Proposal No. 830929
Call H2020-SU-ICT-03-2018

Project start: 1 February 2019
Project duration: 42 months

Cyber Security for Europe

D3.7

Usability Requirements Validation

Document Identification	
Due date	
Submission date	02 March 2020
Revision	1.0

Related WP	WP3	Dissemination Level	PU
Lead Participant	UNITN	Lead Author	Bruno Crispo (UNITN)
Contributing Beneficiaries	VTT, ULM, GUF, IRIT-UPS UMU, KUL, KAU, UM	Related Deliverables	D3.5, D5.1

Abstract:

This document presents the most relevant state of the art in usability requirements validation methodology and frameworks and puts them in relation to the security and privacy usability requirements that emerged in the context of the Cyber Security for Europe project. Then, it presents the most important research works about validation of usability in the security and privacy field, showing that there are many important choices and decisions to take while designing the validation process. Thus, in the end, the document presents some recommendations that ought to be considered while designing a security and privacy usability requirements validation process in general and in the specific context of the use cases related to CyberSec4Europe.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929.

The information in this document is provided as-is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Executive Summary

Deliverable D3.5 highlighted the importance of considering usability requirements in designing, implementing and deploying security and privacy mechanisms and solutions. This deliverable covers the important aspects of validating usability requirements.

The document presents an overview of the most important research and methodologies proposed to validate usability requirements. Some of them are well established and even covered by international standards. While such methodologies are not new, only recently they got wider acceptance in the software industry and elicitation of usability requirements and their validation is becoming common in the design of many software systems and solutions. Security and privacy do not make an exception; thus, the document cover also existing research and approaches used for validating usability in the specific case of security and privacy.

After studying existing validation methodologies and approaches, it is evident how important is the design of the validation process and the choice of the most appropriate testing methods and evaluation criteria among the many available. Choice that needs to be done based on the specific use case to which the validation applies. Based on the research and the expertise of the contributors, we thus provide six recommendations to be considered in designing a security and privacy usability requirements validation process.

1. Selection of appropriate dimensions or attributes to characterize usability requirements in the context of security and/or privacy.
2. Selection of suitable usability inspection methods during the design and development phase of security or privacy mechanisms pertaining to a system.
3. Selection of more than one approach for usability testing with users.
4. Creation of a usability traceability matrix to synergize the usability validation framework. Moreover, usability requirements validation should touch the design, development, and assessment phases.
5. Validation of usability requirements for authenticated encryption.
6. Validation of usability requirements for user authentication.

These recommendations can be applied both in the context of the CyberSec4Europe project and in other instances, where the security and privacy usability requirements need to be validated.

We conclude, presenting what are the key open challenges for usability evaluation that require more research and investigation.

Document information

Contributors

Name	Partner
Bruno Crispo	UNITN
Sandeep Gupta	UNITN
Kimmo Halunen	VTT
Marko Kompara	UM
Davy Preuveneers	KU Leuven
Philippe Palanque	IRIT-UPS
Matthias Beckerle	KAU
Célia Martinie	IRIT-UPS
Alba Hita	UMU
Sebastian Pape	GUF

Reviewers

Name	Partner
Luca Durante	CNR

History

Version	Date	Authors	Comment
0.01	2019-08-28	UNITN	1st Draft
0.02	2020-02-03	UNITN, VTT	2nd Draft
0.03	2020-02-13	UNITN	3rd Draft
0.04	2020-02-21	UNITN, UM, KU Leuven, IRIT-UPS, KAU	4th Draft
0.05	2020-02-24	UNITN, IRIT-UPS	5th Draft
0.06	2020-02-24	UNITN, UMU	6th Draft
0.07	2020-02-25	UNITN, GUF	7th Draft
0.08	2020-02-29	UNITN	Changed as per reviews

Table of Contents

List of Figures

List of Tables

List of Acronyms

A	**ATM**	Automated Teller Machines
C	**CCPA**	California Consumer Privacy Act
	CIA	Confidentiality, Integrity, and Availability
	CIO	Chief Information Officer
G	**GDPR**	General Data Protection Regulation
	GLBA	Gramm-Leach-Bliley Act
	GSM	Graphical Security Model
H	**HCI**	Human-Computer Interaction
	HIPAA	Health Insurance Portability and Accountability Act
I	**IM**	Instant Messaging
	IoT	Internet of Things
	ISO	International Organization for Standardization
M	**MOT**	Metaphors of Human Thinking
N	**NASA-TLX**	NASA Task-Load Index
	NUE	Non-usability Expert
P	**PGP**	Pretty Good Privacy
	PHI	Personal Health Information
	PUTQ	Purdue Usability Testing Questionnaire
Q	**QUIS**	Questionnaire for User Interaction Satisfaction
R	**RUKO**	Rapid Usability Kick-Off
S	**SME**	Subject Matter Experts
	SPARCLE	Server Privacy ARchitecture and CapabiLity Enablement
	SUS	System Usability Scale
	SUMI	Software Usability Measurement Inventory
U	**UBS**	User Burden Scale
	UEM	Usability Evaluation Methods
	UI	User Interaction
	UUX	Usability and User Experience
	UX	User Experience

Glossary of Terms

E **Evaluation**

Evaluation is the process of computing quantitative information of some key characteristics (or “objectives”) of a certain (possibly partial) design [98].

V **Validation**

Validation is the process of checking whether or not a certain (possibly partial) design is appropriate for its purpose, meets all constraints and will perform as expected [98].

Verification

Validation with mathematical rigor is called (formal) verification [98].

1 Introduction

In the last decade, we are witnessing several trends that are changing who the users of a computer system are and the shape and main nature of what a computer system is. With the advent of the Internet of Things and cyber-physical systems more and more devices of different form, shape and with very heterogeneous hardware comes equipped with computational and communication capabilities that were common in the past, only to laptops, personal computers, and servers. There has been a dramatic change in the systems' endpoints used nowadays by users to access computer networks and to use digital services and applications. These remarkable changes in the information technology landscape are getting reflected in both the public and private sectors. The CyberSec4Europe project has identified seven key domains, i.e., Open Banking, Supply chain Security Assurance, Privacy-Preserving Identity Management, Incident Reporting, Maritime Transport, Medical Data Exchange, and Smart Cities. The applications domains touched by these changes relate to all economic sectors from manufacturing to transports, from healthcare to home and building management touching cities and automobiles. As a consequence, the "users" of these systems, compared to traditional computer systems grew in number, types and age range. These paradigm shifts brought many changes, the most relevant one for the scope of this deliverable is the change these new devices and application contexts are bringing to the way users interact with these systems. New interaction metaphors have been implemented since most users cannot be assumed to even be computer literate and new methods of interactions (e.g., based on voice, biometrics, gestures, etc.) are replacing traditional ones (e.g., based on keyboard and monitor as standard input and output). The design of human-computer interactions is becoming pivotal for the success of many digital services and applications. In particular, a very important aspect is that of *usability* defined in the ISO 9241-11[1] standard as: "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use.". Thus, also security and privacy solutions and mechanisms as any other application have to address usability and consider the issue of selecting and validating usability requirements.

For many security and privacy mechanisms and applications, usability emerged as one of the dominant quality attributes or non-functional requirements apart from most common ones like *confidentiality*, *integrity*, and *availability*. Usability can be visualized as an intrinsic characteristic that impacts end users' decisions to use a security and privacy mechanism (generally referred to as *acceptance* [4]). It can be summarized with a phrase, there is no weaker security or privacy mechanism than the one that users simply do not use.

According to ISO 9241 [1], usability can be defined in terms of three orthogonal contributing factors, *i.e.*, *effectiveness*, *efficiency*, and *satisfaction*. However, effectiveness and efficiency must also be adequately captured and stored to meet usability criteria. It is important to note that usability has been defined by different authors highlighting some aspects that have not been captured in the ISO standard. For instance, Nielsen [5] defines usability through five dimensions: *learnability, efficiency, memorability, error tolerance* and *prevention* and *satisfaction*. The main difference is that Nielsen considers complex systems that require training operators before use, hence highlighting the importance of being resilient to user error and the importance of learnability. Consequently, attention is required to explore mechanisms that can validate usability requirements by using measurable dimensions [6], such as 1) ease of learning, 2) efficiency to use a security or privacy mechanism, 3) ease of memorizing, 4) understandability of a task and 5) subjective satisfaction, to design numerous security and privacy mechanisms.

1.1 Aim of the document

This document is part of the CyberSec4Europe project and its research efforts in Work Package 3. This deliverable apprises on usability validation methodology for security and privacy technologies discussed in Task 3.5 [2] and WP5 [3].

The document, thus, considers existing frameworks and standards that cover the issue of validation of usability requirements with emphasis and attention on those applicable to security and privacy usability requirements specified in WP5 and in the deliverable D3.5. It analyses what are the existing works and approaches to validate usability requirements highlighting the specific challenges and impediments that make difficult to design and validate usability requirements when it comes to security and privacy solutions. The document concludes with some recommendations that need to be considered in WP5 while design and validating a selected list of usability requirements specific to the use cases of the CyberSec4Europe project.

1.2 Structure of the document

Section 1 briefly explains the importance of usability in security and privacy mechanisms along with an overview of commonly used security and privacy mechanisms. *Section 2* covers the state-of-the-art in usability evaluation approaches and methods. *Section 3* presents the most relevant cases where usability requirements are crucial for the effectiveness of security and privacy mechanisms indicated in Task D3.5. Then, it focuses on eliciting the usability requirements demonstrated for each use case described in WP5. *Sections 4* present the methodology that can be applied for validation of usability requirements in security and privacy. *Section 5* presents recommendations that should be taken into consideration while performing the validation of usability requirements in some use cases selected in WP5. *Section 6* presents the open challenges. Finally, *Section 7* concludes the document.

This page has been intentionally left blank.

2 Background and state-of-the-art

This section describes the usability evaluation methods and taxonomy for determining usability attributes that are relevant for further research on usable security and privacy related to the CyberSec4Europe project. We also describe usability metrics to quantify usability and their optimization criteria.

2.1 Usability evaluation

Usability evaluation can be performed during the design and development phase of a system, i.e., formative evaluation, or based on users' studies during and after the use of the system, i.e., summative evaluation [18][19]. According to Fernandez et al. [20], usability evaluation methods (UEMs) can be classified into two different types, i.e., inspection methods and empirical methods. Typically, usability evaluation methods incorporate techniques, such as inspection, testing, or survey, for the assessment of usability objectives accomplishment for a system.

2.1.1 Usability inspection methods

In the usability inspection method, experienced practitioners like usability specialists and security professionals examine the usability aspects of a system, i.e., there is no participation of real end-users. The goal is to gather some useful insights by evaluating the designs or testing the systems related to various components that involve human-computer interaction (HCI). This can range from checking the level of achievement of specific usability attributes to heuristic evaluations for predictions of usability problems.

The popular usability inspection methods are Pluralistic Walkthrough [21][22], Heuristic Evaluation [23], Cognitive Walkthrough [24], Heuristic Walkthrough [25], Task–Centred Walkthrough [26], Metaphors of Human Thinking (MOT) [27][28], and Persona Based Inspection [29][30]. Table 1 describe how these usability inspection methods can be applied for validating usability requirements in security and privacy.

Method	Process
Pluralistic Walkthrough	1. Generate high-level design for security and privacy features. 2. SMEs to collect the usability requirements for activities which are directly related to end-users. 3. Prepare a usability validation checklist for a similar set of usability requirements as a result of discussion among the usability experts. 4. The usability validation checklist can be utilized during the final testing of security or privacy features.
Heuristic Evaluation	1. Usability requirements for a security or privacy feature can be compared with design principles (commonly referred to as heuristics). 2. One or more reviewers, preferably usability experts can identify where the feature does not follow the well-proven principles.
Cognitive Walkthrough	1. One or more usability experts can drill a security and privacy feature from an end-user perspective. 2. Here, the focus of the cognitive walkthrough can be to determine the feature's learnability for end-users of different age groups, skills, or familiarity with information technology.

	3. This can be applied to test the usability of critical systems, such as automated teller machines (ATMs) or ticket machines, etc.
Heuristic Walkthrough	1. The heuristic walkthrough combines the characteristics of heuristic evaluation, cognitive walkthrough, and pluralistic walkthrough. 2. Usability validation of a security or privacy feature can be performed in two steps. 3. In the first step, participants can raise "thought-provoking" questions. Subsequently, the evaluators require to work on tasks that are prioritized. 4. In the second step, evaluators can use a set of heuristics (existing principles) to dig out additional usability issues. 5. Generally, the task-based review enhances the heuristic review in each walkthrough.
Task-Centred Walkthrough	1. All the possible user tasks for security or privacy features are identified and described prior to the design and development of the features (they may be part of the requirements) 2. Several scenarios are produced from the list of identified tasks in order to cover the whole set of possible user tasks. 3. One or more reviewers apply the scenarios with the features or with prototypes of the features in order to identify which tasks are possible to be performed and which task are not possible to be performed (and thus to detect eventual effectiveness issues)
Metaphors of Human Thinking	1. Human factors play a vital role in using security and privacy mechanisms. 2. Human factors can be collectively defined as (lack of) awareness, (risky) belief, (risky) behaviour, (lack of) motivation, (inadequate) knowledge of technology [31]. 3. Metaphors of human thinking [28], such as habits, thoughts, awareness and associations, the relationship between utterances and thought, and knowledge can be used for identifying potential usability problems in a security or privacy feature surfacing due to human factors. 4. SMEs can collect these five metaphors from people of different age groups, professions, ethnicity, etc, by providing them a mock-up for security and privacy features. 5. Can help in preparing a checklist from early findings of usability requirements related to human factors 6. This checklist will help to validate usability criteria fulfillment during unit testing of each security or privacy feature.
Persona Based Inspection	1. Persona-based inspection requires the creation of a persona pool (e.g. a teenager, an elderly person). 2. The rapid usability kick-off technique (RUKO) was designed for non-usability experts (NUEs), to enable them to perform usability evaluation by selecting existing personas from the available persona pool [30]. 3. Usability experts can facilitate such workshops to perform the usability evaluation of security and privacy features. Figure 1 gives a high-level overview of the RUKO technique.

	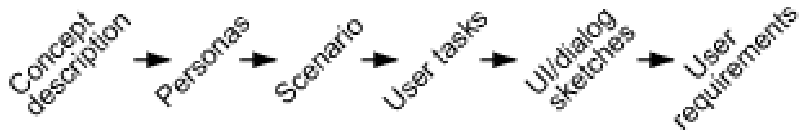 Concept description Personas Scenario User tasks UI/dialog sketches User requirements Figure 1: Rapid Usability Kick-Off (RUKO) [30] 4. The involvement of NUEs with different persona based on the needs, background, tasks, and pain points can increase the end-user focus in the evaluation of the usability requirement in security and privacy.

Table 1: Usability inspection methods

2.1.2 Usability testing with users

Usability testing approaches involve representative users to work on typical tasks using the system. The task execution result of each user is analysed to assess the system's friendliness. Testing methods for usability evaluation include Think Aloud Testing, Wizard of Oz, Coaching Method, Co-discovery Learning, Question asking protocol, Benchmark Testing, and Retrospective testing [32][33]. Table 2 describe how these usability testing with users can be applied for validating usability requirements in security and privacy.

Method	Process
Think Aloud Testing	1. A set of pre-defined tasks to validate the usability of a security or privacy feature can be created. 2. Testers can be encouraged to share their expectations, ideas, feelings, and satisfiability to execute the given tasks. 3. They can continuously verbalize their reactions while executing the given tasks. 4. They can elaborate general questions, like "What they are expecting?", "What more can be done to meet their thinking?", "Why some tasks are frustrating", etc.
Wizard of Oz	1. Wizard of Oz involves systematic observation under-stimulated conditions that can be applied to validate the usability requirements. 2. A tester can be explained with a scenario and requested to carry out the task. 3. Wizard (usability experts) can observe how a tester performs the given task to understand the usability issues. 4. The task performed by users can be recorded as well for future reference.
Coaching Method	1. Testers along with SMEs can participate to validate the usability of a security or privacy feature, together. 2. SMEs can guide the testers and answer their queries related to the feature under validation. 3. They can observe the testers in carrying out the task to find the usability gaps. 4. SMEs – testers' interaction can bring out genuine usability issues, which can be an ideal situation to envisage a usable privacy or security scheme.
Co-discovery Learning	1. Two testers can execute the tasks to validate the usability of a security or privacy feature together. 2. They can help each other to accomplish the task successfully without any external help on the feature design. 3. They can be encouraged to determine any usability issues as per the checklist, which can be obtained by using any one of the methods described in Table 1.

Question Asking Protocol	1. This is like “Think aloud testing” except here the SMEs can ask questions while the tester tests the security or privacy features. 2. Questions can include the testers’ thoughts, opinions, or easiness to use security or privacy features under test for their usability validation.
Benchmark Testing	1. Benchmark testing can utilize the previously available usability validation checklist or standards to validate the new security or privacy features. 2. This can be useful to validate the usability of security or privacy features update.
Retrospective Testing	1. In this method, usability experts can analyse the recording sessions of testers testing the numerous security or privacy features. 2. The major drawback of it is that it is extremely time-consuming.

Table 2: Usability Testing with Users

2.1.3 Questionnaire and survey methods

Questionnaire and survey methods can be categorised as empirical methods, which rely on capturing and analysing usage data from the real end-users. The software product (or a prototype) is distributed to real end-users to perform a predefined set of activities and the outcomes are recorded for detailed usability evaluation, later.

Empirical methods analyse the usability of a system by assessing 1) users' satisfaction to accomplish their objectives with the system and, 2) the mental model perceived by users after using the system for some time. In this category, Rating Scales, Satisfaction Questionnaire, and System Usability Scale (SUS) are some commonly used methodologies [34].

The System Usability Scale (SUS) questionnaire [35] is utilized to gather subjective assessments about the satisfaction dimension of usability of the proposed systems. The questionnaire consists of 10 questions or statements. The response to each question/statement is measured on a 5-point scale ranging from “strongly disagree” to “strongly agree”. The final SUS score ranges between 0 and 100, where a higher value indicates a more usable system. The System Usability Scale (SUS) template for the questionnaire and scoring is available online [36].

Some other questionnaires and survey methods for usability assessment are Software Usability Measurement Inventory (SUMI) [37], the Purdue Usability Testing Questionnaire (PUTQ) [38], Questionnaire for User Interaction Satisfaction (QUIS) [39], and the NASA Task-Load Index (NASA-TLX) [40].

Apart from usability evaluation, some other questionnaires especially focus on the evaluation of User eXperience. ISO 9241-210, the international standard on ergonomics of human-system interaction, defines User eXperience (UX) as "user’s perceptions and responses that result from the use and/or anticipated use of a system, product or service". Since user experience (UX) refers to a person's perceptions of a system’s aspects, in particular, utility and ease of use amongst others, it also allows an insight into the usability of a system, even though it is very subjective and includes the user’s *beliefs*, *attitudes*, and *emotions*.

AttrakDiff questionnaire [41] relies on a theoretical model that distinguishes pragmatic qualities (like perceived usability) and hedonic qualities (like aesthetics and stimulation). A trial version of this questionnaire is available online [42]. iScale [44] is a survey tool for the retrospective elicitation of longitudinal user experience data. This tool minimizes retrospection bias and employs graphing to define a process for the reconstruction of one's experiences. AttrakDiff [43] that measures how users personally rate the usability of a product can utilize the iScale tool to elicit change in product perception and evaluation over time.

2.2 Usability dimensions and attributes

Eventually, to determine usability requirements in security and privacy, end-users' expectations and preferences on these aspects are required to be captured and translated into technical specifications. Table 3 represents some of the dimensions for Usability and User Experience (UUX) evaluation taken from [45].

Dimensions	Source
Memorability, learnability, efficiency, errors/effectiveness, satisfaction	Classic Usability [46][47]
Likeability, pleasure, comfort, trust	Bevan et al. [48]
Anticipation, hedonic, support, impact, user differences	Ketola et al. [49]
Affect and emotion, enjoyment, fun, aesthetics, appeal, engagement, flow, motivation, enchantment, frustration, hedonic	Miscellaneous [50]

Table 3: Commonly available dimensions for UUX evaluation [45]

Alonso-Ríos et al. [51] define a taxonomy that aims at determining attributes to characterize a usability requirement. Figure 2 illustrates six attributes, i.e., *knowability*, *operability*, *efficiency*, *robustness*, *safety*, and *subjective satisfaction*.

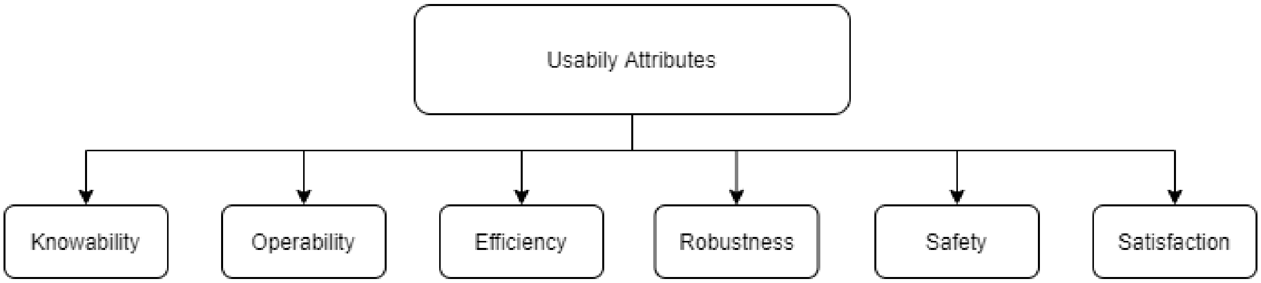

Figure 2: Taxonomy to assign usability attributes [51]

Knowability can be measured as a user's understanding, learning, and ability to remember while interacting with a system. D3.5 described *operability* as effectiveness that corresponds to the capacity of the system to offer means to the users to achieve their goals and *efficiency* as a number of resources (e.g. time, effort, actions) consumed by the users when achieving their goals. *Robustness* refers to a system's ability to cope with errors. *Safety* can be defined as a system's capacity to minimize the risk that a user may encounter while interacting with the system. *Satisfaction* refers to how pleasant it is to use the system.

2.3 Formal usability metrics to quantify usability and optimization criteria

An elegant way to validate usability is opened if easy to measure usability metrics are available. Having a complete set of such metrics would allow us to compare or optimize usability aspects automatically and reliable by aggregating metric scores or using them as optimization criteria.

While usability is influenced by the experience, preference, and ability of each individual user, there are some aspects of usability that are still universal. One usability goal, for example, is often to reduce complexity. One common way to find usability goals is to ask users about the difficulties or usability related tasks that they face and aggregate what the common problems are.

The next step is then to formulate such goals in a measurable way so they can be used as usability metrics. For the technical use of such metrics, formal definitions of such metrics are desirable.

Unfortunately, metrics are by definition abstractions of reality that lead to information loss. Therefore, it is important to validate such metrics by checking if optimizing them indeed improves the usability in the original task.

How this is done in the context of usable access control rule set configuration can be seen in [90]. With the support of related literature and a pilot study, informal usability goals are defined that are formalized, implemented into a test prototype, and successfully evaluated with two user studies.

The goals for access control rule set configuration from [90] there are the following:

G1. Allow no more than the owner wants to be allowed.
This goal defines that a resource should be accessed only by people that are intended to have access to it. Allowing more than intended is the result of less restrictive or missing access rules.

G2. Allow everything the owner wants to be allowed.
This goal states that a resource must be available to the people that are intended to have access to it. This goal basically complements G1. Allowing less than the intended access is the result of too restrictive access rules.

G3. A rule must not be fully covered by another rule of the same ruleset.
Redundant rules augment the complexity of an access control rule set by introducing new rules that are already covered by existing rules, thereby reducing the manageability of the access control system. Redundancies account for one of the reasons leading to errors in access control decisions.

G4. Two rules belonging to the same rule set must not conflict.
Conflicting access control rules impair the understandability of a rule set and often increase its complexity. Moreover, the resulting action from conflicting access control rules will depend on the implementation of the access control mechanism's conflict-resolution method. Deny precedence implies that Deny's rules take precedence over Allow rules. Allow precedence implies the opposite. The order of appearance in the rule set can be used to define the precedence too, i.e., the first fitting rule is picked.

G5. Minimize the number of ruleset elements.
Minimizing the size of rule sets reduces their complexity and facilitates visual inspection. After removing redundancies (G3) and (in some cases) eliminating conflicts (G4), the size of a rule set can be further optimized. One way to further optimize according to G5 is to grant rights based on attributes instead of unique identifiers (granting access rights for Students is one access rule – granting access right for individual students by using the matriculation number leads to number-of-students access

rules), by reducing the amount of attributes per rule and avoiding unnecessary rules. But contrary to G3, this procedure can lead to other conflicts, e.g., opening gaps for intruders.

G6. Minimize maintenance effort in a changing system.
Minimizing maintenance effort of an access control rule set whose access control policies are constantly changing requires a manageable and understandable rule set. Most of the changes in the ruleset happen when access control policies are modified, or when users are added to or removed from the system. Overfitting rule sets results in increased maintenance effort. Overfitting is used here according to its machine learning definition. Here it means that rule sets that perform well at the current state of the system may perform poorly if the system is modified.

[90] shows how these goals can be formalized and put into metrics and how these metrics can be used to understand and optimize rule sets.

In the context of this project, an approach like that would help to build a formal understanding of usability challenges in the context of cybersecurity. With the rise of machine learning and particularly Deep Learning, it will be possible to automatically learn metrics by observing the users and using their feedback to build models that can extract usability metrics. Similar mechanisms are already used to optimize the general usability of digital products. Unfortunately, it is not so commonly used to learn the security preferences of users.

This page has been intentionally left blank.

3 Usability Requirements as indicated by WP5 and D3.5

This section presents the usability requirements in security and privacy described in D3.5 [2]. Followed by the usability requirements identified for the different demonstration cases, namely, *Open Banking*, *Supply chain Security Assurance*, *Privacy-Preserving Identity Management*, *Incident Reporting*, *Maritime Transport*, *Medical Data Exchange*, and *Smart Cities*, mentioned in WP5 [3] of the CyberSec4Europe project. We also identified the attributes for each usability requirement to validate them.

3.1 Usability requirements identified in D3.5

D3.5 described security and privacy techniques related to 1) user authentication, 2) information visualization, 3) graphical security models, 4) encryption of communications, 5) identity and privacy management, 6) error reporting, 7) verifiable credentials, and 8) data privacy. This section describes usability requirements in relation to some of these security and privacy solutions and mechanisms.

User authentication is one of the most studied security properties in recent years and many new solutions and mechanisms have been proposed to implement it. Since all these mechanisms are meant for humans, usability is a critical requirement. In many application scenarios, the underlying authentication mechanisms deployed for *Login* or *Reset* should be friction-less, as well as, not add cognitive load to their users. In terms of usability, it means that these two tasks must be doable on the system (this corresponds to the effectiveness of the system), that they can be performed promptly and without being error-prone (efficiency) while ensuring the satisfaction of the user. Van Hamme et al. [52] emphasized that to protect a wide range of online systems, services, and contents - authentication, and authorization are critical components of a security layer. With an increase in consumer-base for smart wearable and mobile devices, they explained some emerging trends and challenges related to frictionless authentication systems.

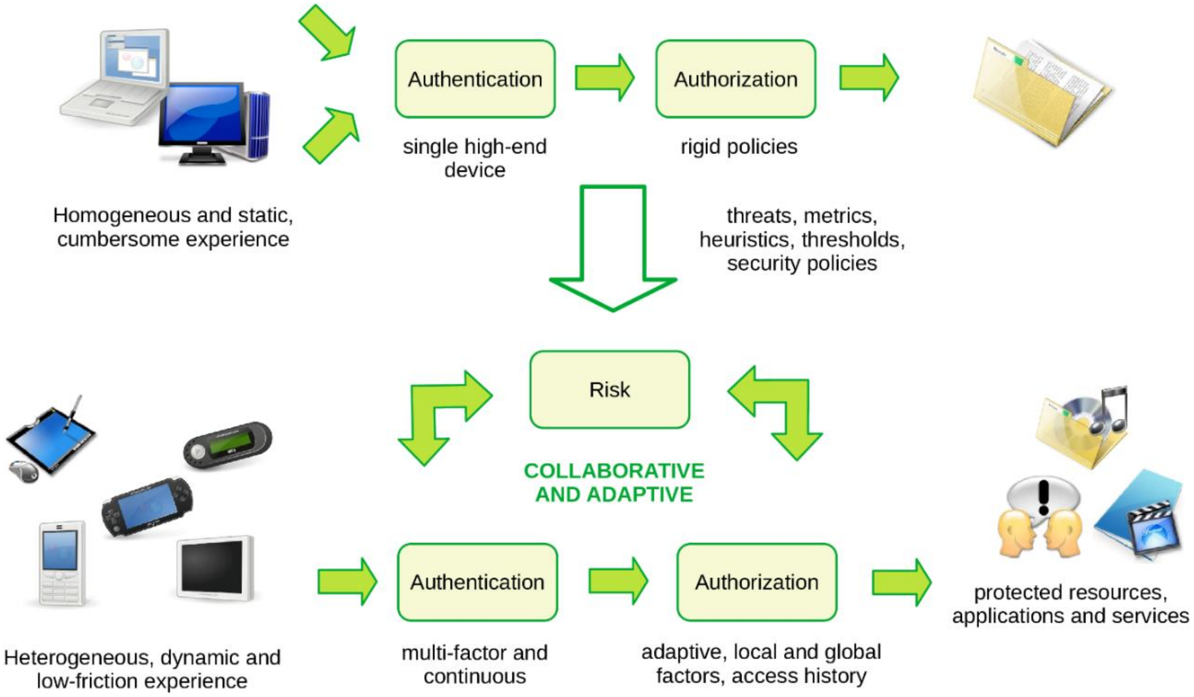
Authentication
Authorization
single high-end device
rigid policies
Homogeneous and static, cumbersome experience
threats, metrics, heuristics, thresholds, security policies
Risk
COLLABORATIVE AND ADAPTIVE
Authentication
Authorization
multi-factor and continuous
adaptive, local and global factors, access history
protected resources, applications and services
Heterogeneous, dynamic and low-friction experience

Figure 3: Collaborative, frictionless and adaptive multi-factor authentication [52]

Figure 3 illustrates collaborative, frictionless and adaptive multi-factor authentication suitable for smart devices. Furthermore, authentication or authorization to perform critical operations can be implicit, continuous, or risk-driven to enhance the usability of sensitive systems [53]-[55]

In software tools that perform security or privacy analysis of large-scale critical systems, usability aspects related to information visualization plays a vital role in their acceptance among the system administrators, security experts, and CIOs [14]. Freitas et al. [56] use the term data usability to describe the quality of information or quality of data in the context of information visualization applications. Data usability can be linked with three principles 1) data reliability, 2) minimal impact on data changing, and 3) support decision-making. They explain dimensions such as user's stress or fatigue level, tasks causing reduction to user's performance can be utilized to evaluate the information visualization usability.

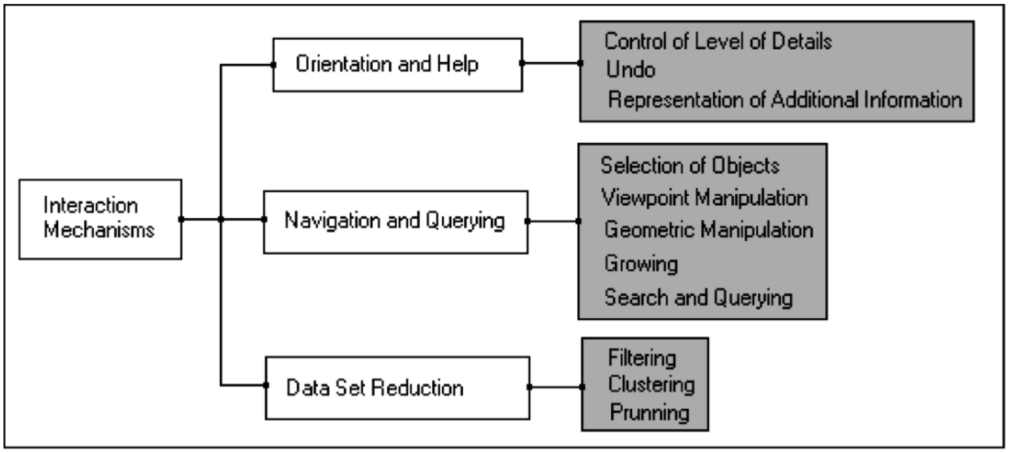

Figure 4: Criteria for the evaluation of interaction mechanisms [56]

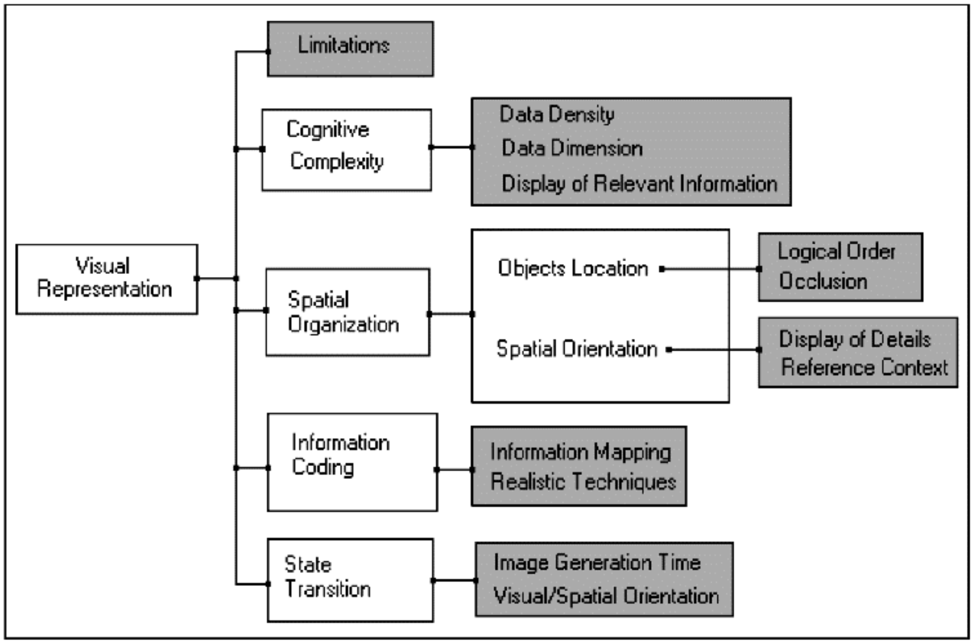

Figure 5: Criteria for the evaluation of visual representations of information visualizations techniques [56]

Figure 4 and Figure 5 illustrate the criteria for evaluating visual representations and criteria for the evaluation of interaction mechanisms, respectively. The greyed boxes describe the attributes to characterize the usability of visual representations elements.

Similarly, with growing concerns about privacy and the integrity of Instant Messaging (IM) [57], usable end-to-end encryption for IM applications becomes an essential security feature. Typically, usability problems with encryption tools involve poorly designed user interfaces, fundamental challenges of safe and scalable key distribution [14] [15]. Herzberg et al. [58] described the challenges associated with usable encryption, e.g., users often fail to properly encrypt using Pretty Good Privacy (PGP) encryption, etc. Thus, user-friendly end-to-end encryption mechanisms are required for secure and private data transmission [13].

Another area where usability plays a crucial role is in the design of security warnings and notifications. Security notification mechanisms must be proactive in nature [59]. They must provide essential information concisely, communicate consequences of the breach precisely, and guide users to take appropriate action to mitigate or minimize its effects, instantaneously. Furthermore, for critical systems like online banking, supply chain security assurance - the usability of errors and security breaches reporting mechanism must consider: 1) completeness of the errors or security breaches reported to end-users, and 2) how easily the end-users can interpret the errors or security breaches presented to them by the system. Bargas-Avila et al. [60] reported on the notion of usable error messages that include salient information such as 1) an error has occurred, 2) the name and information about the error, 3) the impact of the error on the work and data and 4) what the users have to perform to move on from this error state. Seckler et al. [61] have focused their attention on the location of error messages and on the importance of this location of detection and recovery.

End-users required to be made aware of various cyber-threats that they may encounter while using sensitive applications. Thus, efficient indicators to alert users for common attack patterns are necessary for usable security and privacy [62]. Similarly, a valid reason must be provided by service providers to access the resources, which can be easily approved, monitored, or revoked by users [31].

In the case of privacy, long and legalistic license agreements need to be replaced with short and precise communication regarding policies that do not take more than a few seconds of a user reading time [63]. Short audio or video clips can also be used to explain different policies to users that do not tend to frustrate the users.

Social networking platforms can provide user-friendly mechanisms to monitor their publicly available data that must meet the users’ expectations. Similarly, security-sensitive applications can ensure the users that no unfair use of their data, which has been collected for security or privacy purposes. For example, Uber can now predict where you’re going before you get in the car [64], which is a breach of users’ privacy and would be frustrating for a user to rely on on-demand and ridesharing platforms [65].

In the healthcare sector, a large amount of sensitive data, such as patients’ histories, patients’ treatment records from doctors, nurses, and professionals, is collected, stored (locally and on-cloud), and shared in their day to day operations. The usability evaluation of data privacy mechanisms, e.g., data anonymization, data minimization and differential privacy [66] is essential to safeguard people's interest.

3.2 Usability requirements identified in D5.1

In this section, the usability requirements of each demonstration case along with their usability attributes are described, which must be validated to achieve usability objectives specified in D5.1.

3.2.1 Open Banking

Table 4 presents the usability requirements for open banking taken from D5.1.

ID	Requirement	Description	Use Cases
OB-U01	Error Reporting	The system reports errors and security breaches timely and automatically.	OB-UC1
OB-U02	Open banking usability	The proposed network will be expected to support open banking usability characteristics, including real-time and high availability requirements.	OB-UC2
OB-U03	Verifiable credentials	Verifiable credentials remove the need for users to have countless usernames and passwords, to carry physical credentials around with them, and to enter identity attributes and credit card details manually into websites.	OB-UC3

Table 4: Usability requirements for open Banking

Usability attributes for open banking requirements are described using the taxonomy as shown in Figure 6.

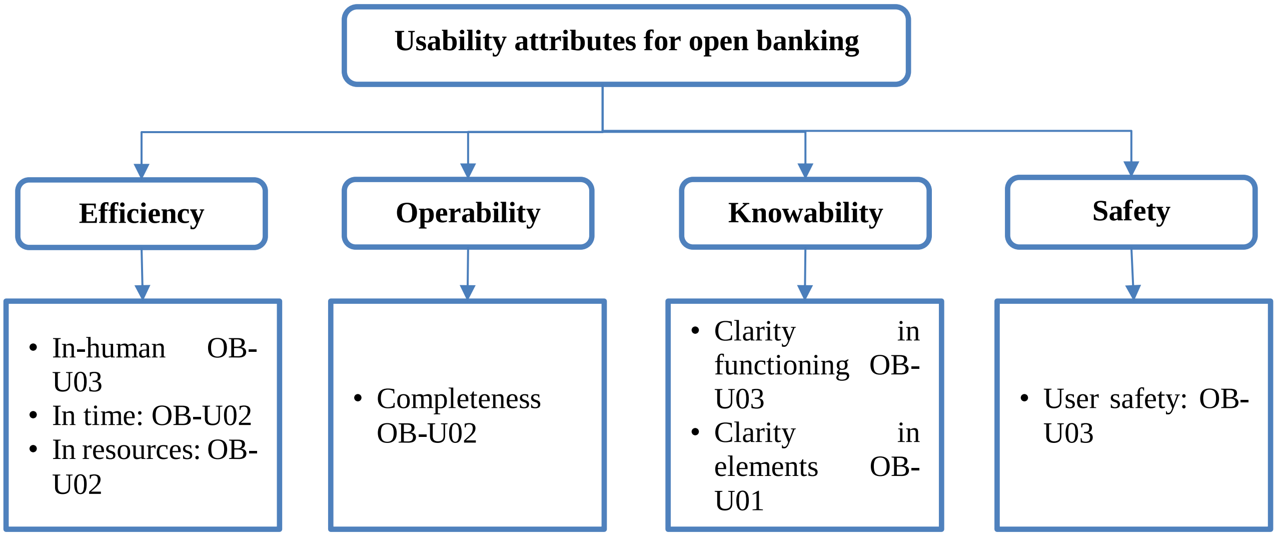

Figure 6: Usability attributes for open banking

3.2.2 Supply Chain Security Assurance

Table 5 presents the usability requirements for supply chain security assurance taken from D5.1.

ID	Requirement	Description	Use Cases
SCH-U01	NoA	The system reports errors and security breaches timely and automatically	SCH-UC1, SCH-UC2

SCH-U02	Config	The system allows all partners to manage and configure the underlying platforms and their policies in a secure, usable, and consistent way.	SCH-UC1

Table 5: Usability requirements for supply chain security assurance

Usability attributes for supply chain security assurance requirements are described using the taxonomy as shown in Figure 7.

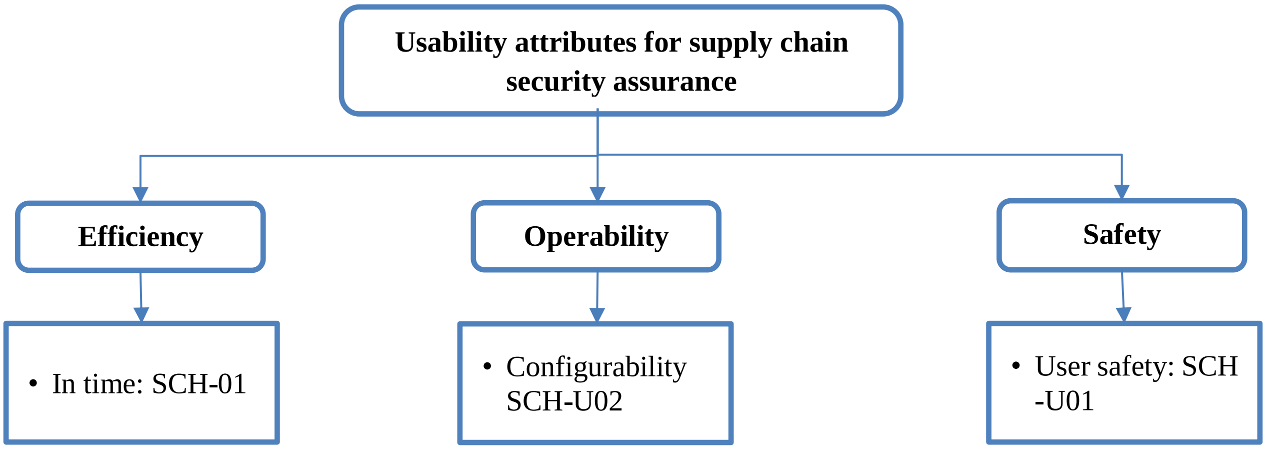
Usability attributes for supply chain security assurance
Efficiency
Operability
Safety
• In time: SCH-01
• Configurability SCH-U02
• User safety: SCH -U01

Figure 7: Usability attributes for supply chain security assurance

3.2.3 Privacy-Preserving Identity Management

Table 6 presents the usability requirements for privacy-preserving identity management taken from D5.1.

ID	Requirement	Description	Use Cases
IDM-U01	Perfo	In order to increase usability and future market penetration, all developed solutions must be highly efficient. In particular, the time needed for the cryptographic operations and necessary communication when receiving or presenting a credential should not exceed 1000ms, even when stored on a commodity smart card. Furthermore, all user data must be presented in a sufficiently compact form to fit on such devices.	All; particularly, IDM-UC3
IDM-U02	Usab	While high privacy and security guarantees are appreciated by end-users, broad adoption of security and privacy technologies requires a high level of invisibility towards the end-user. For instance, canonical or well-known usage patterns should be affected as little as possible, as little additional steps as necessary should be introduced, not non-commodity hardware should be required, or the responsiveness and efficiency of the overall system should not be negatively impacted by the new solutions.	All; particularly, IDM-UC3
IDM-U03	Transp	All privacy guarantees but also the remaining privacy risks shall be communicated to the user in a highly transparent way, e.g., regarding	All; particularly, IDM-UC3

		metadata privacy but also regarding the existence of a third party that may revoke anonymity. This is necessary to enable users to take informed decisions about their private data.	

Table 6: Usability requirements for privacy-preserving identity management

Usability attributes for privacy-preserving identity management requirements are described using the taxonomy as shown in Figure 8.

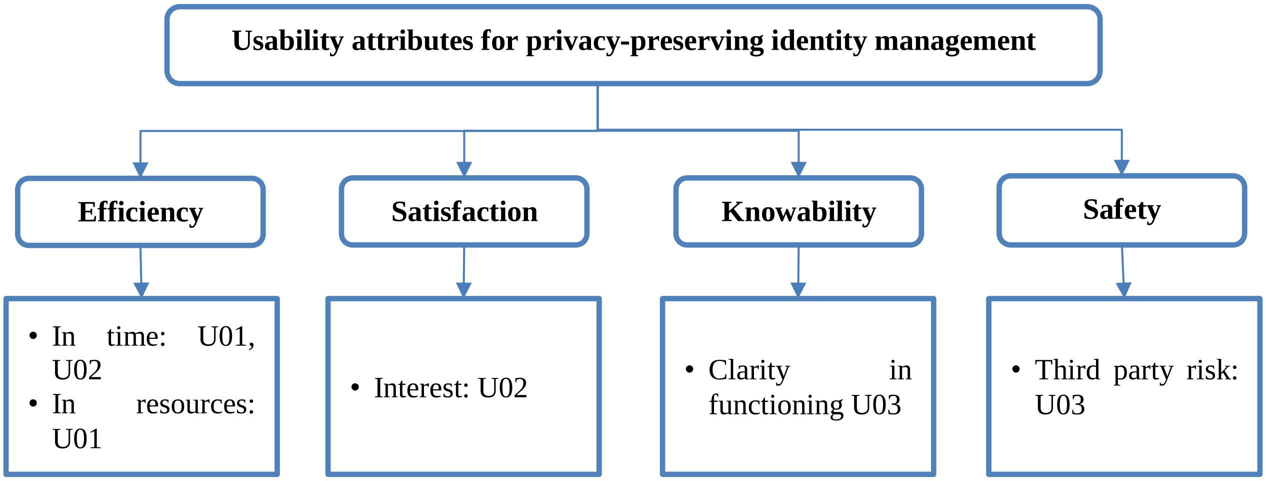

Figure 8: Usability attributes for privacy-preserving identity management

3.2.4 Incident Reporting

Table 7 presents the usability requirements for incident reporting taken from D5.1.

ID	Requirement	Description	Use Cases
IR-U01	Usab	The GUI must be user-friendly, offering a better user experience, improving the response times and facilitating the navigation between several functionalities.	IR-UC1, IR-UC2, IR-UC3
IR-U02	Usab	The GUI must request to the operator all the required information about the incident, including the impact assessment, through different questionnaires.	IR-UC1
IR-U03	Usab	The questionnaires presented to the operator must be self-adaptive, customized depending on the information already provided about the incident.	IR-UC1

Table 7: Usability requirements for incident reporting

Usability attributes for incident reporting requirements are described using the taxonomy as shown in Figure 9.

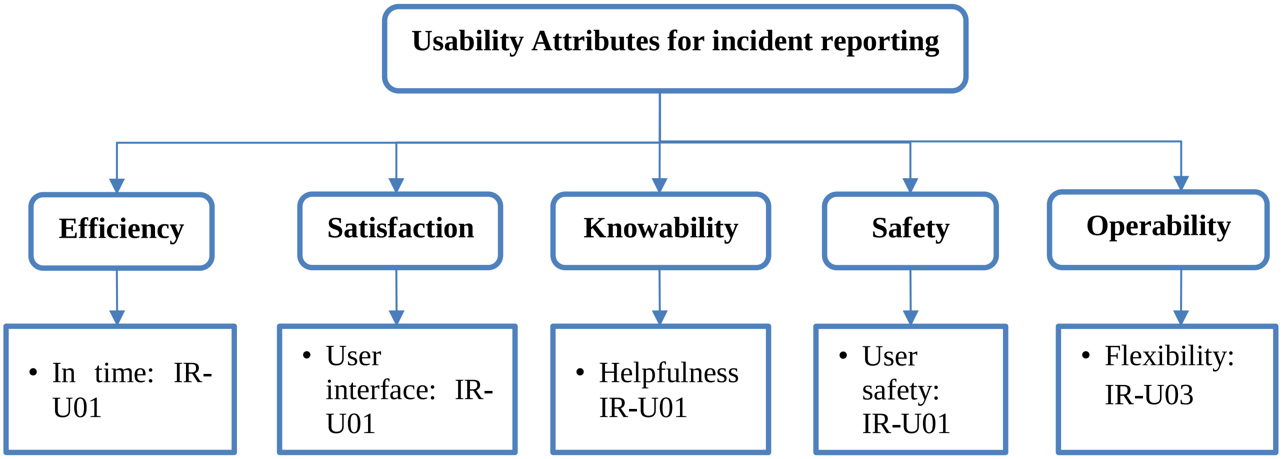

Figure 9: Usability Attributes for incident reporting

3.2.5 Maritime Transport

Table 8 presents the usability requirements for maritime transport taken from D5.1 [38].

ID	Requirement	Description	Use Cases
MT-U01	Usab	Entities that are not familiar with cybersecurity (non-experts) should be able to provide security-related inputs.	MT-UC1 MT-UC4
MT-U02	Usab	There must be ease of applying frequent software security updates to most vessels.	MT-UC2

Table 8: Usability requirements for maritime transport

Usability attributes for maritime transport requirements are described using the taxonomy as shown in Figure 10.

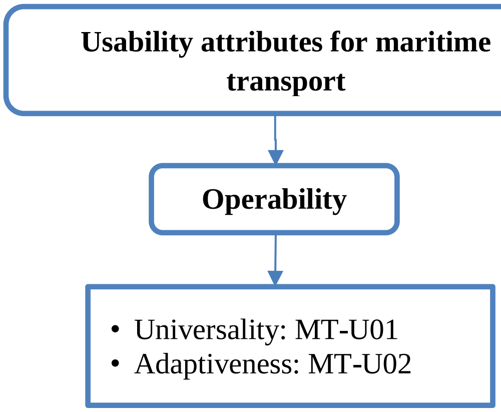

Figure 10: Usability attribute for maritime transport

3.2.6 Smart Cities

Table 9 presents the usability requirements for smart cities taken from D5.1.

ID	Requirement	Description	Use Cases
SMC-U01	Usab	Solutions should be designed to be used by non-IT people with a lack of information technology knowledge.	SMC-UC1, SMC-UC2, SMC-UC3,

			SMC-UC4, SMC-UC5, SMC-UC6, SMC-UC7

Table 9: Usability requirements for smart cities

Usability attributes for smart city requirements are described using the taxonomy as shown in Figure 11.

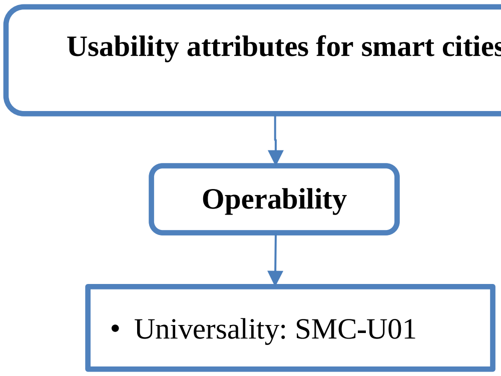

Figure 11: Usability attributes for smart cities

This page has been intentionally left blank.

4 Methods to validate usability requirements in security and privacy

C*onfidentiality*, *integrity*, and *availability* are the most desired attributes for an information system from an end-user security and privacy perspective. However, with the proliferation of connected IoT ecosystems, such as driverless vehicles, smartphones/wearables, smart homes/offices/cities, a security mechanism without fulfilling usability criteria will likely be less acceptable by their consumers. Consequently, usability becomes an equally significant quality-attribute along with more traditional and technical security goals (e.g., CIA) [16][17]. This section presents some usability validation frameworks/methodologies that can be applied in security and privacy. Subsequently, we describe relevant usability validation methods for selected use cases of D3.5.

ISO 9241-11:2018 [74] describes a quantitative method to determine usability for a system. As illustrated in Figure 12, these standard outlines some metrics, such as effectiveness, efficiency, satisfaction, that can be utilized to measure users' specific goals to meet their usability requirements.

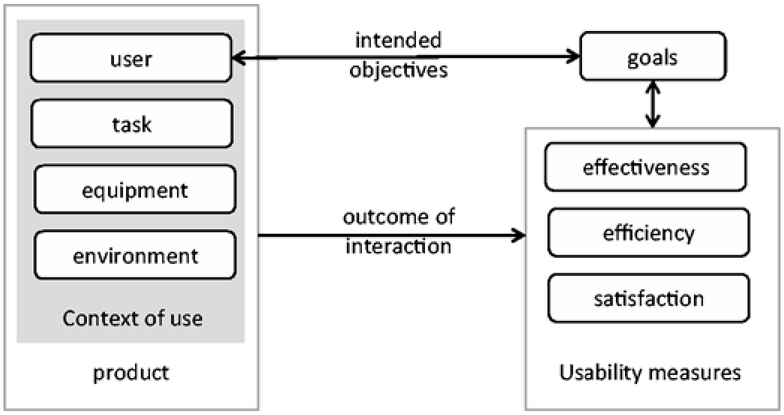

Figure 12: ISO 9241-11:2018: Usability framework [74]

A similar approach can be applied to validate the usability requirement in the context of security and privacy. These mechanisms can incorporate the early involvement of end-users throughout all steps of the requirement gathering and high-level design creation phases to generate a granular usability checklist [75]. Finally, during the integrated testing of the mechanism, the same checklist can be used to validate if the usability requirements have met or not.

The User Burden Scale (UBS) can be applied to evaluate usability requirements in security and privacy. UBS is a 20-item scale with 6 individual sub-scales representing each construct [76]. The 6 unique constructs of user burden: 1) difficulty of use, 2) physical, 3) time and social, 4) mental and emotional, 5) privacy, and 6) financial. Automated methods such as video recording or AI-driven techniques to record various UBS constructs can be applied to validate usability requirements while a user interacts with a security or privacy mechanism.

Grigera et al. [77] described an automated strategy for usability smell recognition based on the analysis of user interaction (UI) events that aim to provide automatic advice about usability smells of user interaction for web applications. Using similar cues, usability smells approach can be generated for empirical validation of usability requirements in security mechanisms.

Heuristic evaluation is a usability inspection method that is widely used to identify usability problems [19]. Quinones et al. [78] presented an exhaustive review of 73 studies related to usability heuristics for specific domains and methodologies including security. They presented numerous studies to develop usability heuristics followed by approaches or methodologies that are used for their creation and validation. A similar approach can be adopted for usability requirements in security and privacy.

Kainda et al. [79] presented a security-usability threat model that focuses on a legitimate user who has no intention of breaking the system. As shown in Figure 13, the model identifies factors that are related to either usability or security and factors that are related to both. They proposed for a successful evaluation, both security and usability factors must be measurable.

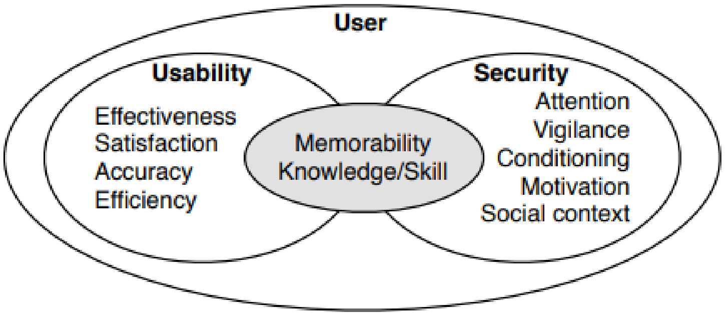

Figure 13: Security-usability threat model [32]

Usability		Security	
Factor	**Measurable metrics**	**Factor**	**Measurable metrics**
Effectiveness	Task success	Attention	Failure rate
Satisfaction	Willingness to reuse	Vigilance	Failure rate
Accuracy	Success rates	Conditioning	Failure rate
Efficiency	Completion times, number of clicks/touch/buttons pressed	Motivation	Perceived, benefits, susceptibility, barriers, severity
Memorability	Recallability	Memorability	Recallability
Knowledge/Skills	Task success, errors, mental models	Knowledge/Skills	Task success, mental models
		Social context	Social behaviour

Table 10: Measurable metrics [79]

Table 10 summarises the measurable metrics for each of the factors in Kainda's threat model. For a specific usability or security criteria, these measurements are crucial for comparative analysis and basic quantification. Therefore, to validate the usability of a system one or more of these factors can be evaluated.

4.1 Usability validation in selected use cases of D3.5

4.1.1 User Authentication

In the case of authentication mechanisms, usability is one of the dominant attributes that influence users to accept an authentication scheme [67]. There has been some work on frameworks for evaluating and validating a variety of security requirements.

Bonneau et al. [68] proposed a framework for evaluating web authentication methods. In their framework, they consider usability as one feature to be evaluated. They list eight different usability benefits in the context of web authentication methods. Their framework also considers deployability and security benefits. This framework has been extended to evaluate a wider range of authentication methods by Halunen et al. [69]. Their framework also considers authentication methods, but in a wider scope so not only limited to web applications. Their framework contains five categories and one of these is usability with seven attributes. Another category of attributes is non-intrusiveness, where they list four attributes. These are somewhat linked to usability as well.

Both frameworks have been used to evaluate authentication methods. The framework of [68] has been used also for validation of authentication methods as in [70]. The research also shows that in both studies some trade-offs between usability and security can be seen. However, these frameworks are very much directed towards an authentication context. Thus, they are not directly applicable to other domains. These could be used to validate usability requirements in the authentication context, but more general applications will require some modifications and further work and research.

Several security schemes [71]-[73] leverage the SUS survey to evaluate the usability of their proposed user authentication schemes. The System Usability Scale (SUS) is a comparatively quick, easy and inexpensive method to validate the usability of a security scheme.

4.1.2 Encryption techniques

The usability of encryption techniques gets affected by parameters, such as poor interface designs, transparency, key length, key management [12][13][80]. The usability validation methods for end-to-end encryption techniques can include evaluation of interface designs, distribution methods for public keys.

Herzberg et al. [58] evaluated the usability of popular IM applications, namely, WhatsApp, Viber, and Telegram, based on usable-security principles. Their evaluation determined that 1) users want protection from rogue operators, 2) users are unaware of opportunistic mode, 3) the authentication ceremony is not usable, and 4) users fail to authenticate upon reset. The authors suggested usability validation techniques must consider human nature and habits that can be determined by involving end-users of different age groups to elicit the usability of security and privacy requirements.

4.1.3 Identity and privacy management

Brodie et al. [81] designed and prototyped a privacy management workbench that can assist organizations to create and manage privacy policies. They further mentioned that organizations need usable methods to ensure that the information policies they put in place are enforced correctly without negatively affecting their business processes. They conducted scenario-based usability walkthrough sessions for the assessment of their privacy policy management workbench called SPARCLE (Server Privacy ARchitecture and

CapabiLity Enablement). These usability walkthrough sessions were performed by SMEs responsible for the creation, implementation, and auditing of privacy policies within large organizations in the domains of health care, banking, and government.

Organizations inform users about their data collection and sharing practices by the means of privacy policies. Kelley et al. [82] proposed and evaluated the development of "privacy" labels, the concept that they borrowed from nutritional labels on packaged food. Their evaluation has shown that presenting privacy policies in the form of Privacy labels enhances usability as it simplifies the understanding of privacy policies by consumers. Natural language processing techniques can be used to create a model that can extract information about data collection in privacy policies and validate them in an automated manner [83].

Harkous et al. [84] designed a framework, Polisis, that leverages deep learning for automated analysis and presentation of privacy policies. Polisis can break down the privacy policies into smaller and self-contained fragments of text, referred to as segments. Then, it automatically annotates, with high accuracy, each segment with a set of labels describing its data practices. This framework can be used to deal with the breadth and depth of privacy policies by enabling scalable, dynamic, and multi-dimensional queries on natural language privacy policies. Further, it can be used to validate privacy policy labels or segments that organizations generate to enhance the usability of their privacy policies from the users' perspective.

4.1.4 Data privacy

Recent privacy regulations, such as General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), or California Consumer Privacy Act (CCPA), mandate an increase in responsibility and transparency around personal data use and storage. Organizations that collect, process, use, and share data of their users are required to ensure that they have readily accessible privacy policies to disclose how they will collect, store, use, or share their users' data along with the exact purpose. Apart from informing users about their data that has been collected and shared, organizations must facilitate user-friendly interfaces for users to access, delete, or opt-out data, as well. To comply with data privacy policies and standards, organizations are bound to incorporate methods to safeguard users‘ privacy.

Often, Personal Health Information (PHI) of patients can be viewed, created, edited and even eliminated without the patient's knowledge and purpose discloser by the professional. However, recent data protection legislation enforced patients' consent and audit trails. Reis et al. [85] evaluated the usability of their proposed tool, MyRegister, by performing the SUS survey.

4.1.5 GDPR compliant user experience

The purpose of data protection regulations is to balance the controller's need to process personal data and the protection of the data subject's privacy. The main guiding principles of the GDPR are lawfulness, fairness, and transparency. Lawfulness simply requires that personal data is processed in a lawful manner. In addition to requiring lawful processing of data in a general sense (common law obligations, whether criminal or civil), GDPR also requires a valid legal reason for processing (including collecting) of personal data. These include consent, contract, legal obligation, vital interests, public tasks, and legitimate interests.

Fairness extends the lawfulness to include how the use of the data could affect its owner. Fairness limits the processing of personal data to what people would reasonably expect and not use it in ways that would have an unjustified adverse effect on them. An example of this would be an insurance company collecting personal data for enrolment in a prize competition, but without disclosing it also use the collected data to adjust the insurance rates of individuals. In this way, fairness depends partly on how the data is obtained – if anybody was misled or deceived when giving their personal data, it is unlikely to be fair. Nevertheless, personal data may sometimes be used in a way that negatively affects an individual without this necessarily being unfair (for example, tax collection). Personal data may not be processed for purposes not disclosed to the data subject. The data subjects must be informed of the processing of personal data in an intelligible manner and it may not be misleading or manipulative.

The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and intelligible (easy to understand)[1]. These communications must be done in a clear and plain language. Legalese, long or overly complicated texts are not acceptable. This is especially emphasized when addressing children. Transparency also includes the easy accessibility of the information organizations must provide to the data subjects. In the name of transparency, the data subject should be informed about what personal data is being collected, for what purpose it is being collected, how it is going to be processed and what rights do they (the data owner) have. Transparency also applies to data not collected directly from data subjects. Transparency is fundamentally linked to fairness because fairness without transparency is not possible.

The combination of lawfulness, fairness, and transparency provides or at least improves the usability of the given information. The GDPR ensures organizations will provide accurate information in a manner that is easier to understand and might bring more people to actually read it, knowing that the information will be presented in an understandable and consistent way, without hiding what they do with their data. This improves the usability of the received information for the data subjects. This is especially beneficial when data subjects have a choice of forming some type of a relationship (join a service, subscription, etc.) and fairness and transparency of information allow the user to make a more informed decision.

Under the principle of transparency and to aid in the usability and the user-friendliness of conveying all the important information (as defined in the Articles 13 and 14 of the GDPR) to the users the GDPR envisioned the use of standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing[2]. The icons should (where possible) also be machine-readable to allow further augmentation. The power to provide the standardized icons was given to the European Commission[3], however, as of the time of this document, there has been no development on this front from the European Commission and to the best of our knowledge no such icons are used anywhere.

GDPR requires a Data Protection Impact Assessment, which is a process designed to systematically analyse, identify and minimise the risks associated with the processing of personal data. This assessment is, however, not designed to validate any specific usability requirements. Article 29 Data Protection Working Party has published its proposed guidelines on transparency [86], which were in turn endorsed by the European Data Protection Board [87].

[1] Recital (58) of the GDPR

[2] Recital (60) and article 12 paragraph 7 of the GDPR

[3] Recital (166) and article 12 paragraph 8 of the GDPR

The recommendations suggest separating the privacy-related information from other information available to the user (e.g. disclaimers, contractual provisions, etc.). The information should be freely available, and the user should not have to take active steps to find this information. It is also desirable for this information to be layered/structured in a way that the user can quickly find/navigate to the topic of their interest and when changes are made, users should be made aware of them (e.g. requiring users to regularly check for changes in not considered sufficient). To ensure intelligibility the recommendation is for the organizations to perform readability or user studies to analyse the average understanding of the content providing the information. United Kingdom’s independent authority – Information Commissioner’s Office has also recommended the organizations carry out user testing to evaluate how effective their privacy information is [88]. To present their information in clear and plain language organizations should adhere to best practices (e.g. How to Write Clearly [89], published by the European Commission). The use of translations is also required if targeted users speak different languages. The WP29 recommendations also include informing their users what are the consequences their processing will have. Compliance with these recommendations can be used to show the fulfilment of GDPR requirements and in a way serve to validate the usability of the (under GDPR required) information.

Some of the attributes that can be defined to validate the usability of GDPR compliant user experience are fairness, transparency, and a smaller number of data breaches.

This page has been intentionally left blank.

5 Recommendations

This section provides recommendations for validating usability requirements for all the demonstration cases described in D5.1. Additionally, recommendations are directed towards specific use cases described in D3.5. Studies have shown that security, privacy, and usability properties are orthogonal to each other. It can be deduced that security, privacy, and usability do not form a one-to-one relationship or direct associativity with each other. On the contrary, they are more independent properties rather than being dependent on each other. The usability validation is necessary to ensure security and privacy technologies meet their usability requirements and wider acceptance by their intended users.

1. **Selection of appropriate dimensions or attributes to characterize usability requirements.**

   Different users can have different expectations and preferences with regard to security or privacy mechanisms to be deployed in a system. Therefore, it is essential to select appropriate dimensions or attributes (*e.g., knowability, operability (effectiveness), efficiency, robustness, safety, satisfaction*) to characterize usability requirements specific to each security and privacy mechanism (refer Section 3.2).

2. **Selection of suitable usability inspection methods during the design and development phase of security or privacy mechanisms pertaining to a system.**

   D3.5 recommended an early user involvement should be ensured for new security and privacy features Table 1 presents popular usability inspection evaluation methods, they should be applied for the usability evaluation of security or privacy designs. The outcome of this step is to generate a usability requirements validation checklist that should be used as an input for usability testing with users.

3. **Selection of more than one "usability testing with users" approaches.**

   D.5 recommended user modelling and/or user tests should be conducted for new security and privacy features. More than one usability testing with users approaches presented in Table 2 should be selected to validate the usability requirements checklist generated as a result of Step 2.

4. **Creation of a usability traceability matrix.**

   D3.5 recommended that usability research methods should be used throughout the design, development, and assessment of security mechanisms. Thus, a traceability matrix should be prepared that can link between 1) the privacy or security specifications, 2) usability requirements for each privacy and security specification, 3) usability validation checklist, and 4) the test cases, surveys, and questionnaires to synergize the usability validation framework.

5. **Validation of usability requirements for authenticated encryption.**

   D3.5 recommended the use of authenticated encryption to protect the integrity of the communications as well as the privacy of the content. It is recommended to capture usability requirements for designing such solutions by involving a wider audience. Subsequently, their nature and habits to be studied to prepare a usability validation checklist.

6. Validation of usability requirements for user authentication.

D3.5 recommended providing user authentication methods that are both secure and privacy-friendly, suggesting the use of biometrics. Generally, a user generally uses a number of smart devices and security-sensitive applications on a daily basis. Usability validation methods must ensure that user authentication schemes do not add cognitive load, ease of use, do not require any technical knowledge, and do not frustrate users.

This page has been intentionally left blank.

6 Open challenges

One of the key challenges for usability evaluation in the context of privacy and security is that these aspects are not directly linked to the activities of the user on the systems (be it work or entertainment). Addressing security aspects, such as authentication, error messages, security messages will always interfere with the user's primary activity and thus will always be perceived as a disturbance [91]. It is, thus, a challenge to design security and privacy mechanisms that can be perceived as of prime importance to users and that can be weaved with their activities.

Another challenge comes from the evolution of usability. Over the last decade, the usability research community has embraced the challenge of designing for user experience [8] and identified six contributing factors to it [9]. These contributing factors can be seen as a profound refinement of the satisfaction dimension of usability. The factors are Emotion, Aesthetics, Identification, Stimulation, Meaning and Value and Social Connectedness and design work aim at embedding those elements that have, in turn, to be assessed on the final system (refer [10] for a detailed presentation of means of evaluating UX in games). A possible direction is to integrate gamification aspects [11] in the design of security and privacy mechanisms distracting users from a primary task to a secondary enjoyable one.

In the area of multi-factor and multi-modal authentication, there is a trend towards continuous authentication with the objective to monitor the behavior of the user continuously, in the background [54]. The advantage over single-shot authentication mechanisms is that analysis of human behavior offers an ongoing assessment of the authenticity of a subject's identity during an application session, as well as a frictionless experience. Indeed, the user does not need to learn how to use the authentication system, as it operates in a transparent manner.

As these types of authentication schemes rely on sensor and/or user interaction events (e.g. the way a user types on a keyboard or uses a mouse), as well as statistical or more sophisticated machine learning-based analysis techniques, there is an inherent trade-off between usability and security on the one hand, and privacy on the other hand. In order for these authentication techniques to be usable and secure, they must exhibit a low false negative and false positive rate (or equivalently a low false rejection and false acceptance rate). The consequence of aiming to achieve low error rates is that more and more data about more and more types of behavior need to be combined to produce an effective multi-modal authentication scheme.

This results in two privacy problems: (1) the collected data may reveal more information about the subject than just his identity, and (2) the same techniques can be used, for example by advertisers, to track individuals. The alternative is to guarantee that all behavior data is analyzed on the client's device such that no sensitive information is leaked to a remote party or service that aims to continuously authenticate its users. However, this, in turn, results in a security challenge in that the remote service must trust the outcome of the behavior analysis on the client device. This is a concern when the sensor or user interaction events are also publicly accessible to other applications, and/or when an adversary can reverse engineer the behavior analysis method itself to launch a presentation attack against a subject.

One of the open challenges for frictionless authentication is the fact that new tracking countermeasures are introduced in web browsers and mobile operating systems, and this on a regular basis. The fact that these can also influence behavioral analysis for multi-modal authentication, means that usability validation for next-generation continuous authentication systems remains an ongoing effort in a continuously evolving security and privacy-enhancing technology landscape.

Some of the use cases described in D3.5 like GDPR compliant user experience, graphical security models, verifiable credentials, and identity and privacy management requires more investigation to capture usability attributes associated with them.

D3.5 mentioned for Graphical Security Models, graphs are often too complex and require some post-analysis to make them usable [6]. They further stated the usability of this kind of security tool is strictly related to the usability of its results as are used by human operators. This document presented some usability requirements for Information Visualization. Similarly, the asset *SelfSovereign-PPIdM* (Self-sovereign privacy-preserving IdM in the blockchain) to tackle the identity and privacy-management is required to provide their usability requirements. Verifiable credentials are part of several use cases of the CyberSec4Europe project, e.g., open banking and privacy-preserving identity management that require to replace conventional user authentication schemes with biometrics and explore users' expectations for their usability validation.

This page has been intentionally left blank.

7 Conclusions

In recent years, there is a growing consensus that usability aspects in designing and implementing information technology solutions for both the public and private sectors are an important success factor. The CyberSec4Europe project identifies that the usability factors play a pivotal role in the wider acceptance of security and privacy solution designed for key domains, i.e., *Open Banking, Supply chain Security Assurance, Privacy-Preserving Identity Management, Incident Reporting, Maritime Transport, Medical Data Exchange,* and *Smart Cities,* by their intended users.

Earlier usability has never been on top of the agenda of security researchers and designers, evidently, D3.5 stated providing recommendations on usability in fields such as security and privacy is a difficult task. However, in this document, we attempted to exhibit relevant examples of usability requirements for various security and privacy specification indicated by D3.5 and D5.1. As a general remark, we recommend that usability requirements in security and privacy must be considered critically in the early stages of the design process. In addition, usability requirements must not only be elicited but also be validated later by referring to the checklist prepared for each usability requirement during the design phase.

This document presented the relevant approaches and methodology that can be used to perform usability validation. Typically, usability validation involves human that is not only complex but also expensive. Thus, designing the validation process and choosing the right mechanisms and metrics is not a straightforward process. However, in the context of security and privacy, the validation process demands diligent research as usability requirements can be seen in contrast (if not in conflict) with more traditional functional privacy and security requirements.

Finally, to validate the usability of the security and privacy requirements of a system, it is essential to generate a framework that can translate the humans' nature, habits, and mental model perceived by them in dealing with those aspects offered by the system. At the end of the study carried out in this document, six recommendations are provided for designing a validation framework for the demonstration use cases specified in D5.1 and D3.5.

This page has been intentionally left blank.

8 References

[1] ISO, "ISO 9241-11: Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs): Part 11: Guidance on Usability." 1998.

[2] Cybersec4europe, "Usable security & privacy methods and recommendations." https://cybersec4europe.eu/wp-content/uploads/2020/02/D3.5-Usable-security-privacy-methods-and-recommendations-Submitted.pdf, [Online Web Reference].

[3] Cybersec4europe, "Requirements Analysis of Demonstration Cases Phase1." https://cybersec4europe.eu/wp-content/uploads/2019/11/D5.1-Requirements-Analysis-of-Demonstration-Cases.pdf, [Online Web Reference].

[4] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," MIS Q., pp. 319–340, 1989.

[5] J. Nielsen, "Usability engineering." Academic Press, ISBN 978-0-12-518405-2, pp. I-XIV, 1-358, 1993.

[6] S. Lauesen, and H. Younessi, "Six Styles for Usability Requirements." In REFSQ (Vol. 98, pp. 155-166), 1998.

[7] J. B. Hong, D. S. Kim, C. J. Chung, and D. Huang, "A survey on the usability and practical applications of Graphical Security Models," *Comput. Sci. Rev.*, vol. 26, pp. 1–16, 2017.

[8] E.L-Chong Law, V. Roto, M. Hassenzahl, A.P.O.S. Vermeeren, and J. Kort. "Understanding, scoping and defining user experience: a survey approach." In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '09). Association for Computing Machinery, New York, NY, USA, 719–728. DOI:https://doi.org/10.1145/1518701.1518813, 2009.

[9] M.M. Pirker and R. Bernhaupt. "Measuring user experience in the living room: results from an ethnographically oriented field study indicating major evaluation factors." In Proceedings of the 9th European Conference on Interactive TV and Video (EuroITV '11). Association for Computing Machinery, New York, NY, USA, 79–82. DOI:https://doi.org/10.1145/2000119.2000133, 2011.

[10] R. Bernhaupt: "Game User Experience Evaluation." Human-Computer Interaction Series, Springer, ISBN 978-3-319-15984-3, 2015.

[11] G.F. Tondello, R.R. Wehbe, L. Diamond, M. Busch, A. Marczewski, L.E. Nacke: "The Gamification User Types Hexad Scale." ACM CHI PLAY conference 2016: 229-243.

[12] S. Dutta, "Striking a balance between usability and cyber-security in IoT devices," 2017.

[13] W. Bai, D. Kim, M. Namara, Y. Qian, P.G. Kelley, and M.L. Mazurek, "Balancing security and usability in encrypted email." IEEE Internet Computing, 21(3), pp.30-38, 2017.

[14] S. Ruoti, and K. Seamons, Johnny's Journey Toward Usable Secure Email. IEEE Security & Privacy, 17(6), pp.72-76, 2019.

[15] S. Parkin, T. Patel, I. Lopez-Neira, and L. Tanczer, "Usability analysis of shared device ecosystem security: Informing support for survivors of IoT-facilitated tech-abuse." In Proceedings of the New Security Paradigms Workshop (pp. 1-15), 2019.

[16] K. Sagar, and A. Saha, "A systematic review of software usability studies." International Journal of Information Technology, pp.1-24, 2017.

[17] L. Cranor and S. Garfinkel, "Security and Usability." O'Reilly Media, Inc., 2005.

[18] S. Kieffer, A. Ghouti, and B. Macq, "The agile UX development lifecycle: Combining formative usability and agile methods." 2017.

[19] H. Hartson, A. Terence & R. Williges, (2003). "Criteria for Evaluating Usability Evaluation Methods." Int. J. Hum. Comput. Interaction. 15. 145-181. 10.1207/S15327590IJHC1501_13.

[20] A. Fernandez, E. Insfran, and S. Abrahão, "Usability evaluation methods for the web: A systematic mapping study." Information and Software Technology, 53(8), pp.789-817, 2011.

[21] R.G. Bias, "The pluralistic usability walkthrough: coordinated empathies. In Usability inspection methods," (pp. 63-76). John Wiley & Sons, Inc., 1994.

[22] S. Chaudhary, T. Schafeitel-Tähtinen, M. Helenius, and E. Berki, "Usability, security and trust in password managers: A quest for user-centric properties and features." Computer Science Review,

33, pp.69-90, 2019.

[23] S.Hermawati, and G. Lawson, “Establishing usability heuristics for heuristics evaluation in a specific domain: Is there a consensus?” Applied Ergonomics, 56, pp.34-51, 2016.

[24] R. Spencer, “The streamlined cognitive walkthrough method, working around social constraints encountered in a software development company,” In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 353-359). ACM.

[25] M. Burghardt, “Usability Pattern Identification through Heuristic Walkthroughs,” In International Conference of Design, User Experience, and Usability (pp. 219-230). Springer, Cham, 2016.

[26] S. Greenberg. “Working Through Task-Centered System Design.” Handbook of Task Analysis for Human-Computer Interaction. Eds. Dan Diaper, Neville Stanton. Lawrence Erlbaum Associates (2003).

[27] E. Frøkjær, and K. Hornbæk, “Metaphors of human thinking for usability inspection and design,” ACM Transactions on Computer-Human Interaction (TOCHI), 14(4), p.20, 2008.

[28] K. Hornbæk, and E. Frøkjær, “Evaluating user interfaces with metaphors of human thinking.” In ERCIM Workshop on User Interfaces for All (pp. 486-507). Springer, Berlin, Heidelberg, 2002.

[29] J. Dong, and M. Byun, “Enhanced Usability Assessment on User Satisfaction with Multiple Devices,” In Advanced Multimedia and Ubiquitous Engineering (pp. 849-853). Springer, Singapore, 2018.

[30] N. Khalayli, S. Nyhus, K. Hamnes, and T. Terum, April. “Persona-based rapid usability kick-off.” In CHI'07 extended abstracts on Human factors in computing systems (pp. 1771-1776), 2007.

[31] S. Gupta, A. Buriro, and B. Crispo, September. “A Risk-driven Model to Minimize the Effects of Human Factors on Smart Devices.” In International Workshop on Emerging Technologies for Authorization and Authentication (pp. 156-170). Springer, Cham, 2019.

[32] S.L. Hura, “Usability testing of spoken conversational systems,” Journal of Usability Studies, 12(4), pp.155-163, 2017.

[33] K. Puri, and S.K. Dubey, “Analytical and critical approach for usability measurement method,” In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 4045-4050). IEEE, 2016.

[34] E. Folmer, and J. Bosch, “Architecting for usability: a survey,” Journal of systems and software, 70(1-2), pp.61-78, 2004.

[35] J. Brooke, “SUS: a retrospective,” Journal of usability studies, 8(2), pp.29-40, 2013.

[36] SUS Template, “https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html.” [Online Web Reference].

[37] J. Kirakowski, “The software usability measurement inventory: background and usage.” Usability evaluation in industry, pp.169-178.

[38] H.X. Lin, Y.Y. Choong, and G. Salvendy, “A proposed index of usability: a method for comparing the relative usability of different software systems.” Behaviour & information technology, 16(4-5), pp.267-277, 1997.

[39] K. Norman, and B. Shneiderman, “Questionnaire for user interaction satisfaction (quis 5.0).” University of Maryland: HCI-Lab, College Park, 1989.

[40] S.G. Hart, “NASA-task load index (NASA-TLX); 20 years later. “In Proceedings of the human factors and ergonomics society annual meeting (Vol. 50, No. 9, pp. 904-908). Sage CA: Los Angeles, CA: Sage Publications, 2006.

[41] M. Hassenzahl, A. Platz, M. Burmester, K. Lehner. Hedonic and ergonomic quality aspects determine a software’s appeal. In Proc. of CHI 2000, pp. 201-208 (2000).

[42] AttrakDiff questionnaire, attrakdiff.de, last accessed Feb. 2020.

[43] M. Hassenzahl, M. Burmester, and F. Koller, “AttrakDiff: A questionnaire to measure perceived hedonic and pragmatic quality.” In Mensch & Computer (Vol. 57, pp. 187-196)., 2003.

[44] E. Karapanos, J.B. Martens, and M. Hassenzahl, M., 2012. Reconstructing experiences with iScale. International Journal of Human-Computer Studies, 70(11), pp.849-865.

[45] S. Hedegaard, and J.G. Simonsen, “Extracting usability and user experience information from online user reviews.” In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 2089-2098), 2013.

[46] E. Folmer, J. Van Gurp, and J. A. Bosch, “Framework for capturing the relationship between usability and software architecture.” Software Process: Improvement and Practice 8, 2 (2003), 67–87.

[47] A. Seffah, M. Donyaee, R. Kline, and H. Padda, “Usability measurement and metrics: A consolidated model.” Software Quality Journal 14 (2006), 159–178.

[48] N. Bevan, “Classifying and selecting UX and usability measures.” In International Workshop on Meaningful Measures: Valid Useful User Experience Measurement (2008), 13–18.

[49] O. Ketola, and V. Roto, “Exploring user experience measurement needs.” In 5th COST294-MAUSE Open Workshop on Valid Useful User Experience Measurement (2008).

[50] J. A. Bargas-Avila, and K. Hornbæk, “Old wine in new bottles or novel challenges: a critical analysis of empirical studies of user experience.” In Proceedings of the 2011 annual conference on Human factors in computing systems, CHI ’11, The ACM Press (2011), 2689–2698.

[51] D. Alonso-Ríos, A. Vázquez-García, E. Mosqueira-Rey, and V. Moret-Bonillo, “Usability: A Critical Analysis and a Taxonomy.” Intl. Journal of Human–Computer Interaction. 26. 53-74. 10.1080/10447310903025552, 2010.

[52] T. Van Hamme, V. Rimmer, D. Preuveneers, W. Joosen, M.A. Mustafa, A. Abidin, and E.A. Rúa, “Frictionless authentication systems: emerging trends, research challenges, and opportunities.” arXiv preprint arXiv:1802.07233, 2018.

[53] S. Gupta, A. Buriro, B. Crispo, “Driverauth: A risk-based multi-modal biometric-based driver authentication scheme for ride-sharing platforms, “Computers & Security 83 (2019) 122-139.

[54] S. Gupta, A. Buriro, and B. Crispo, “Demystifying authentication concepts in smartphones: Ways and types to secure access,” Mob. Inf. Syst., vol. 2018, 2018.

[55] A. De Luca, J. Lindqvist, “Is secure and usable smartphone authentication asking too much?” Computer 48 (2015) 64-68.

[56] C.M. Freitas, P.R. Luzzardi, R.A. Cava, M. Winckler, M.S. Pimenta, and L.P. Nedel, "On evaluating information visualization techniques." In Proceedings of the working conference on Advanced Visual Interfaces (pp. 373-374), 2002.

[57] T. Dinev, P. Hart, and M. R. Mullen. "Internet privacy concerns and beliefs about government surveillance–an empirical investigation. " The Journal of Strategic Information Systems, 17(3):214–233, 2008.

[58] A. Herzberg, and H. Leibowitz, "Can Johnny finally encrypt? Evaluating E2E-encryption in popular IM applications." In Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust (pp. 17-28).

[59] Y. Zou, S. Danino, K. Sun, and F. Schaub, “You might' be affected: An empirical analysis of readability and usability issues in data breach notifications, “ Proceedings of the CHI Conference on Human Factors in Computing Systems, CHI '19, 2019.

[60] J.A. Bargas-Avila, G. Oberholzer, P. Schmutz, M. de Vito, K. Opwis, “Usable errors message presentation in the World Wide Web: do not show errors right away.” Interacting with Computers 19, 330–341 (2007)

[61] M. Seckler, A.N. Tuch, K. Opwis, J.A. Bargas-Avila, “User-friendly locations of error messages in web forms: put them on the right side of the erroneous input field.” Interacting with Computers 24, 107–118 (2012)

[62] S. Chaudhary, “The use of usable security and security education to fight phishing attacks,” The School of Information Sciences, University of Tampere (2016).

[63] S.Weinhardt, and O. Omolola, “Usability of policy authoring tools: A layered approach,” 5th International Conference on Information Systems Security and Privacy, 2019, pp. 301-308.

[64] J.P. Titlow, “Uber Can Now Predict Where You’re Going Before You Get In The Car,” https://www.fastcompany.com/3035350/uber-can-now-predict-where-youre-going-before-you-get-in-the-car [Online Web Reference].

[65] S. Gupta, A. Buriro, B. Crispo, “DriverAuth: Behavioral biometric-based driver authentication mechanism for on-demand ride and ridesharing infrastructure." ICT Express, 5(1), pp.16-20.

[66] C. Dwork, N. Kohli, and D. Mulligan, “Differential privacy in practice: Expose your epsilons!” Journal of Privacy and Confidentiality 9 (2019).

[67] M. F. Theofanos, R. J. Micheals, and B. C. Stanton, “Biometrics systems include users,” IEEE Systems Journal, vol. 3, no. 4, pp. 461–468, 2009.

[68] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, “The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes,” in Security and Privacy (SP), 2012 IEEE Symposium on, 2012, pp. 553–567.

[69] K. Halunen, J. Häikiö, and V. Vallivaara, “Evaluation of user authentication methods in the gadget-free world,” Pervasive Mob. Comput., vol. 40, 2017.

[70] R. Peeters, J. Hermans, P. Maene, K. Grenman, K. Halunen, and J. Häikiö, “N-Auth: Mobile authentication done right,” in ACM International Conference Proceeding Series, 2017, vol. Part F1325.

[71] T. Van Nguyen, N. Sae-Bae, and N. Memon, “DRAW-A-PIN: Authentication using finger-drawn PIN on touch devices." computers & security, 66, pp.115-128, 2017.

[72] K. Reese, T. Smith, J. Dutson, J. Armknecht, J. Cameron, and K. Seamons, “A usability study of five two-factor authentication methods.” In the Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019).

[73] A. Buriro, B. Crispo, S. Gupta, and F. Del Frari, “Dialerauth: A motion-assisted touch-based smartphone user authentication scheme.” In Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy (pp. 267-276), March 2018.

[74] International Organization for Standardization. “Ergonomics of human-system interaction — Part 11: Usability: Definitions and concepts. “The International standard, ISO 9241-11:2018(en), 2018.

[75] M. Georgsson and N. Staggers, “Quantifying usability: an evaluation of a diabetes mHealth system on effectiveness, efficiency, and satisfaction metrics with associated user characteristics.” Journal of the American Medical Informatics Association, 23(1), pp.5-11, 2016.

[76] H. Suh, N. Shahriaree, E.B. Hekler, and J.A. Kientz, May. “Developing and validating the user burden scale: A tool for assessing user burden in computing systems.” In Proceedings of the 2016 CHI conference on human factors in computing systems (pp. 3988-3999), 2016.

[77] J. Grigera, A. Garrido, J.M. Rivero, and G. Rossi, “Automatic detection of usability smells in web applications.” International Journal of Human-Computer Studies, 97, pp.129-148, 2017.

[78] D. Quiñones, and C. Rusu, “How to develop usability heuristics: A systematic literature review.” Computer Standards & Interfaces, 53, pp.89-122, 2017.

[79] R. Kainda, I. Flechais, and A.W. Roscoe, “Security and usability: Analysis and evaluation.” In 2010 International Conference on Availability, Reliability and Security (pp. 275-282). IEEE, 2010.

[80] W. Bai, “User Perceptions of and Attitudes toward Encrypted Communication.” Doctoral dissertation, 2019.

[81] C. Brodie, C.M. Karat, J. Karat, and J. Feng. “Usable security and privacy: a case study of developing privacy management tools”. In Proceedings of the 2005 symposium on Usable privacy and security (pp. 35-43), 2005.

[82] P.G. Kelley, L.J. Cesca, J. Bresee, L.F. Cranor. “Standardizing privacy notices: an online study of the nutrition label approach”. Proceeding of 2010 SIGCHI Conference on Human Factors in Computing Systems (CHI 2010); 2010: 1573–1582.

[83] D.R.G. de Pontes, and S.D. Zorzo, “PPMark: An Architecture to Generate Privacy Labels Using TF-IDF Techniques and the Rabin Karp Algorithm”. In Information Technology: New Generations (pp. 1029-1040). Springer, Cham, 2016.

[84] H. Harkous, K. Fawaz, R. Lebret, S. Schaub, K.G. Shin, and K. Aberer, “Polisis: Automated analysis and presentation of privacy policies using deep learning.” In 27th {USENIX} Security Symposium ({USENIX} Security 18) (pp. 531-548), 2018.

[85] S. Reis, A. Ferreira, P. Vieira-Marques, and R. Cruz-Correia, “Usability Study of a Tool for Patients’ Access Control to Their Health Data”, 2019.

[86] EU Commission, “Guidelines on Transparency under Regulation 2016/679 (wp260rev.01),” https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227, [Online web reference].

[87] EU Commission, “GDPR: Guidelines, Recommendations, Best Practices,” https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en, [Online web reference].

[88] ICO, “Right to be informed,” https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/, [Online web reference]

[89] EU Commission, “How to write clearly,” https://op.europa.eu/en/publication-detail/-/publication/c2dab20c-0414-408d-87b5-dd3c6e5dd9a5, [Online web reference]

[90] M. Beckerle, and L.A. Martucci. “Formal definitions for usable access control rule sets from goals to metrics.” Proceedings of the Ninth Symposium on Usable Privacy and Security. 2013.

[91] C. Lewis, P.G. Polson, C. Wharton, and J. Rieman. “Testing a walkthrough methodology for theory-based design of walk-up-and-use interfaces.” In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI ’90). Association for Computing Machinery, New York, NY, USA, 235–242, 1990.

This page has been intentionally left blank.