (very weak)
	A (1.64)	B2 (2.12)	0.045	-0.1	3803.5 (very weak)
	B2 (2.12)	C2 (1.68)	0.0	-0.16	68645.0 (weak)
Sum	A (21.56)	B1 (27.42)	0.0	-0.18	4548.0 (weak)
	B1 (27.42)	C1 (29.78)	0.0	-0.12	101247.5 (weak)
	A (21.56)	B2 (28.82)	0.0	-0.28	2272.5 (weak)
	B2 (28.82)	C2 (28.91)	0.66	0.01	85451.5 (insignificant)

Table 2: Statistical comparison of the samples for Item 1

Item	Sample 1	Sample 2	Significance	Effect Size	Mann-Whitney-U
First name	A (1.19)	B1 (1.27)	0.254	-0.03	7287.0 (insignificant)
	B1 (1.27)	C1 (1.21)	0.032	-0.06	112552.5 (very weak)
	A (1.19)	B2 (1.26)	0.333	-0.03	4332.0 (insignificant)
	B2 (1.26)	C2 (1.23)	0.303	-0.02	84239.0 (insignificant)
Last name	A (1.52)	B1 (1.51)	0.872	0.06	7833.0 (insignificant)
	B1 (1.51)	C1 (1.37)	0.0	-0.13	102589.5 (weak)
	A (1.52)	B2 (1.52)	0.989	0.14	4656.0 (insignificant)
	B2 (1.52)	C2 (1.39)	0.0	-0.11	75571.0 (weak)
Address	A (1.98)	B1 (1.76)	0.001	-0.15	6216.0 (weak)
	B1 (1.76)	C1 (1.58)	0.0	-0.18	98353.5 (weak)
	A (1.98)	B2 (1.77)	0.002	-0.18	3681.0 (weak)
	B2 (1.77)	C2 (1.61)	0.0	-0.13	73801.0 (weak)
Email address	A (1.6)	B1 (1.39)	0.01	-0.11	6300.0 (weak)
	B1 (1.39)	C1 (1.3)	0.003	-0.09	108832.5 (very weak)
	A (1.6)	B2 (1.4)	0.02	-0.13	3756.0 (weak)
	B2 (1.4)	C2 (1.31)	0.012	-0.07	79286.5 (very weak)
IBAN	A (1.88)	B1 (1.85)	0.613	0.01	7707.0 (insignificant)
	B1 (1.85)	C1 (1.88)	0.13	-0.04	115710.0 (insignificant)
	A (1.88)	B2 (1.86)	0.723	0.04	4566.0 (insignificant)
	B2 (1.86)	C2 (1.88)	0.526	0.0	85734.5 (insignificant)
PayPal account	A (1.8)	B1 (1.79)	0.867	0.05	7836.0 (insignificant)
	B1 (1.79)	C1 (1.84)	0.059	-0.05	114039.0 (insignificant)
	A (1.8)	B2 (1.8)	0.965	0.11	4565.0 (insignificant)
	B2 (1.8)	C2 (1.83)	0.343	-0.01	84739.0 (insignificant)
Billing Address	A (1.61)	B1 (1.45)	0.055	-0.08	6907.5 (insignificant)
	B1 (1.45)	C1 (1.32)	0.0	-0.13	104071.5 (weak)
	A (1.61)	B2 (1.46)	0.087	-0.08	4109.5 (insignificant)
	B2 (1.46)	C2 (1.34)	0.001	-0.1	76677.5 (very weak)
Customer ID	A (1.34)	B1 (1.38)	0.621	0.02	7443.0 (insignificant)
	B1 (1.38)	C1 (1.43)	0.14	-0.03	113994.0 (insignificant)
	A (1.34)	B2 (1.35)	0.948	0.1	4526.5 (insignificant)
	B2 (1.35)	C2 (1.43)	0.035	-0.06	80283.5 (very weak)
Mobile number	A (1.86)	B1 (1.68)	0.016	-0.1	6510.0 (very weak)
	B1 (1.68)	C1 (1.55)	0.0	-0.12	104007.0 (weak)
	A (1.86)	B2 (1.73)	0.081	-0.09	4068.0 (insignificant)
	B2 (1.73)	C2 (1.56)	0.0	-0.14	71946.0 (weak)
telephone number	A (1.82)	B1 (1.75)	0.396	-0.01	7626.0 (insignificant)
	B1 (1.75)	C1 (1.48)	0.0	-0.27	86890.5 (weak)
	A (1.82)	B2 (1.8)	0.794	0.05	4296.0 (insignificant)
	B2 (1.8)	C2 (1.52)	0.0	-0.23	62950.5 (weak)
Social media accounts	A (1.64)	B1 (1.7)	0.46	-0.0	6948.0 (insignificant)
	B1 (1.7)	C1 (1.85)	0.0	-0.18	101511.0 (weak)
	A (1.64)	B2 (1.74)	0.187	-0.05	3886.5 (insignificant)
	B2 (1.74)	C2 (1.81)	0.041	-0.05	81634.5 (very weak)
Social media accounts of friends	A (1.87)	B1 (1.78)	0.163	-0.05	7792.5 (insignificant)
	B1 (1.78)	C1 (1.91)	0.0	-0.18	104074.5 (weak)
	A (1.87)	B2 (1.82)	0.395	-0.02	4573.5 (insignificant)
	B2 (1.82)	C2 (1.87)	0.051	-0.05	82586.5 (insignificant)
Sum	A (20.23)	B1 (24.68)	0.0	-0.34	1904.5 (moderate)
	B1 (24.68)	C1 (24.28)	0.053	-0.05	110971.0 (insignificant)
	A (20.23)	B2 (24.83)	0.0	-0.43	1030.0 (moderate)
	B2 (24.83)	C2 (24.29)	0.023	-0.06	78473.0 (very weak)

Table 3: Statistical comparison of the samples for Item 2

A.2 Participant Demography

Since the majority of our participants were students, we surveyed their study subjects. For non-student participants, the fields are marked with "-".

	Gender	Age	Study Subject
P1	male	23	Civil Engineering
P2	male	19	Computer Science
P3	male	24	Mechanical Engineering
P4	male	25	Civil Engineering
P5	male	21	Political Science
P6	male	22	Computer Science
P7	female	34	Education in global mechanization processes
P8	male	26	Computer Science
P9	male	21	Mathematics
P10	female	24	Civil Engineering
P11	male	26	Mechanical Engineering
P12	female	22	Political Science
P13	male	23	Information Systems Engineering
P14	male	23	Computer Science
P15	male	23	Computer Science
P16	male	22	Computer Science
P17	male	24	Computer Science
P18	male	27	IT-Security
P19	male	27	Civil Engineering
P20	female	28	Data and Discourse Studies
P21	male	18	Computer Science
P22	female	23	Political Science
P23	male	19	Computer Science
P24	female	20	Computer Science
P25	male	21	Mathematics/Computer Science
P26	male	29	Computer Science/Philosophy
P27	male	19	Computer Science
P28	female	21	Computer Science
P29	male	21	Computer Science
P30	male	22	Computer Science
P31	male	19	Computer Science
P32	male	20	Computer Science
P33	male	17	Computer Science
P34	male	24	Computer Science
P35	male	23	Computer Science
P36	female	19	Business Informatics
P37	male	42	Computer Science/History
P38	male	23	Business Informatics
P39	male	21	-
P40	male	19	Business Informatics
P41	female	20	Computer Science
P42	female	32	-

Table 4: Gender, age and study subjects of participants

A.3 Interview Guideline

A.3.1 Outline.

(1) **Introduction**: First, the evaluation begins with the introduction of the topic and the informing of the test subject. For this purpose, the Informed Consent (mailed beforehand to the participant) is handed out and discussed in detail. When a brief introduction to the topic is given, care should be taken not to anticipate too much, as this could bias the results. We do not want to "put words in the mouths" of the participants. It is important to clarify that the purpose is to test a particular tool for its practicality and that the purpose is not to evaluate the participants themselves. Finally, the consent of the participant and their signature on the Informed Consent are obtained.

(2) **First questionnaire**: The participant is asked to fill in the questionnaires that have already been opened on a laptop computer. Care should be taken to ensure that the interviewers gives the test person a little more space and does not give the impression that they are permanently looking over their shoulder.
   (a) Demographics
   (b) OPLIS-questionnaire
   (c) items from the quantitative pre-study for comparison

(3) **Hands-on experiment**: The experimenter instructs the participant to please say each thought and idea out loud. The so-called think-aloud method helps with the evaluation, as it is important to collect initial impressions of the product and to record how the participant reacts to the device. In this way, problems and pitfalls can be identified that would otherwise not be explicitly noted.
   Intro-text as reference for briefing: Due to new advancements in research, it is possible to generate a second pair of secret keys during the establishment of a TLS-connection, a secured connection in the internet. This was designed for people who want to communicate with companies that per default share the secret keys with the firewall to scan all network traffic or for people who live in countries where the government surveils all communication. The second key can be used to add another layer of encryption to communicate with those people. We investigate, whether this approach can also provide benefits for normal citizens in Germany in everyday use cases such as communicating with doctors. We prepared two demonstrators for this use case: When you fill out the online form, you can decide which information is only visible for the doctor and no other person in the office.
   (a) **A/B-Testing:** Participants with an odd participants ID get the *non-customizable version* first, participants with en even participant ID get the *customizable version* first.
      Tasks:
      (i) Fill in the form with data that looks reasonable to you. You do not have to fill in your real address but data that would make sense in your opinion. Order an receipt for a medicine of your choice or a letter of referral to another doctor of your choice.
      (ii) We simulate the process of submitting the form and transmitting it to the doctor. You can see this on the second view.
      (iii) After completing to your request the doctor sends you an email as answer. You can see this in the third view.
   (b) UEQ-S questionnaire for the corresponding demonstrator

(c) Repeat the tasks for the other demonstrator: participants with odd ID get the *customizable version*, those with an even ID get the *textfield version*
(d) UEQ-S questionnaire for the corresponding demonstrator
(e) questionnaire to compare both demonstrators
(i) Choose the version you liked best
(ii) Give a brief explanation of your choice

(4) **Discussion and Interview** (10 minutes)
(a) **Guiding questions:**
(i) How would you improve the system or which feature would you like to add?
(ii) Which aspect did you like in particular?
(iii) In the *customizable version* you chose to protect <item>. Would you change which items you would protect based on the medicine you are ordering or the requested referral?
(iv) In the answer email the protected fields were hidden and had to be decrypted manually. Can you imagine use cases where it would be beneficial to you if people in your household or surroundings cannot see for what reason you contacted the doctor?
(v) The protected fields were only visible for the doctor and no one else in the doctor's office. In which use cases would it be important to you that no one knows why you are in the doctors office?
(b) **Asking for discretion:** At the end we ask the participants not to reveal the content of the study to others who are yet to participate in the study. This would negatively influence the results of our study.

A.3.2 Hardware.

- Laptop for the participants to answer the questionnaires (hosted via own LimeSurvey instance) and interact with the demonstrators
- Mouse for the participant's laptop for easier use
- Laptop for the interviewer, which was used for audio recording
- Microphone for audio recording

A.4 Overview of Methods

In this section, we provide a brief overview of the different methods used in this paper:

Step 1: Quantitative Pre-Study (see Section 3): In order to find the most relevant use case for our concept, we conducted a quantitative study with a representative sample (N=1011) for the German population. Quantitative research provides results that can be generalized because they are representative. However, it does not provide extensive feedback for in-depth investigations on one topic. Therefore, we chose to use quantitative research to find a suitable and relevant use case for secure and private communication. Detailed information on the method of this step can be found in Section 3.1.

Step 2: Theoretical Concept (see Section 4): Our aim is to enable users to customize their privacy in Consumer-to-Business (C2B) communication. Therefore, we derived a concept from related work that adapts methods from cryptography to enhance privacy for users. Please note that we did not implement this concept into a real application because we followed an iterative design process that utilizes feedback loops with possible users.

Step 3: Qualitative Evaluation (see Section 5): We conducted 42 interviews to gain extensive feedback on our concept. For this purpose, we implemented two interactive demonstrators: one that provides no customization options and another that provides full customization options for each data field in the message to investigate the control paradox (see Section 5.1.2). Qualitative research uses smaller sample sizes, which makes it difficult to generalize the results for the entirety of a population. However, this form of research allows participants to engage with the research subject (e.g. the demonstrators) and provide rich feedback. Furthermore, the general concept can be discussed in depth and differentiated opinions can be identified, which would not be possible in quantitative approaches like pre-defined questionnaires. The recruitment of participants, the used materials, and detailed information on the procedure can be found in Section 5.1.

A.5 Illustration of the D³ Concept

In Figure 3 the interaction between the user trying to contact a recipient within an organization is depicted.

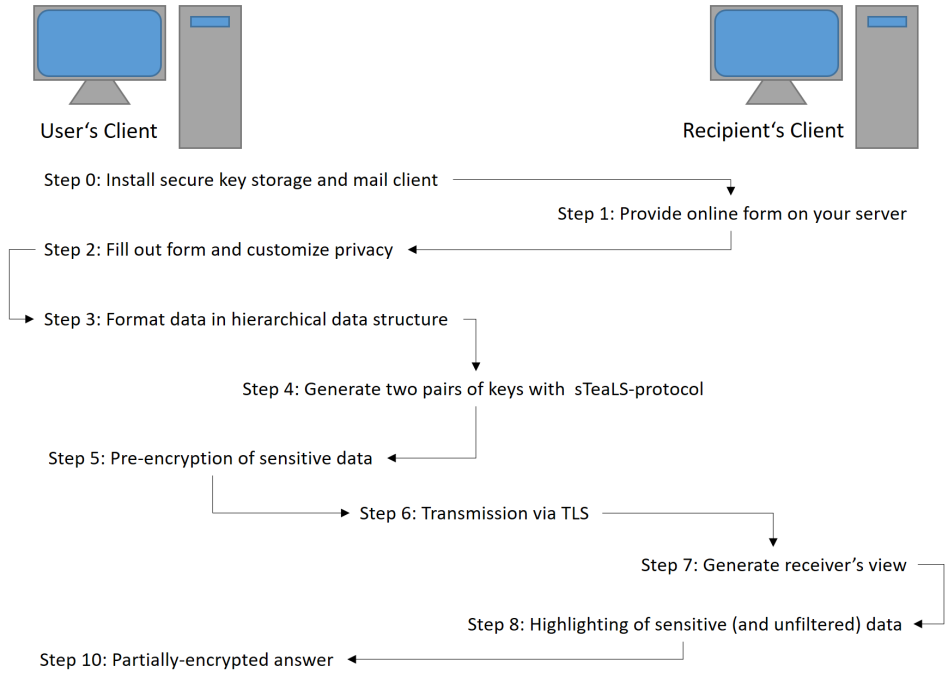

Figure 3: Illustration of the D³ concept: Interaction between user and recipient

A.6 Demonstrators

In the two figures below are screenshots from the demonstrators used in the evaluation. Please note that the depicted demonstrators were translated into English for this paper. The demonstrators used in the study were in German. Figure 4 shows the non-customizable version, while Figure 5 depicts the customizable version.

A.7 Usability Scores

In Table A.7 the detailed scores of the UEQS-S scale are shown. Since all values are above 4.5, our demonstrators were attested with excellent usability. This implies that the results of our evaluation were not negatively affected by lacking usability.

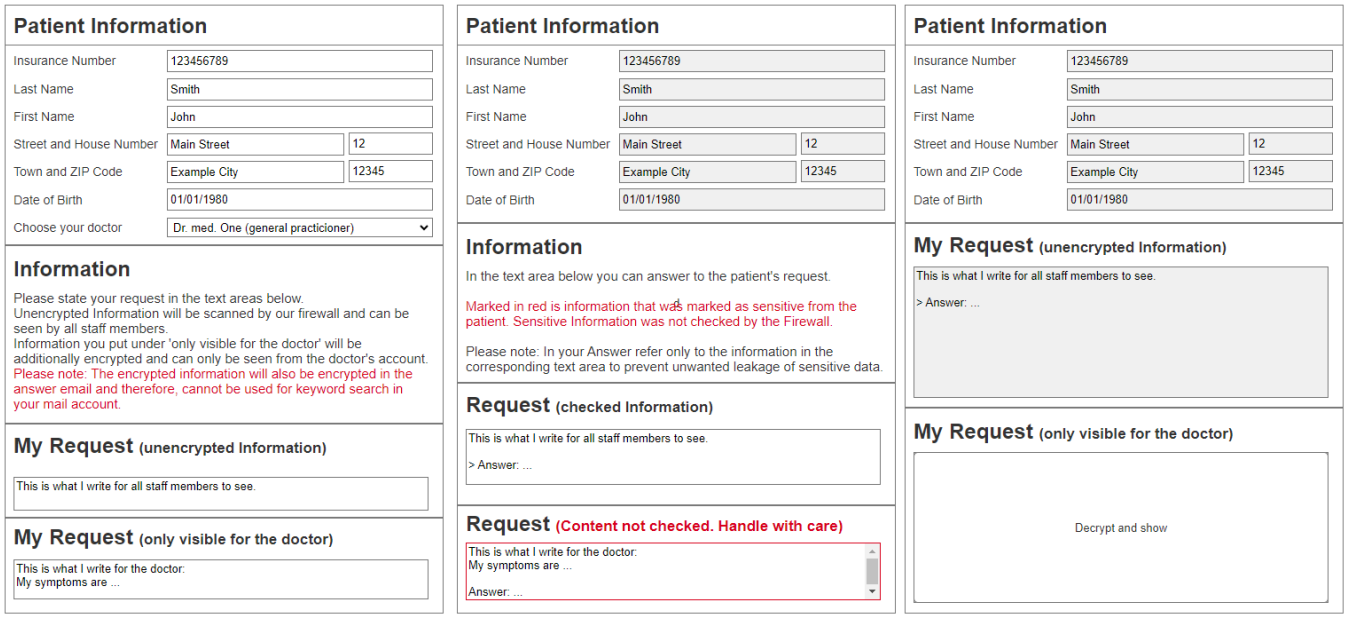

Figure 4: Mock-up for the non-customizable version: online form (left), doctor's view (middle) and answer email (right)

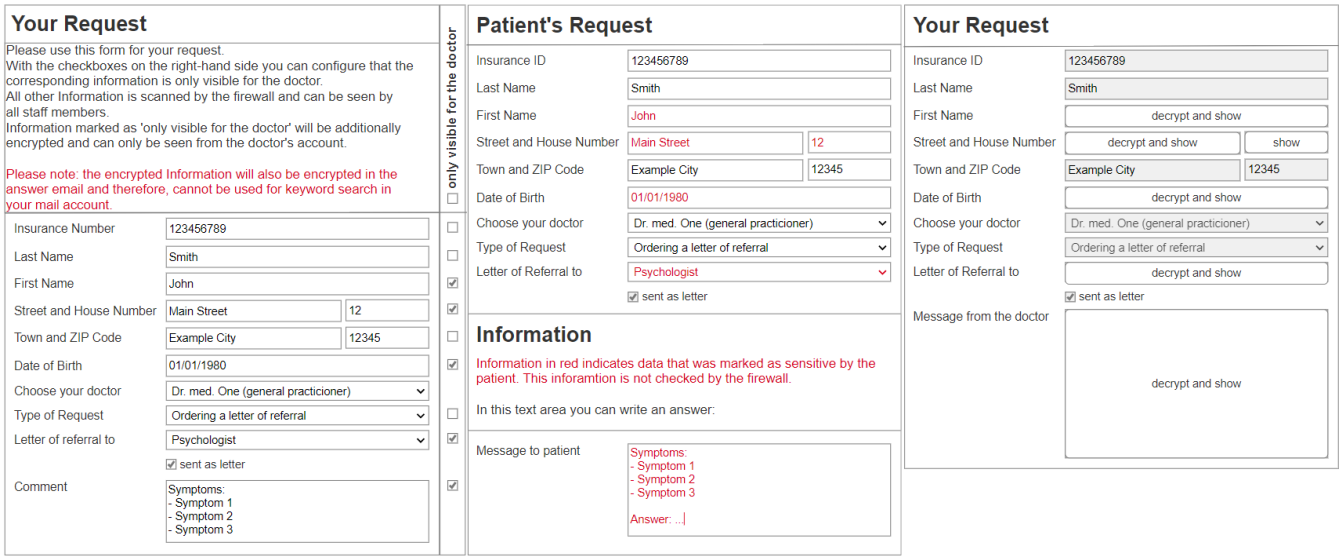

Figure 5: Mock-up for the customizable version: online form (left), doctor's view (middle) and answer email (right)

Table 5: Results of the UEQ-S questionnaire for usability.

Scale	Non-Customizable Version					Customizable Version				
	Mean	STD	N	Confidence	Confidence Interval	Mean	STD	N	Confidence	Confidence Interval
UEQ-S Overall	5,19	1,01	42	0,30	4,89 - 5,50	5,55	0,77	42	0,23	5,31 - 5,78
Pragmatic Quality	5,49	1,32	42	0,40	5,09 - 5,89	5,76	1,03	42	0,31	5,44 - 6,07
Hedonic Quality	4,87	1,12	41	0,34	4,53 - 5,22	5,34	1,03	42	0,31	5,02 - 5,65

A.8 Code Book

We split the code book into two parts because it would not fit the template otherwise.

A.8.1 Code book Part I: Need for increased privacy in medical offices. This part contains the codes that refer to the reasons why participants wish for increased privacy when they are attending a medical office. This does not include statements that wish for more privacy when reaching out to the medical office online. due to the design of our interaction concept we distinguish between remote patients and those who are present in the office.

Codes	Sub-Codes	Qualifications and exclusions	Number of Participants
Trust in staff members		Trust that staff members in medical offices will not leak data due to training in their job and the adherence to German data protection laws	10
Sensible Topics		Topics that can be a reason that a person is not visiting the medical office or having the feeling of strong discomfort when being in a public office; Includes only statements that refer to the wish for increased privacy when present at the medical office (e.g. being eavesdropped by other patients); excludes: shame or fears that prevent from getting help at all or all statements that refer to increased privacy in private context	2
	Intimate topics	Statement of the embarrassment when being witnessed at the doctor for intimate reasons.	8
	Psychological issues	Fear when being seen at the psychologist or getting a referral to the psychologist	19
	Taboos or embarrassing issues	The fear of being stigmatized for the reason for visiting the medical office.	17
Social aspects		Reasons to not visit a medical office that are not due to the diagnosis but to social circumstances	1
	Living in rural areas or small towns	Participants stating that they live in an area where most people know each other. Being seen in a medical office would leak information on health condition and spread rumors	8
	Rumors	General fear of rumors spreading	3
	Relatives or Acquaintances among personnel	Wish for increased privacy (especially layered encryption) to hide information from relatives or acquaintances who work in the medical office; Also includes statements of participants who avoid medical offices for this reason and instead go to doctors where nobody knows them	19
Fear of using the telephone		Statements covering the general fear of using the telephone as well as statements that the voice of the staff member would leak information even if the patient is not present at the office	8

A.8.2 Code book Part II: Reasons to utilize security and privacy. This part consists of the codes regarding topics that raise the need for increased privacy for the communication with doctors from the patients' circumstances. This includes situations in which privacy is important or topics that require secrecy.

Codes	Sub-Codes	Qualifications and exclusions	Number of Participants
Coping with diagnoses and decision whether to share it		Participants talking about the wish to cope with a diagnosis themselves before disclosing it to others; Wish for sovereignty to decide when or whether others are informed about health issues and diagnoses; Especially lethal diagnoses or information about life expectancy are wished to kept secret until the patients have processed it themselves	12
Housing Situation		Privacy and security decisions are affected by the housing situation so that the behavior would be different if the person was living alone.	2
	Family and friends are not critical	The participants state no hesitation to talk openly about their health condition with family and friends. Health issues are disclosed to them.	12
	Mistrust at home	The participants do not want to share sensitive information with other cohabitants due to mistrust or a bad relationship between them	4
	parents protect their children	Parents do not want that their children get worried because of the parents' diagnosis	3
	protect children from their parents	Measures taken to circumvent parental surveillance; Contacting doctors without the parents knowing; Hide incidents from parents	8
	going to the gynecologist against the will of the environment	Minors wanting to attend the gynecologist against their parents will; Women in general having contact with the gynecologist against the will of their families; Exclusion: personal beliefs that hinder the attendance of the gynecologist are not applicable here (e.g.religious beliefs or other personal reasons are covered by other codes)	3
	Shared flats	Participants state the influence of roommates on their privacy behavior: e.g not wanting them to know about doctoral appointments	8
	Having a divorce	A couple still living together but having a divorce; Increased need for privacy due to legal reasons	1
	Domestic violence	Victims of domestic violence should be protected from the people in their household; Challenges in teh communication with doctors due to domestic violence	4
Intimate topics		Topics mentioned by the participants that are embarrassing but do not resemble a topic stigmatized by society	11
	(unplanned) pregnancy	Participants stating special needs for the communication with doctors; Being pregnant against the will of the family	6
	Results from the urologist	Results of tests conducted by the urologist; Issues in the genital area	5
	Abortion	Having an abortion; Family and social environment may be against it	3
Taboos or topics stigmatized by society		Topics that are stigmatizes or have a bad reputation within society leading to hesitation when getting help	13
	STIs	Quotes about sexually transmittable infections	12
	Depression (+ other psychological issues)	Statements about feeling shame in the context of psychological problems such as depression; Statements on the intolerance of others regarding this topic; criticism on society for stigmatizing these problems	9
	Drugs (incl. Alcohol)	Statements on drugs and dependencies; includes the abuse of alcohol	3
	Help for suicidal people	Special needs for suicidal people in order for them to get help	1
Fear of discrimination		Topics mentioned by participants that state a general or specific fear of discrimination; Includes the general fear of being discriminated regardless the of the background as well as specific prejudices against marginalized groups; Fear of not being able to live the own life in the same way as it was before disclosing information	2
	LGBTQ topics	Fear of discrimination due to gender, sexual orientation or sexuality	2
	(mental) disablement	Being discriminated due to physical or mental disablement	1
School topics		Protecting the communication between teachers, students and parents	3
Legal documents		Communicating with lawyers or the court; Participants stating the use of D^3 for legal use cases; Protection of important documents from the eyes of others	22
Religious reasons		Religious beliefs, traditions and moral codes that can cause cultural clashes or prevent people from getting help; Religious gender roles and restrictions	3