HCI Patterns for Cryptographically Equipped Cloud Services

Thomas Länger[1], Ala Alaqra[2], Simone Fischer-Hübner[2], Erik Framner[2], John Sören Pettersson[2] and Katrin Riemer[3]

[1] Université de Lausanne, Lausanne, Switzerland
thomas.laenger@unil.ch
[2] Karlstad University, Karlstad, Sweden
[3] XiTrust Secure Technologies GmbH, Graz, Austria

Abstract. Recent cryptographic research has devised several new algorithms and protocols with a potential of mitigating several of the most ardent security and privacy threats, existing in currently available public cloud services. Nevertheless, such cryptographic schemes often exhibit counterintuitive functionality to end users, or they work differently to other already established traditional schemes with which users are already familiar. A practical solution to address these problems involves a human centered design approach, deriving Human Computer Interaction (HCI) requirements from consultations and extensive testing with experts, prospective end users, and other stakeholders. The European Horizon 2020 project PRISMACLOUD "Privacy and Security Maintaining Services for the Cloud" uses such an approach and provides HCI patterns as part of its proper cloud service development methodology CryptSDLC to communicate HCI requirements to cloud service designers and user interface implementers. In this article, we present several new cryptographic cloud services, e.g. for redacting digitally signed data, and for redundant storage and sharing of confidential data in a public cloud scenario, together with three example HCI patterns for specific interactions of end users with these services. We show how these patterns were elaborated and validated in practice to prove the suitability for their intended purpose. To summarize, we give an account on our practical experience during the actual prototype development and implementation and show how they constitute an essential element of the CryptSDLC development methodology.

Keywords: Cloud computing, cryptography, HCI patterns, end-user security, end-user privacy

1 Use of Cryptography in the Cloud

1.1 Current Security and Privacy Situation

For end users of public cloud systems, be they individuals, corporations, administrations, or other entities, a central feature is that data is given to someone else for storage and processing. This is assumed as being cost effective, enabling sharing of data and applications among devices and other cloud users, and providing protection against data

loss. But as regards protection of confidentiality, and also of integrity, and availability of the data, the cloud provider (the "controller" and "processor", in the terms of the GDPR [1]) has to be trusted to protect the data against all kinds of attacks by malicious hackers and other outsiders. In many cases, the cloud provider itself has full access to the end user data—plus the metadata arising from usage and access to the data. The cloud provider may be honestly defending end user data against outsiders, but be curious, and untrustworthy with respect to confidentiality. In several currently available public cloud offerings for individual end users, it is the very business model of the cloud provider to collect and use the user-generated content and the knowledge of user interaction for their own business.

Hence, end users have to face threats against the confidentiality of their data, and that the data remains available through the cloud service. In specific cloud applications, the integrity of private or personal data may also be under threat. However, cloud controllers, and especially now also the processors that perform the actual storage and processing in the cloud of data related to subjects in the European Union, have strong reasons to combat such threats: From May 25, 2018, when the GDPR will apply, they are facing significant fines if there are no appropriate means of security in place.

1.2 Suitable Cryptographic Primitives and Protocols

A preferred method to address several of these security and privacy concerns would be to use cryptographic protection from end to end, together with specific cryptographic functionality to reduce the amount of metadata being generated in secure and authentic transactions. However, in public cloud systems currently available on the market, cryptography is mostly only used for protecting the data between the end user and the cloud, while in the cloud the data is completely entrusted to the protection capabilities and the benevolence of the cloud provider. Most cloud services provide cryptographic protection of the data only in motion between end users and the cloud, and some provide encryption of data at rest in a simple use case, precluding further sharing and processing of the data in the cloud plus requiring from the end user a fully-fledged cryptographic key management system with all its consequences.

Nevertheless, cryptographic research carried out by researchers from universities, research centers, and corporations, is currently proposing cryptographic primitives and protocols for addressing several of these threats, and demonstrating technology readiness of its solutions with several application demonstrators in realistic cloud environments. The H2020 project PRISMACLOUD proposes the use of secret sharing for distributed storage and archiving of data among multiple cloud providers, with no single cloud provider aware of the plain data. In fact, a *secret sharing algorithm* can give more information to storage providers that are more "trustworthy". The secure data archive also enables the implementation of a secure and securely private data sharing service in a cloud of clouds, without having to rely on the need to trust one cloud provider. We demonstrate such a service in an infrastructure provider for administrations of municipalities of a region in Europe, providing secure and reliable archiving services, in a mix of private clouds and public clouds that are rented on demand.

A *selective authentic exchange service* enables end users to have verified and digitally signed information hosted in a cloud service with the intention to have precisely selected verifiable information items disclosed to a third party. This particular service wants to ensure that only an exactly specified subset of the data is revealed, the authenticity of which nevertheless can be cryptographically verified. This counters the unfavorable consequence in current certificate based authenticity systems: That always the entire certificate, the entire information need to be revealed, even when only e.g. one particular piece of authentic data (e.g. the age, the name to a key…) is required. The selective authentic exchange service is demonstrated by a prototype in the health domain. In a hospital, doctors digitally sign medical data, e.g. diagnosis data, or lab data. The patients, if they need to show some of the medical data to third persons (employer, dietician etc.), can select several data to be "blackened out", i.e. redacted from the document, without the other, remaining items losing their valid signatures.

Nevertheless, cryptographic schemes such as the ones used in PRISMACLOUD often provide "crypto-magic" and thus exhibit counterintuitive functionalities to end users, or they work differently to other already established traditional schemes with which users are already familiar [2]. Also for this reason, the HCI (Human Computer Interaction) research in PRISMACLOUD has played an important role, and the HCI patterns discussed in this paper are reflecting the results of this HCI work.

1.3 HCI Patterns as Promoter of Cryptography Diffusion.

An analysis of promoters and inhibitors of cryptography diffusion in the (public) cloud context [3] yielded several results, among these that it is favorable to have during the cloud service development process the proper instruments and procedures in place to communicate requirements and capabilities across the domains of experts, involved in the development process on the different layers. Design patterns in their different expressions as *security and privacy patterns***,** as well as *HCI patterns* are such communication instruments—of which we will show three instantiations below. The HCI patterns are being developed with feedback from end users, and codify requirements and design decisions for several HCI aspects of the application of cryptographic cloud services. As such, the HCI patterns support the creation of usable and accepted end user applications.

Other promoters identified. Another promoter for the diffusion of cryptography in cloud applications, as identified in the context of the PRISMACLOUD project, is the *usage of a service and tool based approach,* where the cryptography, with its complexity, is hidden inside a tools layer, and thus can more safely and securely be used by cloud service developers. *Standardization of cryptographic primitives and protocols* (algorithms and parametrization) *and compliance to regulation* are also beneficial to increase trust in cryptographic cloud services and make them more widely used. Compliance, in the European context compliance with the GDPR, will require from controllers and processors (aka providers) that they use appropriate technical means of protection, which could include for privacy-sensitive applications, such as eHealth applications, strong cryptography to (provably) protect entrusted personal data—otherwise,

the GDPR foresees severe financial fines for cases where a breach happens with no adequate data protection in place.

Other inhibitors identified. The *complex and frequently rudimentary specification* (at least for a practical use case) of a cryptographic algorithm or protocol in the scientific literature makes transformation and secure implementation in a real service difficult and expensive. Notations are often very formal and the security assumptions and the correct parametrization not derived easily. Other identified inhibitors include the existence of *artificial requirements*, where cryptographic primitives are being brought forward, satisfying more requirements of cryptographic research, and of academic beauty—than being practically applicable in a real world application.

2 HCI Patterns as Integral Part of a Cloud Service Development Methodology

2.1 The PRISMACLOUD CryptSDLC Method

The construction of cryptographically equipped cloud services is a huge undertaking and requires contributions by and collaborations among many involved disciplines on different layers. To structure that process, and to enable a secure development process, the project PRISMACLOUD proposes a fourfold architecture [4], plus a proper methodology for the research and development activities required during cloud application development an all of these layers.

The architecture layers are:

- The **applications layer**—of the applications using (public) cloud services.
- The **services layer**, providing the cloud services to the end user applications. The services use cryptographic tools of the tools layer to implement security and privacy functions.
- The tools of the **tools layer** completely encapsulate the cryptographic primitives and protocols, including the correct parametrization, thus supporting a secure and effective use.
- The **cryptographic primitives' layer** containing the cryptographic primitives and protocols. Here the cryptographic research is being carried out.

The PRISMACLOUD CryptSDLC ("Cryptographic Software Development Lifecycle") defines the activities connected with traversing the architecture during cloud service development [5]. From the applications layer down, high-level requirements are derived and translated to more formalized language; such requirements are mapped to cryptographic models on the layer of cryptographic primitives and protocols. Cryptographic research is being carried out to fill gaps and provide the required functionalities. The algorithms and protocols are built into software, which is being structured as a tool to be used by a cloud services on an upper layer. Security and privacy is built into the tool *by design and by default* and in an optimal world, the practical security can also be quantified and (formally) proven. The tool is deployed, and the cryptographic capability provided to high-level applications through a cloud service. The CryptSDLC method is

based on conventional software development lifecycles, like Microsoft SDL, but augmented with steps specifically dealing with designing cryptographic systems [5].

2.2 Experts involved in the CryptSDLC

Table 1 lists for each architecture layer, which group of individuals needs expertise on that particular layer–plus at least in the adjoining layer above and below (if there is a layer above or below) during the development process [5]. For example, a tool designer with main expertise in the tools layer needs knowledge of the capabilities of the cryptographic primitives developed and configured in the primitives layer, as well as of the requirements postulated by the experts of the Services Layer. A service designer, on the other hand, only needs knowledge of the tools but no longer the detailed cryptographic knowledge of the cryptographic primitives and protocols layer.

Table 1. Experts, engaged on architecture layers

Primitives layer	Cryptographers
Tools layer	Tool designers, specialized software engineers, HCI experts
Services layer	Service designers, usability and HCI experts, cloud service providers and sub-providers (GDPR: “controllers” and “processors”);
Applications layer	Business model developers, general domain experts;
On several or all layers	Project communicators, IT security specialists

PRISMACLOUD maintains specific communication tools and mechanisms to support the layered development process governed by the CryptSDLC, as well as to support the diffusion of new paradigms and capabilities among prospective providers and end users of the proposed tools and services. These communication tools and mechanisms are applications of design patterns: *Cloud security and privacy patterns*, and *HCI–human computer interaction–patterns*.

2.3 Role of HCI Patterns

Design patterns on several levels provide communication functions during the development process. The patterns support the layered development process governed by the CryptSDLC. Cloud security and privacy patterns codify and explain the new paradigms and capabilities from cryptographic researchers to prospective service providers and end users. Specific HCI patterns guide the implementation of interfaces guiding the human computer interaction.

Cloud security and privacy patterns and HCI patterns are applications of design patterns. In similar structures, they are used to codify expert knowledge and requirements within a specific scope in a way that the information remains accessible across domains of involved actors. The main idea is that a design pattern shall “describe(s) a problem

which occurs over and over again (...) and then describe(s) the core of the solution to that problem, in such a way that you can use this solution a million times over (...)" [6]. This is done by describing the (empirical) background of the pattern, i.e. the "problem", and giving instructions for the "solution" in natural language in a framework of categories.

The concept was invented in Berkeley, CA, in the 1970s for application in architectural design [6] and has later on been modified for application in several information technology subdomains. The first application of design patterns in information technologies was in software architecture in the 1990s when object oriented design and reusability required efficient communication of complex issues across different domains of involved people [7]. Later on, the concept was used for the specification of security and privacy concerns in security and privacy patterns [8, 9], as well as for human computer interaction aspects in HCI patterns [10]. Since several years, there exist collections and catalogues of cloud security and privacy patterns specifically for modelling threats and solutions in the cloud context.

2.4 HCI Patterns Methodology

We will follow the structure of the HCI patterns as presented in [10], and additionally embrace the pattern with an overview section and a motivation section at the beginning, and a section testing and validation, showing how the pattern was elaborated and validated. In Table 2 we give a short definition of each of the categories used to describe the HCI patterns.

Table 2. HCI pattern categories

Overview:	Title of the pattern, including information on its maturity (i.e. how intensely it has been tested so far). For pattern HCI.P2 the overview contains a description of the underlying cryptographic primitive of redactable signatures to an extent required for the comprehension of the following HCI pattern.
Motivation:	Description, why the necessity arose for the particular pattern.
Problem:	Outline of existing problem; description of the context and applicability of the pattern.
Solution:	Describes the elements necessary to solve the given problem. Describes how the elements need to be arranged to achieve this goal. "The solution describes the elements that make up the design, their relationships, responsibilities, and collaborations" [7].
Use when:	Outline of the situation and context when the pattern is best applied in.
Use how:	Provide detailed insight into the way the solution is being achieved; provide detailed information for the developer and implementer (steps needed to achieve the solution);
Use Why:	Rationale as why the pattern is needed and where the benefit for the end user lies;

Related patterns:	Related patterns (in this collection, in other catalogues).
Testing and validation:	Description on how the testing was carried out and how the pattern was validated.

The HCI pattern categories grid is not to be seen as orthodox and fixed—for specific presentations and communication need, categories may be omitted, or other categories (as e.g. “GDPR context”, or “Standardization status”) could be added.

3 Example HCI Patterns for Cryptographic Applications in the Cloud

3.1 PRISMACLOUD use cases

In the PRISMACLOUD project, several end user applications were developed to demonstrate the capabilities and security benefits of the proposed cryptographic tools and services. A *Health Care Data Sharing Platform* uses a selective authentic exchange service to enable the minimization of data to be shared with third parties to the items actually required. The *e-Government IaaS (Infrastructure as a Service) Cloud* provides a redundant and highly secure backup solution in a hybrid cloud scenario. The three presented patterns were tested and are being applied in the *Health Care Data Sharing Platform* (HCI.P1, HCI.P2) and the *e-Government IaaS Cloud* (HCI.P3). The *Privacy Enhanced Simon* equips an existing application of the FP7 SIMON project (an implementation of a mobile application for prioritized parking for people with disabilities) with capabilities for effective privacy protection and data minimization of the involved end users. An *Evidence Sharing Platform* capable of deployment to a public cloud protects its information against curious cloud providers. The three HCI patterns are being applied in the Health Care Data Sharing Platform, as well as the e-Government application.

3.2 HCI.P1 Digital Signature Visualization

Overview. Digital Signature Visualization is a relatively mature pattern and is already practically applied in XiTrust’s commercial MOXIS solution[1]. It was user-tested in the PRISMACLOUD eHealth use case “Healthcare Data Sharing Platform”. The tests included two sets of users, the signers of the document (medical staff) and the redactors (users of the medical document: patients). Several results of the user test were incorporated into that pattern.

[1] Online (8.2.2018): https://www.xitrust.com/en/products/xitrust-moxis/. The MOXIS solution is currently available for qualified digital signatures, but not for malleable signatures. The identities are provided with trust service provider A-Trust, online (8.2.2018): https://www.a-trust.at/%C3%BCber-uns/en/

Motivation. XiTrust has been active in the field of digital signatures for more than 15 years and experience shows that users need a graphical visualization for digital signatures. Consequently, the graphical representations have been revised constantly over the last years. In principle, a digital signature does not need to be visualized, but then it would not be visible to the human eye. One option would be to simply apply the hash value of the signature to the document. However, this option has found only little acceptance. Thus, we implemented the possibility to upload an image into the XiTrust MOXIS digital signature solution, which shows a scan of the handwritten signature. In times when more and more people are doing their business on tablets and smartphones, a more flexible solution was requested. Therefore, we provide now also the possibility to create the signature visualization directly with a stylus or finger. Furthermore, it is possible to display the name of the signer, the date, the time and a short user-defined message under the visualization.

Problem. Prospective digital signers of documents need to see which document they are just going to digitally sign in an electronic document flow. Then signers need to be sure whether a digital document they are seeing on a computer display has already a valid digital signature attached to it. This is particularly of importance right after the process of signing a document (to confirm that the operation has been successfully carried out), but also in review of a past action (e.g. that the document has already been signed). Signature verifiers, i.e. the people receiving the signed document, need a straightforward and intuitive way to check the signature's validity (invalid signatures need visual representation). Additionally in the eHealth use case, when viewing the final document there are two types of signatures: signing the document with malleable signatures, and signing the redaction for accountability with a digital signature. Although the second (the digital signature of the redactor) could be valid, it does not necessary mean that the malleable signature (the first) is still valid; that is due to the dependency of malleable signatures on redaction rules (validity of the signature remains when redacting only allowed fields from the document).

Solution. Provide the user the required information in a way that resembles the common process of handwritten signatures on paper documents. Digital documents are rendered on the screen black on white, resembling printed documents. Digital signatures are represented by images of signers' handwritten signatures, and on the location where signatures would be expected on a paper document, i.e. at the bottom of the last page.

Use when. Use it in the generation and verification process of digital signatures in a digital documents flow.

Use how. Prospective signers shall be presented with a placeholder, indicating that a signature may be placed on a certain document. Such a placeholder has the form of a frame or box, which is empty (i.e. contains no image of a written signature) but contains information on who is entitled to sign the document (see Fig. 1). This can be a list of natural persons' names, or the name of a group, of which any individual member may sign (e.g. "medical doctor"). The placeholder shall be positioned at the bottom of a document, as this is mostly the case for handwritten signatures on paper. If there are

more than one signatures required on a particular digital document, several such placeholder boxes should be placed next to each other. Enabling the placing of the placeholder by the signer is not advised, as this tends to confuse the signer.

After the signature process itself has been triggered (and the proper authentication of the signer has been established) an image of the signer's manual signature is displayed in the frame (see preview in **Fig. 2.** Handwritten signature visualization). Therefore, the signer has immediate feedback that the signature process was successfully carried out. Likewise, a verifier can have an efficient signalization that a document is signed, and by whom.

The signer shall be given the opportunity to revoke a signature on a document that was erroneously signed, e.g. when digital signatures have to be created in a stressful working environment, e.g. in a hospital. The revocation should be easily achievable by the signer immediately after the signing process (probably within a defined time limit, or while one particular session is ongoing) and should not involve a lengthy and difficult procedure, as this is common in current digital signature applications.

Fig. 1. Signature placeholder mock-up. The QR code encodes metadata associated with the signer (e.g. identity) and the application (e.g. position of visualization in document, descriptor of business process related to document) in mixed electronic/paper document environments.

Use Why. Although digital signatures are intended as equivalent to handwritten signatures, they are merely bits of digital data that are not easily identifiable as a signature. A similar discrepancy exists between a document on paper to be signed, and electronic data, representing some document. Consequently, there is the problem of how both the digital document to be signed and the digital signature itself are visualized. We are here concerned with the latter problem, the visualization of the digital signature. The visualization of the space where a signer may 'place a digital signature (i.e. at the bottom of a 'virtual document'), provides for the signer an intuitive way to assess the quantity of data that the signer is about to digitally sign. The visualization of a valid digital signature by a box containing an image of the signer's handwritten signature provides, for both the signer and the verifier, an intuitive way to understand that a document is validly signed.

Fig. 2. Handwritten signature visualization

Related patterns. This pattern is used in several other HCI patterns having to do with digital signature applications, e.g. HCI.P2 Stencil for Digital Redaction (see below)

Testing and Validation. The visualization of signatures was tested as a part of the eHealth use case scenario walkthroughs on two sets of users: the medical staff who are the signers of the medical documents with malleable signatures, and the prospective patients who will be redacting the document, signing the redaction with digital signatures, and using their medical document for further purposes. We used low fidelity mockups[2] for the interface testing. In total there were 13 medical staff interviewed individually for testing the signing of redactable medical documents, and 5 focus groups for testing the redaction of signed documents and signing the redaction. The groups consisted of 32 participants of patient-users: 2 experts groups and 3 lay user groups.

Medical staff appreciated the visualization of the digital signatures, however raised their concerns regarding multiple signatures process across different departments in the medical facility. The signature placeholder was confused for the actual signature by some lay users, however it was noted by the participants that it is due to first time learnability encounter. Among the focus groups participants, views varied from appreciating the visual representation (non-expert users).

3.3 HCI.P2 Stencil for Digital Document Redaction

Overview. Redactable signatures provide a means for, within given boundaries, redacting parts or field blocks from digitally signed digital documents, without the signature losing its validity. In applications employing redactable signatures, one signer signs a digital document, from which a second user is able to redact some information (redacting in the sense of suppressing or "blacking out"), keeping in mind that redaction rules apply, i.e., not all fields are redactable. Meanwhile a verifier still can check the authenticity (versus the first signer) of the remaining information, as well as the authenticity of the redaction made by the second signer. HCI.P2 is also being applied in PRISMACLOUD in the eHealth use case "Healthcare Data Sharing Platform".

Redactable signatures are based on relatively recent cryptographic primitives, and there is (by the time of this document) not much end user experience available with the use of redactable signatures in digital signature applications. HCI tests have revealed that people tend to have problems to grasp the correct functionality and implications of a redactable signatures application and often preconceptions are uttered. A potential explanation of this phenomenon may be twofold: First, digital signatures in current digital signature applications are conventionally connected to the property that any modification destroys the validity of a connected digital signature. That situation is acerbated by the very name of "redactable signatures", which, being a technical term in the field of cryptography research, is misleading from an end user application point of view. This is because from an end-user point of view, it is not the signature that is being

[2] Balsamiq Mockups 3 by Balsamiq Studios LLC. online (8.2.2018): https://balsamiq.com/

redacted, but rather the signed electronic document. From an end-user perspective, e.g. “redactable authentic documents” would be a more suitable name.

Motivation. In our previous user studies, we have elicited and evaluated HCI and user requirements for malleable signatures [11,12]. It was clear that there is a need to communicate and facilitate the functionalities (redacting of documents) to the user using suitable and understandable user interfaces and metaphors. Furthermore requirements for redaction called for suitable metaphors and support for the user. Therefore, we have chosen the stencil metaphor for the process of redaction and developed mock-ups user interfaces for visualizing redaction of signed documents. To improve usability and ease human computer interaction, a practical application for the redaction of digital documents shall at any time provide an immediate feedback on which of the visible elements on the screen will be visible, or redacted from the final document.

Default settings for redactions complying with the privacy principle of data minimization and data protection by default (Art. 25 GDPR) are needed.

Problem. During redaction of digital documents, the redacting end user may lose control of which parts of an electronic document are redacted (and which parts will remain visible for a potential verifier). Some parts of the document may not be redacted without the digital signature losing its validity. An end user may redact too little or too much information, so that the remaining document either does not disclose minimal data or may no longer fit for its intended use.

Solution. The elements that are redactable within the predefined framework, i.e. the elements that can be redacted by a user without the initial signature losing its validity, shall be clearly indicated; users shall be given templates that propose redactions for a specific purpose, and indicate which fields may be redacted, without the document losing its suitability for the intended purpose in situations where it may be applicable.

Fig. 3: Icon for redacting fields in the document

In **Fig. 3**, the icon depicts the “blacking out” based on the stencil metaphor, which can be used in the user interface for choosing the functions to redact documents. However, for the process of redaction “greying-out” of fields should be used instead of “blacking out” for leaving the text to be redacted visible and thus helping the user to verify which parts of the text will be redacted and which will remain. Hence, greyed-out fields highlight the parts of the text that the user chooses to redact and thereby limit the information they would like to share.

In **Fig. 4**, mock-ups (for a redaction template that the users first have to choose) depict an overview of how a document would look like after redaction, where users get to see the greyed-out blocks of text to be redacted. Two different views marking either the text to be redacted or the text to be kept are offered. The actual final document without the markings is shown to the user (‘Document After’ view).

Use when. The Stencil for Digital Redaction should be used for the user interface during the redaction process of digital documents in redactable signatures applications, i.e. the Stencil for Digital Redaction shall support the redactor during the redaction process. Moreover, icons based on the stencil metaphor should be used for allowing the users to easily choose the redaction functions.

Use how. The digital document shall be presented on the screen resembling the printed document. At any time, and for all parts of the document visible on the screen, all potentially redactable elements shall be clearly indicated by displaying them inside a frame or box. Of these elements, not redacted elements, i.e. visible for a verifier, shall be displayed inside boxes with transparent background, while redacted elements, i.e. not visible for a verifier, shall be displayed in a box with grey background ('greyed-out'). Non-redactable text shall be displayed without a frame or box around it. At the beginning of redaction, users are given two options: one that users are clicking on the fields to be redacted and greyed out (View A in **Fig. 4**), the second is clicking on fields to be highlights and kept (View B). Both views will have the same end document result; it is mainly the mental model and preference of people selecting either hiding or showing information (**Fig. 4**). Each redactable section (i.e. each frame) shall have an adjoining button for toggling the redaction status (visible/not visible for a verifier) of that specific section (**Fig. 5**) User tests have proven an eye symbol as button as being convenient and effective for conveying the meaning of 'hiding' or 'making visible again' to the redactor.

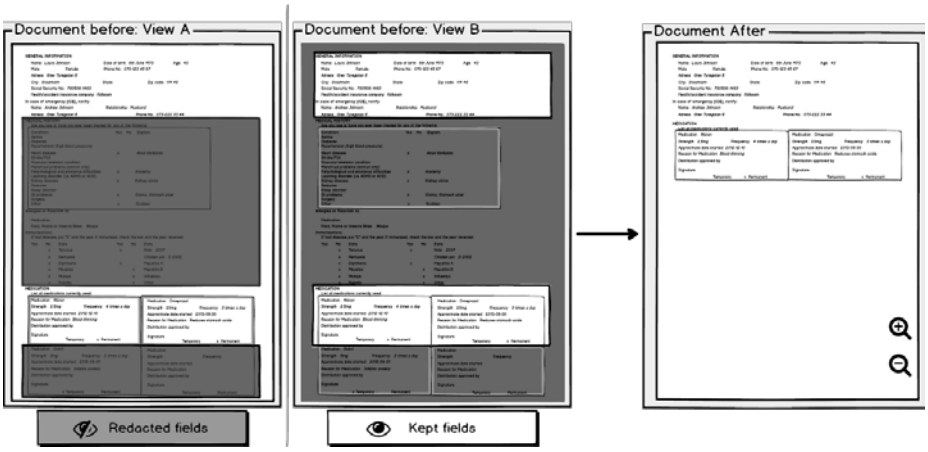

Fig. 4. Selecting redaction views

The redactor shall be presented a choice of templates for the redaction of documents for specific purposes. E.g. if the original document would be results of a lab test in an eHealth portal (signed by the lab or responsible medical doctor), a template could be provided for the end user passing on information to his or her dietician. The templates shall be designed to enforce Privacy by Default, i.e. in the lab use case the template should propose to the redactor to redact all test results not primarily needed for dietary counselling, i.e. the data proposed by the template to be redacted shall be put in already

greyed-out boxes. The information on the template currently in use shall be indicated on a separate portion of the screen at any time when the end user does the redaction.

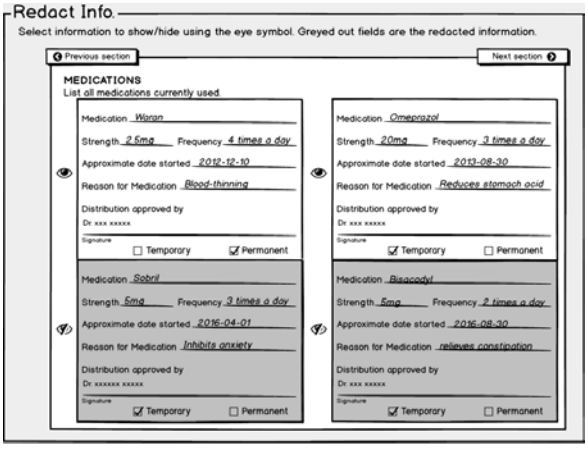

Fig. 5. Hiding/showing more information than the template.

Use why. HCI.P3 Stencil for Digital Document Redaction in combination with redaction templates guide a redacting user through the difficult process of digital redaction of signed documents. It helps the end user to grasp the consequences and implications of his or her actions during redaction and to enforce data minimization.

Related patterns. The accountability of a redactor for the effected redactions is usually implemented by a digital signature of the redactor. Use HCI.P1 Digital Signature Visualization for the digital signature process of the redactor.

Testing and Validation. The focus group study mentioned in HCI.P1 (**Sec.** 3.2) included the testing of redaction process by patient-users. Participants of all 5 focus groups understood the greying-out of fields in redaction process. In the overall view of document redaction, almost all participants chose View A (**Fig. 4**) as the suitable view for redaction, where they prefer to select further information to be greyed out rather than selecting information to be shown from the greyed-out view. Templates were perceived to be important part of redaction, since they act as a guide of redacting sensitive information by default; many participants indicated that they would rely on the templates for redaction. Therefore, it was concluded that there is a need for data protection certification (as promoted by the GDPR) for the template redaction specification for data minimization rights as well as setting the boundaries for data requirements of recipients, e.g., employers who would request more information than legally needed from their employees' documents.

3.4 HCI.P3 Secret Sharing Configuration Preferences

Overview. ARCHISTAR is a framework for secure distributed data storage and sharing in the cloud, it constitutes a system that applies Secret Sharing to a multi-cloud setting,

meaning that the user's data is divided into "chunks" which are distributed to separate clouds/storage nodes [13]. This implies that an incident at a single cloud/node will not cause the data to be lost, stolen or tampered with. Hence, it intrinsically protects data privacy and availability. When adopting a Secret Sharing (or Secret Splitting) scheme, there are two fundamental parameters that need to be considered: (1) ***n***, representing the number of "chunks" that data should be divided into. (2) ***k***, which constitutes the threshold of chunks required to reconstruct the data into its original state. A higher threshold makes data more protected against data privacy breaches because a higher number of cloud servers (least ***k***) would have to collude against the user (i.e., data owner) to restore the data without permission. However, a higher threshold also makes the data less accessible for not only unauthorized individuals, but also for the user themselves, as a data recovery would require the availability of a higher number of servers. As illustrated in [14], different configurations of ***n*** and ***k*** affect the availability of data chunks in a multi-cloud setting. The availability of cloud services is commonly expressed in percentage of uptime – or number of "leading nines" [14]. A typical cloud service availability rate is 99.9%, or three nines [13], which constitutes a downtime of 8.76 hours per year. From that point on, three main categories for setting up the configuration preferences are set and are focusing on: "Cost Minimization", "Data Confidentiality Maximization" and "Data Availability Maximization", which constitute the 3 packages/categories of this pattern. The use of the word "Maximization" should clearly indicate to the user that even though all kinds of configurations will, through the use of secret sharing, already protect the confidentiality and availability of the data, there are options to even strengthen or "maximize" these protections.

Motivation. 16 structured interviews were conducted to derive suitable ARCHISTAR configurations and guidelines for organizational/private use, and to identify trust factors, unique advantages and risks of ARCHISTAR that should be communicated to different user groups. The respondents were IT experts who are familiar with the notion of cloud storage and had previous experience of organizational and/or private cloud storage use. Based on the interview results, it was noted that setting up configurations of data chunks and locations required guidance and support. Compared to encryption, secret sharing was generally perceived as less secure against breaches, while some reasoned that it would constitute a greater protection against data loss. The majority of respondents argued that secret sharing would not single-handedly be a sufficient security measure for sensitive data in the cloud and a layer of encryption would be valued or required in addition, as they would not trust or would not want to rely on the non-collusion assumption of secret sharing and/or as they anyhow would internally use encryption for protecting sensitive data.

When asked how many chunks (n) their data should be divided into and what the threshold for reconstruction (k) should be, most respondents did not appear to understand (or put much thought into) how different values on k would influence the level of security and availability of data. In other words, the implications of different combinations of n and k might not be clear to the user and arbitrary values may therefore be selected, resulting in a less suitable configuration.

The perceived importance of cost was mixed among the respondents. Some argued that they would not use the solution if the expenditure would be too high, while others

though cost was a less crucial factor. However, regardless of the perceived significance, it was acknowledged that cost could have an impact on other key factors (such as security and reliability). This indicates that cost still may have be taken into consideration throughout the configuration process. However, other interviewees rather opted for data protection or for data loss preventions as their highest preferences.

Problem. Secret Sharing is a security measure for protecting both the availability and privacy/confidentiality of data. Various types of data may be stored/backed up in the cloud, all of which may involve different requirements in terms of the degrees to which Confidentiality, Integrity and Availability (CIA) are protected, which in turn can be influenced by the secret sharing configurations. . Particularly the sensitivity of data and the frequency in which it needs to be accessed by the user may determine which Secret Sharing configuration is appropriate. However, during the interviews some respondents found it difficult to give their personal/organizational data a particular classification in regards to the CIA triad. This suggests that the requirements and priorities should be specified in a different manner.

Solution. The user should be presented with three configuration preferences –"Cost Minimization", "Data Confidentiality Maximization – High Data Protection", and "Data Availability Maximization – High Data Loss Prevention"– which should be prioritized from most important to least important. Based on the priority, the user will be provided with recommended default settings and configuration options. The aforementioned categories have the following implications and trade-offs:

Cost Minimization: The expenses should be kept small by selecting cheaper cloud storage options. The pre-selection of providers should be dictated by the price of the cloud storage offering, rather than locations in different regions or jurisdictions. However, if "Data Protection" is the second-highest priority, locations at least one chunk needed for restoring the data should still be located in the EU or within the organization's private cloud for guaranteeing data protection in compliance with the GDPR. Similarly, if "Data Loss Prevention" is the second-highest priority, some pre-selected providers might reside in areas with a low risk of natural disasters to ensure that more than (***n***-***k***) chunks cannot be hit by the same natural disaster at the same time.

Data Confidentiality Maximization – High Data Protection: The data is sensitive and requires high confidentiality. Accordingly, encryption in addition to secret sharing should be a mandatory feature. Compared to the total number of chunks (***n***), a relatively high threshold for reconstruction (***k***) should be recommended to the user in order to minimize the risk of collusion attacks. The (pre-selected) cloud storage providers should be geographically located in EU and follow EU privacy legislation (and particularly the GDPR). If the second-highest priority is "Data Loss Prevention", the configuration of ***n*** and ***k*** should be adjusted so that a high availability rate still will be achievable with a high threshold (i.e. increase the total number of chunks). Also, the choice of providers will additionally be determined by the geographical distance between them to minimize the risk that more than (***n***-***k***) chunks can be simultaneously destroyed or be inaccessible due to the same natural disaster. If "Cost Minimization" is the second-

highest priority, the choice of providers will rather be influenced by the charged costs for the cloud storage offering.

Data Availability Maximization- High Data Loss Prevention: The data has high availability requirements. The option to add encryption should not be provided by default since it increases the risk of data being lost or inaccessible due to key loss issues. The recommended number of chunks (***n***) should be significantly bigger than the threshold for reconstruction (***k***) to ensure that the user will be able to restore the data if incidents occur at several storage nodes. That is, the user interface should suggest a configuration for a high availability rate (i.e. >99.9%). The pre-selected locations should have a sufficient distance between them to ensure that a single disaster will not cause multiple chunks (i.e. > (***n-k***)) to become inaccessible. Storage nodes in high risk areas for natural disasters should not be available options in the interface. If "Data Protection" is the second-highest priority, the threshold should be slightly increased to ensure that the data will be protected against a higher number of breaches. Locations that are compliant with EU privacy laws should mainly be suggested, which might limit the distance between storage nodes. Out of the chunks needed to restore the data, at least one should be located in the EU or even be part of the organization's private cloud. If "Cost Minimization" is the second-highest priority, the choice of providers will again rather be influenced by the costs charged for the offered storage.

Use when. Throughout the ARCHISTAR configuration process of data backups that the user intends to protect in the cloud with Secret Sharing.

Use how. The first step in the configuration process should involve data classification to indicate the user's/organization's needs. The user should be presented with three main categories "Cost Minimization", "Data Confidentiality Maximization" and "Data Availability Maximization" (see **Fig. 6**), which should be prioritized from most important to least important.

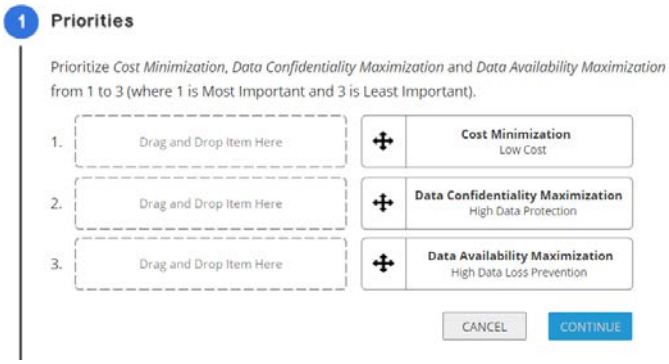

Fig. 6. Selection of the three categories according to priority.

Default settings should be suggested by an interface which can be manually adjusted by the user if desired. In particular, the user could change values for n and k, as well as

the selection of storage nodes (to which data chunks should be geographically distributed) on a map. The configuration process would subsequently be completed by proceeding to an "Overview" and a "Confirmation" page.

Use Why. To avoid any ambiguity regarding the Secret Sharing mechanism and to assist the user in creating the most suitable configuration for their intended data backup.

Testing and Validation (KAU). A first iteration of the interface was evaluated during 5 preliminary walkthroughs/interviews. The respondents constituted 1 Administrative Director at a municipality's IT department, 1 IT Security Coordinator at a university, and 3 IT experts of which one had several years of experience in an IT security consultant company.

While some respondents appeared to perceive the categories as sufficient for describing the user needs/requirements of the intended data backup, some questioned the category names. The distinction between "Data Protection" and "Data Loss Prevention" was not totally clear for all respondents. Moreover, one respondent desired more information about what "Cost minimization" implied (i.e. to what extent are the expenses reduced?).

Providing recommended default settings based on the user's priorities appeared to be seen as an appropriate solution. While some respondents still would like the *option* to change the total number of chunks (***n***) and the threshold for reconstruction (***k***), most of them seemed to prefer using default values provided by the system. Some respondents even argued that parameter ***n*** and ***k*** should not be presented by the user interface at all, since their implication would not be clear to the user. The notion of selecting cloud storage providers based on location was also received with mixed views. Some respondents thought that the user should be able to select specific data centers, others thought locations should be selected on a higher level of abstraction (e.g. country or continent) – or even be pre-selected by the system based on already signed contracts with providers.

In correspondence to these evaluation results, we have, as described above, introduced default settings (in particular for the values ***n*** and ***k***) for the next UI iteration that the user can adapt if they would like to. Besides, the names of the three categories were slightly changed or amended (see **Fig. 6**).

4 Assessment and Lessons-Learned of Practical Application

In a research project of 3.5 years duration, it was only after 3 years, that our first HCI pattern came into practical use during the project internal service and application development process, governed by the CryptSDLC methodology. The service architecture was roughly available one year into the project, while the CryptSDLC method was available as first draft after 1.5 years, and fully specified after 2.5 years. It was also then, that the first three HCI patterns were published as part of the HCI Guidelines[3].

[3] The respective PRISMACLOUD deliverable D3.2 „HCI Guidelines" is unfortunately marked *confidential* and thus not publicly available. An iteration D3.3 „HCI Research

Currently, the patterns are used in feedback cycles to application developers to adjust the user interfaces with results from the tested HCI patterns. To our experience, it would have been better to have the HCI patterns available at an earlier stage of the application development process (so that that they might have led to more *initial design* and less retroactive *adjustment*) but the obviously sequential processes of service definition / user interface development and testing / presentation of results as HCI patterns explains to some extent why the patterns came into play so late. So one result for similar projects would be to look into HCI pattern in an early as possible phase of a development process, and thus probably also rely on existing catalogues of HCI patterns, as e.g. given in [10], or in the patterns resulting from the PRISMACLOUD project[4].

In the PRISMACLOUD project, we are using design patterns also as cloud security and privacy patterns for the communication of requirements and capabilities during cloud cryptographic tools and cloud services development. Already in this area of application (earlier in the project), design patterns helped to communicate across domains of experts and stakeholders, as they later supported communication for improved HCI. The actual development of patterns requires a detailed study of the proposed cryptographic tools and services from several perspectives (from implementers, from cryptographers, from different end-user views, like e.g. these of doctors and patients, or organizations and customers, etc.). The pattern development helped to draw the focus from a technical approach to a user centered approach, which supports more the production of usable and accepted cryptographic applications.

As regards research on HCI concepts supporting usability and trust of cryptographically secured cloud services, the process of developing the HCI patterns supported empirical work on user experiences and perceptions of new paradigms, like redactable signed documents, social secret sharing, and privacy preserving authentication. The tested and evaluated HCI patterns provide the requirements for metaphors influencing the mental models, suitable to support end user acceptance and ease in the difficult field of cryptographically secured cloud services.

5 References

1. European Commission: Regulation (EU) 2016/679 of The European Parliament and of The Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2016. (online 20.7.2017)
2. Wästlund, E., Angulo, J., & Fischer-Hübner, S.: Evoking comprehensive mental models of anonymous credentials. In. Open problems in network security (pp. 1-14). Springer, Berlin, Heidelberg (2012).

Report“ with classification *public*, containing all the HCI patterns developed in the project, will be available by project end 31 July 2018 on the project homepage https://prismacloud.eu.

[4] Ibid. PRISMACLOUD D3.3

3. Lorünser, Th., Krenn, S., Striecks Ch., Länger, Th.: Agile Cryptographic Solutions for the Cloud. In e & i Elektrotechnik und Informationstechnik, September 2017, ISSN: 0932-383X (printed version) ISSN: 1613-7620 (electronic version) (2017)
4. Lorünser, Th., Slamanig, D., Länger, Th., Pöhls, H. C.: PRISMACLOUD Tools: A Cryptographic Toolbox for Increasing Security in Cloud Services. In: Proceedings of the International Conference on Availability, Reliability and Security (ARES 2016). IEEE, (2016).
5. PRISMACLOUD: Improved Guidelines and architectures for Secure Service Composition. Public deliverable D7.6 of the PRISMACLOUD H2020 project. https://prismacloud.eu, (2017).
6. Alexander C., Ishikawa, S., Silverstein, M.: A Pattern Language: Towns, Buildings, Construction. Oxford University Press, (1977).
7. Gamma, E., Helm, R., Johnson, R., Vlissides, J.: Design Patterns: Elements of Reusable Object-Oriented Software. Addison-Wesley. ISBN 0-201-63361-2, (1994)
8. Schumacher, M, Fernandez-Buglioni, E., Hybertson, D., Buschmann, F., Sommerlad, P.: Security Patterns - Integrating Security and Systems Engineering. John Wiley & Sons, Ltd. West Sussex, England, (2006).
9. Länger Th., Pöhls, H. C., Ghernaouti, S.: Selected Cloud Security Patterns to Improve End User Security and Privacy in Public Clouds. Privacy Technologies and Policy: 4th Annual Privacy Forum, APF 2016, Frankfurt/Main, Germany, September 7-8, 2016. Pages 115-132. Springer LNCS, ISBN 978-3-319-44760-5, (2016).
10. Fischer-Hübner, et al. (ed.): HCI Pattern Collection–Version 2. PrimeLife Deliverable D4.1.3 (2010). http://primelife.ercim.eu/images/stories/deliverables/d4.1.3-hci_pattern_collection_v2-public.pdf
11. Alaqra, A., Fischer-Hübner, S., Pettersson, J. S., & Wästlund, E.: Stakeholders' Perspectives on Malleable Signatures in a Cloud-based eHealth Scenario. In: HAISA (pp. 220-230). (2016).
12. PRISMACLOUD public deliverable D3.3 HCI Research Report. The report, containing the HCI patterns developed in the PRISMACLOUD project will be available by project end, 31.7.2018, through the project homepage https://prismacloud.eu.
13. Loruenser, T., Happe, A., & Slamanig, D. (2015, November). ARCHISTAR: towards secure and robust cloud based data sharing. In *Cloud Computing Technology and Science (CloudCom), 2015 IEEE 7th International Conference on* (pp. 371-378). IEEE.
14. Happe, A., Wohner, F., & Lorünser, Th. (2017, August). The Archistar Secret-Sharing Backup Proxy. In *Proceedings of the 12th International Conference on Availability, Reliability and Security* (p. 88). ACM

Acknowledgments. The authors' work is supported by the European Union Horizon 2020 research project № 644962 PRISMACLOUD "Privacy and security maintaining services in the cloud"; (2/2015-7/2018); online (8.2.2018): https://prismacloud.eu.