Project number: 653454
H2020-DS-2014-1

Project start: October 1, 2015
Project duration: 3 years

D3.1

UI Prototypes V1

Document Identification	
Due date	March 31, 2017
Submission date	March 31, 2017
Revision	1.0

Related WP	WP3	Dissemination Level	PU
Lead Participant	KAU	Lead Author	Farzaneh Karegar, John Sören Pettersson
Contributing Beneficiaries	AIT, ATOS, FOKUS, GUF, KAU, KGH, LISPA, OTE	Related Deliverables	D2.1, D2.3, D2.6, D3.2, D5.1, D6.1, D6.4-6.

Abstract: This report covers the background research through various literature surveys as well as partner inputs and reviews of the prototypes that eventually resulted in the first stable version of the CREDENTIAL user interfaces, the UI Prototypes V1. The report also covers the content (not graphical design) of user interfaces for the eHealth pilot as the eHealth pilot, in contrast to the eGovernment and the eBusiness pilots, embodies a totally new kind of application and therefore includes user interfaces developed specifically for the CREDENTIAL pilot.

In a first usability test of the general user interfaces, some problems with people's mental model of authentication surfaced. Using one's fingerprint for giving consent was from a simple usability perspective not a problem, but most of the participant had not a correct view of where it is stored and what entities have access to it. Moreover, and in line with other studies participants, did not pay sufficient attention to details of data releases and settings for disclosure policies. However, the participants showed a desire to have control over their data and expressed a wish to select the mandatory information manually. This can be a way of slowing users down and make them reflect more. There are also some other issues to develop alternative solutions for. Besides the test results, this deliverable also summarises literature reviews on users' perceptions and acceptance of CREDENTIAL related technologies.

This document is issued within the CREDENTIAL project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 653454.

Executive Summary

The growth of internet has shown a wide range of applications in different domains. Often users need to prove their rights to access certain functions and information, be it email, bank accounts, or others, and also to provide information. Helping service providers to trust users' information and users to trust that their personal information is not used for other purposes than they intend when providing it is an urgent matter in the growing information society. In addition, usability issues grow with growing information and security demands.

CREDENTIAL is an EU-funded Horizon 2020 project that involves developing, testing and presenting cloud-based services for storing, managing and sharing digital identity information and personal data with a higher level of security than existing technology.

The CREDENTIAL Wallet is the central component of the tools and components developed within the project. It offers a set of security and application services providing, among others, authentication and authorization mechanisms combined with novel cryptographic technologies like proxy-re-encryption and malleable signatures. Three pilot cases are developed within the project to demonstrate how the CREDENTIAL technology can be deployed in diverse contexts.

In order to demonstrate the CREDENTIAL Wallet solution, the demonstrated system has to be equipped with user interfaces (UIs). Besides the pilot-specific user interfaces, there must also be some general user interfaces to demonstrate the functionality. This report covers in essence two sets of UIs: (1) general ones that future users of CREDENTIAL-based identity services will most likely use when they, as private individuals, use the Wallet in their daily lives, and (2) specific ones for use in eHealth scenarios to facilitate the management by patients and health workers' use of Personal Health Records and wearables sending patient status data to clinics' staff. (Other pilots within the CREDENTIAL project do not have specific apps for the CREDENTIAL functions why no UIs besides the general ones need to be designed.)

Furthermore, just as the pilot prototypes, the general user interfaces can be used to evaluate how ordinary users and systems owners would appreciate the CREDENTIAL Wallet functionality. They also enable the project to evaluate the communicability of various user interface designs. A first user test has already been conducted based on mockups of the general UIs with faked functionality, which made the mockup Wallet appear interactive to the test participants, and a fake web site service, which seemed to interact with the faked Wallet app on a smartphone.

The results, as measured by the very widely used SUS scale – System Usability Scale – indicate that this group of first-time users appreciated the concept, the graphic layout, and also the interaction design. For the two task of authorization and authentication, the SUS score ranged 75-80. However, the participant were familiar with using smartphone for the service of identity providers, in contrast to most EU citizen presently. Thus, a similar study has to be conducted with other types of internet users.

Moreover, the user test also showed a lack of understanding of how the identity key (in this case, the fingerprint) is kept and used. There were also a not entirely satisfying result as to what data the participants thought had been released to the service provider. This report will thus serve as a basis for exploring slight modifications of the interaction and presentation elements within the general UIs. The

eHealth-specific UIs has not yet been subjected to any user evaluation, but they will be as part of the pilot development cycle.

This report discusses also other means of enhancing users' understanding. These discussions are based on literature surveys of research literature within identity management and usable privacy and reflection on actual cases from partners within the project. As made explicit, the introductions to new technology is not only made via UIs but also via specifically crafted introduction presentations and via champions like public bodies or private companies that already are trusted by citizens.

Document information

Contributors

Name	Partner
Charlotte Bäccman	KAU
Andreas Happe	AIT
Felix Hörandner	TUG
Simone Fischer-Hübner	KAU
Farzaneh Karegar	KAU
Alexandros Kostopoulos	OTE
Stephan Krenn	AIT
Daniel Lindegren	KAU
Silvana Mura	LISPA
Andrea Migliavacca	LISPA
Nicolas Notario McDonnell	ATOS
Juan Carlos Pérez Baún	ATOS
John Sören Pettersson	KAU
Anna E. Schmaus-Klughammer	KGH
Evangelos Sfakianakis	OTE
Welderufael Tesfay	GUF
Florian Thiemer,	FOKUS
Melanie Volkamer	KAU

Reviewers

Name	Partner
Felix Hörandner	TUG
Stephan Krenn	AIT
Andrea Migliavacca	LISPA
Anna Schmaus-Klughammer	KGH

History

0.1	2016-11-02	Editors set sections headlines	John Sören Pettersson
0.2	2016-12-06	Added and explained requests	John Sören Pettersson
0.3	2017-01-10	Time plan uploaded Sharepoint	John Sören Pettersson
0.4	2017-01-19	Most sections on time except sec. on use cases	“All”
0.5	2017-01-27	Add eHealth pilot explanation	Florian Thiemer
0.6	2017-01-27	Add section 5 and 6	Farzaneh Karegar
0.7	2017-01-31	Edit sec 2 and 6.1	Farzaneh Karegar
0.8	2017-02-01	Add to 3.2, 4.1	Melanie Volkamer, Andrea Migliavacca
0.9	2017-02-06	Edit sec 5 and 6, Add to sec 6.2, new section in 3 (3.1)	Farzaneh, Florian, Alexandros
0.10	2017-02-11	Edit sec 4.2, sec 2-2.6, sec 3.1, sec 6.3.1.	John Sören
0.11	2017-02-13	Edit sec 4.1, 3.2, 3.3, …	On inputs

0.12	2017-02-13	Rearranged subsection in 3	John Sören Pettersson
0.13	2017-02-14	Edit 3.1, 6.2 (Doctor's), 1-2, 3.2; new 3.3.3, Appendix Ö	Alexandros Kostopoulos, Florian Thiemer, John Sören Pettersson, Nicolas Notario McDonnell, Farzaneh Karegar
0.14	2017-02-17	High-Level Reviews	Felix Hörandner, Stephan Krenn
0.15	2017-02-19	Starting to adapt to comments from Felix (and Stephan), and also from LISPA, and Welde.	John Sören Pettersson
0.16	2017-02-21	Put changes by Charlotte into 1-3.4 (Melanie will rewrite so we wait; and sec 6), Farzaneh 5, Appendix B-F	John Sören Pettersson, Charlotte Bäccman, Farzaneh Karegar
0.17	2017-02-22	Put changes by Charlotte in section 6., Farzaneh Appx G on Additional UI, start section 8	-"-
0.18	2017-02-23	Summary sections here and there. Slight update of eHealth UI	John Sören Pettersson. Florian Thiemer
0.19	2017-02-23	For internal review	-"-
0.20	2017-03-03	Restructure after telco Mar-02	John Sören Pettersson
0.21	2017-03-03	Completed Adoption section and rewrote outline section	John Sören Pettersson
0.22	2017-03-06	Updated all general UI and appx.	Farzaneh Karegar
0.23	2017-03-06	Might be errors in legend linking (Word started inserting figures in refs to figures!)	John Sören Pettersson
0.24	2017-03-07	Updated introduction to project	Felix Hörandner
0.25	2017-03-09	eHealth UIs	Florian Thiemer
0.26	2017-03-10	Abstract, Executive Summary	John Sören Pettersson
0.27	2017-03-12	Added Melanie's refs to 3.3.1	John Sören Pettersson
0.28	2017-03-12	Anna's spelling corrections	John Sören Pettersson
0.29	2017-03-14	Elaborations in 2, 4, 6, Refs, Questionnaires	John Sören Pettersson
0.30	2017-03-15	Rewriting section 7, edit 6.7, 5	John Sören Pettersson
0.31	2017-03-15	Refs alphabetically ordered	John Sören Pettersson
0.32	2017-03-16	Correction 1 page sec 5 (eHealth)	John Sören Pettersson
0.33	2017-03-22	Corrections according to Reviewer. Additions sec 4.	Farzaneh Karegar, John Sören Pettersson
0.34	2017-03-23	Changes in first para sec. 5 (question to Florian in separate file with comments on Review 2 by AM).	John Sören Pettersson
0.35	2017-03-23	Inserted general UI in one eHealth figure and changed preceding text. Accepted some spelling changes suggested in Review 2 by by AK.	John Sören Pettersson, Florian Thiemer
0.36	2017-03-24	Minor errors corrected. Had to make new layout on several pages, and made changes in test descr. Sent to PC, TM and QM.	Farzaneh Karegar, John Sören Pettersson
0.37	2017-03-28	Comments from Felix (doc) and Stephan (email)	John Sören Pettersson
0.38	2017-03-29	Updates	John Sören Pettersson
1.0	2017-03-31	Final copy-editing	Stephan Krenn, Agi Karyda

List of Contents

List of Figures

List of Tables

List of Acronyms

2FA	2-Factor Authentication
AGID	Agenzia per l'Italia Digitale (the Agency for Digital Italy)
eIDAS	Electronic identification and trust services for electronic transactions (legal doc.)
GDPR	General Data Protection Regulation (EU directive)
HCI	Human-Computer Interaction
IdP	Identity provider
IdPC	Identity Provider of the Citizen (Lombardian public system)

ISO	International Organization for Standardization or prefix for standards' ID numbers
KPI	Key Perfomance Indicators
PHR	Personal Health Record
SUS	System Usability Scale
SPID	Sistema Pubblico di Identità Digitale
SMS	Short Messages Service (text messages via mobile telephones)
TAM	Technology Acceptance Model
UI	User Interface
UMA	User-Managed Access

1 Introduction

1.1 Project Scope and Background

The growth of internet has shown a wide range of applications in different domains. Often users need to prove their rights to access certain functions and information, be it email, bank accounts, or others, and also to provide information. Helping service providers to trust users' information and users to trust that their personal information is not used for other purposes than they intend when providing it is an urgent matter in the growing information society. In addition, usability issues grow with growing information and security demands.

The goal of CREDENTIAL is to develop, test and showcase innovative cloud based services for storing, managing, and sharing digital identity information and other critical personal data. The security of these services relies on the combination of strong hardware-based multi-factor authentication with end-to-end encryption representing a significant advantage over current password-based authentication schemes. The use of sophisticated proxy cryptography schemes, such as proxy re-encryption and redactable signatures, will enable a secure and privacy preserving information sharing network for cloud-based identity information in which even the identity provider cannot access the data in plain-text and hence protect access to identity data. The project goal is to extend the application of the CREDENTIAL approach to a comprehensive cloud system and to existing solutions by using and exploiting recognized standards and protocols.

CREDENTIAL's **basic architecture** is based on the integration of cryptographic mechanisms involving three key components namely a user, the CREDENTIAL Wallet, and a data receiver, as shown in Figure 1-1.

- The **User** owns data that might be securely stored or shared with other members of the CREDENTIAL Wallet. A client application in the user's domain handles cryptographic operations involving the user's private key, such as signing or generating a re-encryption key.
- The **Wallet** is a cloud-based data storage and sharing service characterized by important advantages such as constant availability on the internet, scalability, and cost effectiveness. The Identity and Access Management system implements a multi-factor authentication and authorizes access to data stored. This leads to two main advantages: proxy re-encryption system does not expose plain data, therefore confidentiality of data shared and stored by CREDENTIAL Wallet in the cloud is ensured; once a re-encryption key is available for some specific set of data as specified by the user, these data can be shared with specified receivers even if the user or his/her client application are not available.
- The **Data Receiver,** that can be either another CREDENTIAL user or a service provider, reaches data stored in or authentication assertions issued by the CREDENTIAL Wallet and can perform arbitrary data processing.

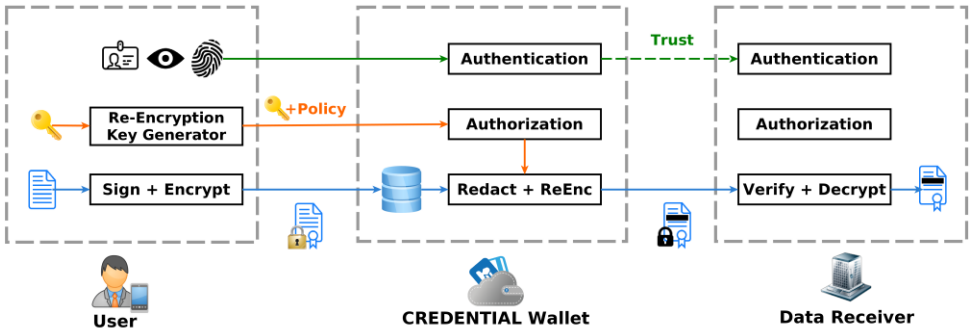


Figure 1-1: CREDENTIAL's Basic Architecture

The **data sharing process** involves the actors of CREDENTIAL's basic architecture in the following steps:

1. The user authenticates at the Wallet to get read and write permission to her Wallet account, which are used to upload signed and encrypted data.
2. To later share this data, the user generates a re-encryption key towards a selected data receiver in her trusted domain. Along with this key, the user defines a policy defining which data may be disclosed to which entity and installs it at the Wallet.
3. When an authorized receiver tries to access the user's data, not required parts are redacted and the remaining parts are transformed into ciphertext for the data receiver by using the re-encryption key.
4. Finally, the data receiver is able to decrypt the data and verify the signature on the disclosed parts.

To showcase the functionality of the CREDENTIAL Wallet and to demonstrate how a higher security and privacy can be achieved by the means of the CREDENTIAL Wallet, **three different pilots** in the domains eGovernment, eHealth and eBusiness are developed by the project (Hörandner et al., 2016); in brief:

- **eGovernment**: the pilot focuses on identity management to authenticate citizens and assess their eligibility for a service, based on sensitive identity attributes. Standardized identity protocols such as SAML or OpenID Connect should be used in CREDENTIAL's identity management data sharing process. Within this protocol, the service provider (i.e., the data receiver) triggers the process by requesting authentication and identity attributes from the identity provider (i.e., the CREDENTIAL Wallet). The pilot will not only enabe authentication via national eID solutions but also cross-border authentication according to the eIDAS regulation. The CREDENTIAL Wallet reacts to the user consent and generates a re-encryption key, whilst the service provider receives re-encrypted attributes disclosed in a selective way.
- **eHealth**: The pilot focuses on secure data sharing between patients, doctors, and further parties, in the field of Type 2 Diabetes. In particular, the process applies to patients, which can use mobile devices to record their health data, those data are collected by a CREDENTIAL e-Health mobile app which remotely stores them in the CREDENTIAL Wallet. This data sharing approach offers several advantages to the patient, such as enhanced privacy by minimizing disclosed data, having a continuous control of health data, as well as saving time and money for personal visits.

- e**Business**: The pilot focuses on the integration of modular libraries implementing CREDENTIAL's technologies into existing solutions to provide additional value. In particular, it tackles the issue of forwarding encrypted mails, which are nowadays increasingly used by companies to protect data and products, when employees are not at work. In fact, according to the current legislation, an employee has to provide her private keys to access the company e-mail system to give the possibility to other colleagues to still read and eventually take over incoming mail. Through proxy re-encryption, an employee can generate a re-encryption key towards an authorized colleague and hand this key to the mail server before leaving. The mail server is then able to re-encrypt incoming mail during the worker's absence and forward it to the authorized colleague.

1.2 Aims and Scope of this Report

In order to demonstrate the CREDENTIAL Wallet solution, the demonstrated system has to be equipped with user interfaces. The development of user interfaces (UIs) brings with it the possibility to make assessments of different aspects of various user groups' preferences and experiences of such a service. It also makes it possible to develop guidelines for usability and understandability assessments. This report covers the work and considerations made within the CREDENTIAL project during its first one and a half year to produce a first version for the UI prototypes for people's access to and utilization of data stored in their CREDENTIAL Wallets. These prototypes will be further evaluated as will the assessment methods themselves in order to produce a second version further on in the project together with UI design patterns for relevant functions, and this work will also inform the design of the specific user interfaces of the pilot implementation. How this deliverable relates to different work packages and deliverables is explicated in section 1.3 below.

This report covers not only some essential UIs, but also the various sources for inspiration that have been used during the design work.

1.3 Related Deliverables

The design of the user interfaces serves to give specification for implementers of the CREDENTIAL UIs where such exists. Moreover, the design of the user interfaces makes it possible to assess the feasibility of individual steps that a user would have to go through in order to complete a desired goal. Problems to complete such steps, to understand the implications as regards data disclosures, and the willingness to use such an aid as this project elaborates will constitute inputs to future deliverables. The present deliverable draws from previous deliverables and contributes to coming deliverables in the following way.

D2.1, Scenarios and use-cases, outlines the first version of the use cases, but the present deliverable relies more on D6.1, see below, as the use cases have been refined since the publication of D2.1.

D2.6, User-centric privacy and usability requirements, as the preparation involved workshops and focus group, the results to be reported in D2.6 have influenced the thinking behind the various stages of the UI Prototypes V1, and similarly, the problems reported here in D3.1 concerning user understanding as well as future studies for V2, informs the work on D2.6.

D3.2, UI Prototypes V2 and HCI Patterns, is the second and final version of the general user interfaces for the CREDENTIAL Wallet. It will not only build on the UI presented in the present deliverable but will also infer HCI design patterns from these studies and future studies.

D5.1, Functional Design, provides the basic functionalities (cf. also D4.1), but the present deliverable has relied more on task analyses of the use cases presented in D6.1.

D6.1, Pilot use cases specification, outlines in detail the pilot use cases, why the task analysis reported here has been adjusted according to deliverable D6.1 (compare above about D2.1).

D6.4-6, Test and evaluation report of pilot domain [1-3]: The user tests and possibly other user tests made for the development will inform the development of the pilots.

1.4 Outline

This report is structured in the following way. The following section, 2 Methodology, explains the general approach to UI development within the project, and then also the various methods employed for gathering data whether secondary data or primary data from user studies.

Section 3, Task Analysis, gives brief summaries of the use cases mentioned in section 1.1 which are planned to be piloted in the project, but most importantly this section provides a detailed task analysis wrought out for the development on the UI prototypes presented in this deliverable.

Section 4, General UIs for CREDENTIAL, gives the *general* UIs needed for the CREDENTIAL Wallet while section 5, eHealth-specific UI, presents sketches for the UIs needed for the special apps that go with the *eHealth* pilot – this is the only pilot needing special UIs for the pilot-specific applications.

Section 6, Research Challenges: Adoption of New Technologies, gives an overarching view of factors affecting user adoption and understanding of the CREDENTIAL Wallet. It points out the spectrum of research challenges in order to explain research planned or under way within the CREDENTIAL project.

Finally, section 7, Conclusion and Outlook, sums up the lessons learned and hints on the content of the deliverable for the Version 2 UI prototypes.

2 Methodology

This section describes the approach taken in the work reported in this deliverable. As the user interface mockups constitute the main part of the deliverable, the focus has been on the development of these: below, we account for the user-centred design approach taken and the role of prototyping. The literature reviews conducted so far, while also connected to more general questions of user adoption of technology, are set in the context of the CREDENTIAL prototype development cycle, as is also task analysis as well as user evaluation by usability testing and questionnaires, and the role of interviews. More specifics of the usability test conducted in the evaluation of the third draft of UI Prototypes V1 are found in section 4.2.

2.1 User Centred Design

The requirements for the kind of technology that CREDENTIAL tries to develop are many and difficult to meet. The solution must work in existing information ecologies and provide a distinct advantage over existing security and privacy solutions. These are concerns from security specialists, business developers, and authorities. In CREDENTIAL, Work Package 2 collects and elaborates these requirements. Parallel to such expectations from service providers and their users, are requirements for the usability of the CREDENTIAL solutions. They too will depend on the existing information ecologies and the digital service landscape, and the usability and adoption rate of existing solutions.

For the development of the front end of the CREDENTIAL pilots, the project has adopted a design approach that recalls the Human-Centred Design approach described by ISO 9241-210: "an approach to interactive systems development that aims to make systems usable and useful by focusing on the users, their needs and requirements, and by applying human factors/ergonomics, and usability knowledge and techniques" (International Standard Organization (ISO) 2010). User requirements are among the stakeholder requirements that have been considered right from the start in the CREDENTIAL project by exploring research literature literature and mapping legal privacy requirements form the General Data Protection regulation (GDPR) to Human-Computer Interaction (HCI) requirements, following the approach by Patrick and Kenny (2003), as well as studying existing solutions, and the requirements of the pilot use cases. Thus, the Human-Centred Design approach concerns the whole design, evaluation, and development cycle, where workshops and focus groups carried out with stakeholders and user representatives have played (see D2.6) and will play a significant role.

UI prototyping is brought into this process to gain an understanding of how well the CREDENTIAL UIs would possibly work in a real context by using the prototypes to gauge ease of use but also other aspects such as preferences, experiences, and learnability. Insights into this will be used in the further project work as explained in 2.2. The sections following thereafter briefly describes the methods applied for data generations that have to varying extent influenced the development of the UI Prototypes V1.

2.2 Literature Reviews

As the work on the user interfaces started already a few months into the project, it was dependent on input from literature reviews made in conjunction to the research. Some reviews are on major theoretical strands, *Diffusion of Innovation* and *Technology Acceptance Model*. Other reviews have been more targeted on specific question on organisations' or end-users' perception of specific types of solutions for

identity management. Also reviews of actual login solutions for various services have been made even if the selection of login procedures was limited to one by fingerprint and one by pin code.

2.3 Prototyping for User Interface Development

Within the broad approach that the CREDENTIAL project applies, the work on user interfaces has a specific task assigned to it, besides the UI development carried out as a result of the implementation of the key technologies and the demonstrator pilots.

The UI design work has followed an iterative process where three major drafts of the general UI for a citizen/customer using a smartphone have been developed before the user test reported here, after which a fourth draft adding some options for the user was added. Input has come from various processes which not all have been directed to usability and users' perceptions but rather to clarify what different scenarios proposed by project partners in project meetings, internal documents and diagrams, would actually mean. In the same time, inputs from pilot-specific workshops and other requirements gathering processes have also served this work, as well as insights and inspiration from the literature surveys belonging to the initial phases of the research work.

As indicated above, evaluation by usability testing has also started, and will continue for the refinement of the UIs to D3.2. Also within the pilots' development will user evaluations be made (as described in D6.1). The user tests and possibly other means of user demonstrations made for D3.2 will inform the pilots and the user evaluation work on the pilots will inform the work on the general UI finally reported in D3.2.

2.4 Task Analysis

Researchers frequently recommend designers to build user-centred systems that enable people to reach their goals, take account of natural human limitations, and generally are intuitive, efficient and pleasurable to use (Preece, Rogers, Sharp, 2002). The tasks users have to complete when using CREDENTIAL-based technology will determine how efficiently, pleasantly, etc., they can reach their goals.

Task analysis techniques, which provide a framework for the investigation of existing practices to facilitate the design of complex systems, are particularly important because they enable rigorous, structured characterizations of user activity (Crystal and Ellington, 2004). Task analysis is especially valuable in the context of human-computer interaction (HCI). Designers should define user interfaces at an extremely low level with details about styles and widgets for example, while still mapping them effectively to users' high-level tasks. Inflexibility of computer interfaces magnifies the impact of interface design problems. Consequently, the close integration of task structure and interface support is especially crucial (Crystal and Ellington, 2004).

Task analysis is widely recognized as a fundamental way not only to ensure some user-centred design but also to improve the understanding of how a user may interact with a user interface to accomplish a given interactive task (Hackos and Redish, 1998). Task analysis aims at ensuring that the system design allows the users to achieve their goals (Diaper, 2004). Performing a task analysis enables researchers to understand the users' activities in the context of an existing or future system (Kieras, 2004). Redish and Wixon (2003) explain that a task analysis can be constructed throughout the project as analysis is relevant

at any stage. For instance, at some stage one may apply the technique to analyse the efficiency of actions. Redish and Wixon also explain that at the beginning of a project – during the creation of application design – it is important to determine what the exact workflow for the users is and what the conditions are.

Many task models, task analysis methods, and supporting tools have been introduced in the literature and are widely used in practice. The methods have their own scopes and their differences. Diaper and Stanton provide a thorough review of selected, significant task models along with their method and supporting tools in their *Handbook* (Diaper and Stanton, The Handbook of Task Analysis for Human-Computer Interaction, 2004). Existing task models show a great diversity in terms of formalism and depth of analysis. According to Diaper' and Stanton's *Handbook*, different task models are used to achieve a range of objectives: to inform designers about potential usability problems, to evaluate human performance, to support design by providing a detailed task model describing task hierarchy, objects used, and knowledge structures or to generate a prototype of a user interface.

One of the most common task analyses is hierarchical task analysis. It was developed in the late 1960s as a response to the need for a rational basis for understanding the skills required in tasks (Diaper, 2004). Crystal and Ellington (2004) explain that hierarchical task analysis concerns breaking tasks into subtasks. When a set of goals and issues is assembled, the analyst can begin to specify how these goals should be achieved using a hierarchical task analysis approach. Data, in hierarchical task analysis, may be derived from different sources (Redish and Wixon, 2003; Diaper and Stanton, 2004). Hierarchical task analysis was adopted (see section 3) to analyse the design proposals and to see what users should do to achieve their goals in different CREDENTIAL use cases. It is important to ensure that the scenarios are covered by the UI prototypes.

2.5 Usability Test of Prototyped Functionalities

For this first version of the CREDENTIAL UIs, we have made one major test with users recruited outside of the project (Rubin and Chisnell 2008). Even if a usability study can be thought of as aiming for a swiftly functioning service which users mindlessly can safely use, minimizing task completion times are not the aim in this project, but rather to find what are obstacles for user, especially as concerns their ideas – their mental models – of the solutions developed within the project. In order to address questions of preferences, experience, and understandability, our usability test was followed by a questionnaire. In the future, the user evaluations may include semi-structured interviews.

In order to test the prototype a hierarchical task analysis was performed to find the essential steps and to design tasks to give to the participants within a limited scenario. Further screens were made to match a defined scenario to answer research questions constructed for questions related to specific items in the UI as explained in section 4.2, Evaluation with Users.

The test was conducted using screen designs prototyped using Balsamiq and made interactive with Axure[1] and shown on a laptop and a smartphone which the test moderators provided. The test was made in

[1] For more information tools and equipment used, see section 4.2.

English although the actual testing was conducted in Sweden. The participants were told to imagine having a CREDENTIAL account and wanting to sign up (Task 1), and later on sign in (Task 2) to a prototyped service provider via its web site. In this way the participants were presented with the authorization (and later the authentication) screens on the mobile phone.

As performance indicators, task completion (main indicator) and duration (for future reference) was used.

After each scenario (i.e., Task 1 and Task 2) had been completed the participant were given a questionnaire of System Usability Scale (SUS; Brooke, 1996) and other questions related to the CREDENTIAL app. The SUS was introduced by Brooke in 1986 and aims to assess a user's or test participant's view of the usability of an interactive product. Ruoti et al. (2015; also, Ruoti and Seamon, 2016) propose that usability studies concerning authentication systems should use a standard metric like SUS, and we followed this (cf. 4.2.2).

Finally, a general questionnaire captured some standard demographics (e.g., age, educational background, gender), familiarity with authentications services, and questions for analysing participants' comprehension of the CREDENTIAL Wallet solution and data disclosure.

A stratified sampling at Karlstad University was used to select 20 participants, to have equal representations of sex and age. The sample consisted of academics in the age range of 20-60. None was an IT specialist.

2.6 Semi-structured Interviews

One method very common in qualitative oriented, explorative usability testing are semi-structured interviews, that is, interviews where not all questions are designed or planned before the interview, allowing the interview to follow and explore new directions as they come up in the interview process (Bernard 1988). They can be performed after a test session instead of a questionnaire with open questions, and they can be performed as walk-throughs either instead of a plain usability test or after such a test. Such interviews will target specific issues while leaving it open for the participants to verbalise their feelings and understanding. Semi-structured interviews are considered a good method for capturing the challenges regarding understandability and preferences in standard literature on usability testing (e.g. Rubin and Chisnell 2008). However, this method has not yet been applied for external persons but only in project-internal review discussions of the earlier drafts of the UI Prototypes V1. For the work on V2, this method is expected to be used also with external persons, for instance with the members of the User Advisory Board.

2.7 Ethical Considerations

Before the work with external participants in tests, focus groups and workshops commenced, a description of the work planned and the relation to the CREDENTIAL project in large was evaluated to assess possible needs for ethical approvals. The plan described the recruitment of participants who provide their informed consent. Besides, the plan described routines for handling and anonymising data at the earliest possible time, providing transparency and guaranteeing data subject rights to all participants. As no

sensitive data were obtained and rules of the EU Directive were clearly followed, no ethical or legal privacy concerns were seen.

3 Task Analysis

As mentioned previously in section 2.4, task analysis methods focus on different levels of analysis and contribute different insights. In this report, we have adopted the hierarchical task analysis to obtain a clear understanding and descriptions of what users should do to achieve their goals in different CREDENTIAL use cases, to represent those descriptions and to evaluate the system against functional requirements. Obtaining clear understanding and descriptions of what users should do to achieve their goals, we can highlighting users' workflow and the most common tasks between different use cases. When the common and the most required tasks are extracted, we can focus on designing and mapping proper interfaces for those tasks and conducting the user studies to gradually ameliorate them.

In this section, based on the definitions of selected use cases which are briefly described here and elaborated in D6.1 in more detail, a hierarchical task analysis for each of the selected use cases in eGovernment, eHealth, and in eBusiness is presented. This section ends with a summary of the analysis highlighting the implications for the UI prototyping reported in sections 4 and 5.

3.1 eGovernment

LISPA has considered two use cases for CREDENTIAL project: Lombardian and foreign citizen get access to eGovernment services. In the following, we have generally analyzed the tasks users should undertake to achieve the goals of each use case.

The eGovernment pilot aims at experimenting incremental levels of security and to simplify the relationship and interactions between users and the government.

The pilot is based on a Lombardy Region Service SIAGE web portal provided to citizens and companies to request tax breaks and other types of fiscal advantages. The Pilot scenario previews a new way to access to the Service using CREDENTIAL Wallet for preserving the citizen data and guarantee a higher privacy level.

SIAGE and its users can have several benefits using CREDENTIAL as it is meant to provide a user-friendly and secure way to share eGovernment-related identity data, while the users stay in full control of their personal information.

The CREDENTIAL architecture is integrated to assure confidentiality during secure user online authentication, to demonstrate cross-border interoperability and to securely get user data, stored in an encrypted form in the Wallet.

The benefits over the state of the art are:

- Any Identity Provider can be plugged into the CREDENTIAL architecture and can be used to release an identity assertion; the only effort requested is to add a component, called "IdP Adapter", created to translate several authentication protocols.
- User can store into the Wallet additional data in addition to the pure identity data; those data benefit from the same encryption and CREDENTIAL components which assure that only the target Service Provider can access to plain data.

- User data, released by an Identity Provider, are encrypted; only target Service Provider can decrypt those values. This goal is possible thanks to proxy re-encryption technique.
- During authentication, user can apply a selective disclosure of her/his data, in order to forward to Service Provider just the personal data she/he wants.

LISPA eGovernment pilot mainly consists of two use cases.

1. *Lombardian Citizen Accesses eGovernment Service*
2. *Foreign Citizen Accesses eGovernment Service*

For the justification of the selection of these two use cases, see section 4.3.3 in D6.1.

*

Use case 1: Lombardian citizen gets access to the eGovernment services

Brief description: A Lombardy citizen signs into a Lombardy Regional Service (SIAGE) using IdPC, the Lombardy Region Identity Provider. The CREDENTIAL Wallet may be used in order to retrieve additional user data if it is needed for the service provider.

- Conditions: The Lombardy citizen has a CNS smartcard, its PIN, and a smartcard reader. The Lombardy citizen has a CREDENTIAL account and a working Credential app installed on his/her device.
- Goal: A Lombardy citizen requests an eGovernment service like tax breaks or paying house rent from the SIAGE service provider.
- Desired outcome: The Lombardy citizen can successfully login to SIAGE and submit the request regarding tax breaks, for example.

Tasks:

Plan: Do 1.1 to 1.4 sequentially, 1.5 is optional and then do 1.6 to 1.7.

1.1. Go to the SIAGE website to login and request tax breaks.
1.2. Authenticate to the SIAGE service provider first.
1.3. Select IdPC between different IdPs to authenticate.
1.4. Insert CNS into the smart card reader.
    1.4.1. Provide the PIN.
1.5. Select the CREDENTIAL Wallet to send more data to the SIAGE service.
    Plan: Do 1.5.1 to 1.5.5 sequentially.
    1.5.1. Enter the CREDENTIAL Wallet account in the proper place
    1.5.2. Run the CREDENTIAL app on the mobile device.
    1.5.3. Scan the fingerprint to login to the CREDENTIAL app if it is logged out.
    1.5.4. Select the desired information among available data to be sent to the SIAGE from the CREDENTIAL Wallet.
    1.5.5. Accept sharing the selected data with the SIAGE service provider from the CREDENTIAL Wallet.
1.6. Go back to the SIAGE website.
1.7. Fill out the form for requesting the tax breaks on the SIAGE website.

For retrieving data from the CREDENTIAL Wallet during the login process to the SIAGE service provider using the IdPC, there are three options. Among the different options, we assume that the user can login first to the SIAGE service provider using the LISPA's IdPC, and subsequently select the CREDENTIAL Wallet to import more data to the SIAGE service provider (with separate authentication data). If the Wallet trusts (and technically supports) the LISPA's IdPC, the user can authenticate using the LISPA's IdPC and the resulting IdPC assertion is then sent to the Wallet. For a valid assertion, the Wallet would then issue an access token. In this case, task 1.5 will be completely replaced by just task 1.5.4 and 1.5.5 on the SIAGE website. Despite the different options, to help users to achieve their goals in this use case we need authorization interfaces (1.5.4 and 1.5.5).

Use case 2*:* Foreign citizen gets access to the eGovernment services

Brief description: A Spanish citizen sign into a Lombardy Regional Service using CREDENTIAL Wallet app as the identity provider.

- Conditions: The foreign citizen has a CREDENTIAL account and a working CREDENTIAL app installed on his/her device.
- Goal: The foreign citizen wants to authenticate to the SIAGE service.
- Desired outcome: The foreign citizen can successfully authenticate to the SIAGE service.

Tasks:

Plan: Do 2.1 to 2.4 sequentially.

2.1. Go to the SIAGE website to login.

2.2. Authenticate to the SIAGE service first.

2.3. Select the CREDENTIAL Wallet between different IdPs to authenticate.

Plan: Do 2.3.1 to 2.3.3 sequentially.

2.3.1. Enter the CREDENTIAL Wallet account in the proper place.

2.3.2. Run the CREDENTIAL app on the mobile device.

2.3.3. Scan the fingerprint to login to the CREDENTIAL app if it is logged out.

Plan: Do 2.3.3.1 to 2.3.3.2 sequentially or just do 2.3.3.3.

2.3.3.1. Select the desired information among available data to be sent to the SIAGE from the CREDENTIAL Wallet.

2.3.3.2. Accept sharing the selected data with the SIAGE service provider from the CREDENTIAL Wallet.

2.3.3.3. Accept the authentication request.

2.4. Go back to the SIAGE website.

In this use case, the ultimate goal is to authenticate to the SIAGE service provider which can be fulfilled using the authentication (2.3.3.3) and authorization (2.3.3.1 and 2.3.3.2) interfaces. If for authentication to the SIAGE service provider, new pieces of the user's personal information is required, the user should first give her consent to disclose that information in the authorization screen exercising the selective disclosure function. Otherwise, the user should just accept the request in the app to assure the SIAGE that she is the right person to get access to it.

3.2 eHealth

The eHealth pilot aims to demonstrate how novel cryptographic technologies offered by the CREDENTIAL Wallet and its libraries can be integrated in established eHealth standards. One of the main concepts for the eHealth pilot is the patient health record (PHR). The PHR is the storage of all medical related data and documents for a patient. For example, it holds the medication plan or health related activity data. The PHR itself is managed and owned by the patient. Thus, the patient has the initially rights to add data to the PHR. By agreeing on a medical treatment relationship to a certain doctor, access rights are granted to the doctor. The doctor is able to view or add new data after this consent is given.

The eHealth pilot introduces a couple of pilot-specific services that targets the abstraction of established eHealth services as well as the integration with the CREDENTIAL services. Figure 3-1, adapted from D6.1, shows the functionality between the main components in the eHealth pilot where the two "PHR" boxes represents the two pilot-specific services.

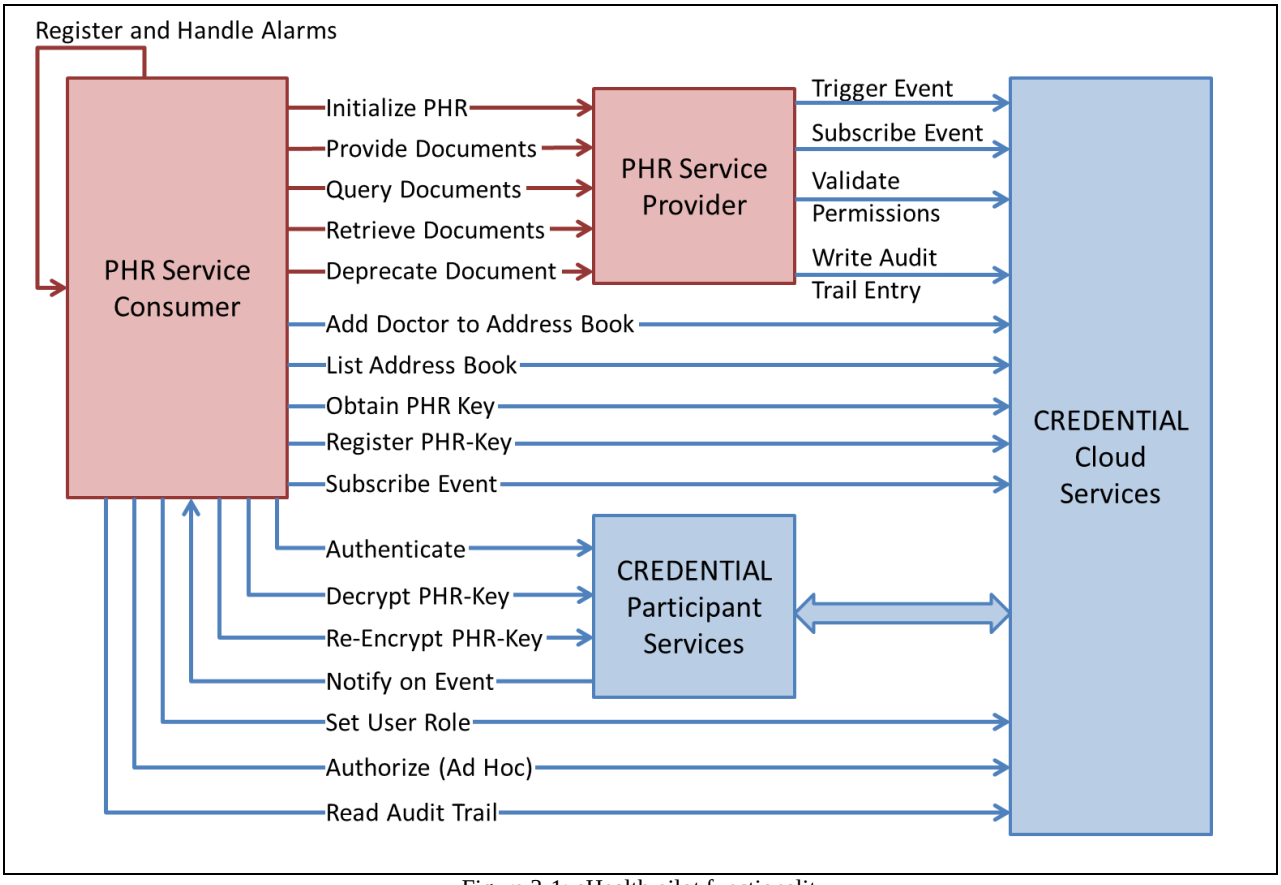


Figure 3-1: eHealth pilot functionality

The following six use cases have been chosen for the eHealth pilot:

1. *Care Planning and Progress Tracking*. This use case is considered as the entry point for patients in the CREDENTIAL Wallet. A new PHR for the patient is created and sharing information between the patient and the doctor is stored in the CREDENTIAL Wallet.
2. *Nutrition and Activity.* A patient has already a CREDENTIAL account. She collects medical and health related data by herself and decides to share her data with a doctor. Notifications about the document to be shared are forwarded to the doctor.
3. *Therapy Monitoring and Screening for Complications.* To assist the doctor, a threshold system is integrated in her IT-System. Before she receives notifications of newly added data, the IT-system computes if the incoming data may exceed certain thresholds. Thus, a pre-filtering of incoming data streams can be made and only relevant data for the doctor are shown.
4. *Oral Medication.* This use case elaborates a medication plan, where the doctor is able to publish certain medications and a time plan which describes when the patient has to take which amount of medicine.
5. *Insulin therapy*. A slight modification of the previous use case. The doctor also adds information and guidance of how many insulin intakes the patient has to perform. This information is stored in the medication plan document.
6. *Application for a Wearable Glucometer*. Glucometer devices are handed out by the patient's insurance company. In order to qualify for a bonus programme information about the medical treatment relationship with the patient's doctor has to be distributed. Therefore, selective disclosure of verified healthcare related data plays a huge role in this use case.

The justification of the selection of these use cases are that they directly derive from the "Diabetes type 2" focus mentioned in the introduction to section 5.3 in deliverable D6.1. For a more general reason for focusing chronic diseases, see the argument above in section 6.2 on adoption factors for the CREDENTIAL Wallet.

*

Use case 1: Care planning and Progress tracking

Brief Description: This use case focuses on the definition of therapy goals and continuous tracking of progress towards these goals. The diabetologist is responsible, at the first visit and the follow-up visits every three months, to collect core vital data (e.g., blood pressure, HbA1c, blood sugar) from the patient and upload it to her PHR (personal health record) and to inform her about her recent situation and further diseases which may show up if the patient is not able to control her diabetes at a reasonable level. In the first visit, the diabetologist also gives the patient the tracker devices like glucometer and helps the patient to pair it with her phone and guides her how to use it.

- Conditions: The patients and doctors have the CREDENTIAL accounts and working CREDENTIAL app installed on their devices. The patients also have the eHealth patient apps and the health records are set up and the required accesses are granted when they visited their doctors. The doctors have also the eHealth doctor app.
- Goal: To define and monitor or track the therapy goals and progresses.

- Desired outcome: Patient's health data are measured by tracker devices and uploaded to her PHR so the diabetologist has immediate access to it when needed. Also, the diabetologist monitors the patient's measured data and produces lab reports from the visits and uploads to the patient's PHR.

Role 1: Diabetologist.

Tasks: (Pre-condition) Set up the personal health record for the patient (the first visit with patient)

Plan: Do 1.1 to 1.5 sequentially.

1.1. Open the eHealth doctor app.
1.2. Fill the form of patient registration (manually or by reading the health card)
1.3. Give the paper consent to the patient and confirm that as a doctor you fully informed the patient.
1.4. Print and give the code to the patient (e.g., the QR code).
1.5. Help the patient to scan the code in her eHealth patient app to continue.

Tasks: Provide necessary documents the patient's PHR

Plan: Do 1.1 to 1.3 sequentially, 1.4 is optional and then do 1.5.

1.1. Open the eHealth doctor app.
1.2. Authenticate to eHealth doctor app using the CREDENTIAL app.
1.3. Within the eHealth doctor app, find the specific patient.
1.4. Access to the patient's records and check the vital data being uploaded by the patient (because previously the doctor received the required permissions from the patient)
1.5. Access to the patient's records and create a new document and upload it (e.g., initial health status and definition of care goals for the first visit and lab reports for follow-up visits) (because previously the doctor received the required permissions from the patient) – the patient receives a notification for the newly uploaded data if it is set in her eHealth patient app.

Role 2: Patient

Tasks: (Pre-condition) Set up the personal health record/give access permissions to a doctor for the whole PHR

Plan: Do 1.1 to 1.6 sequentially.

1.1 Go to visit the doctor.
1.2 Give consent by a paper consent form and give it back to the doctor
1.3 Open the eHealth patient app.
1.4 Authenticate to the eHealth patient app using the CREDENTIAL account.
1.5 Scan the code given by the doctor in the eHealth patient app.

1.6 Accept the authorization requests in CREDENTIAL app (it pops up when the patient scans the code)

Tasks: Connect the required tracker devices (with the doctor's help)

Plan: Do 1.1 to 1.4 sequentially.

1.1 Open the eHealth patient app.
1.2 Authenticate to the eHealth patient app using CREDENTIAL app.
1.3 Navigate to find the connected devices.
1.4 Search for devices and pair them.

Tasks: Measure the data by the tracker devices

Plan: Do 1.1

1.1 Use each device individually and it sends the data it collects automatically to the PHR.

The required pre-condition for setting up the PHR and giving access to the diabetologist at the first visit is described in this first use case and will not be repeated in the following use cases. For any other doctors (e.g., diet specialists), in order to have access to the whole PHR, at the first visit with the patient they give a code to the patient and the patient scans the code to give the permission.

Use case 2: Therapy monitoring and screening for complications

Brief Description: This use case focuses on the doctor's review process. The diabetologist is responsible for monitoring and documenting the progress of therapy by using the alarm registration functionality, scheduling regular visits to other specialists and assembles relevant data into a short report for patients that can be shared with other specialists in a way that they can provide patients with their feedback.

- Conditions: The patients and doctors have the CREDENTIAL accounts and working CREDENTIAL apps installed on their devices. The patients also have the eHealth patient apps and the health records are set up and the required accesses are granted to the doctors. Also tracker devices are connected to the eHealth patient app collecting the vital data. The doctors have also the eHealth doctor app.
- Goal: To monitor the therapy by the diabetologist and to involve other actors into the treatment process.
- Desired outcome: Thresholds can be defined and registered for supporting a fine grained monitoring of the patient's performance and compliance and relevant specialists can use their eHealth doctor apps for sharing treatment related (diagnostic) data with the patients and the diabetologist.

Role 1: Diabetologist.

Tasks: Provide short reports and set alarms if necessary

Plan: Do 2.1 to 2.3 sequentially, 2.4 is optional and then do 2.5 to 2.6 sequentially.

2.1. Open the eHealth doctor app.
2.2. Authenticate to eHealth doctor app using the CREDENTIAL app.
2.3. Within the eHealth doctor app, find the specific patient.
2.4. Set alarms to better catch critical situations for this patient (e.g., if certain monitoring data for more than 3 days is not provided)
2.5. Access to the patient's records (because previously the doctor received the required permissions from the patient).
2.6. Create a new short report for the patient (because previously the doctor received the required permissions from the patient).

Role 2: Specialist.

Tasks: Provide feedback and comments

Plan: Do 2.1 to 2.5 sequentially.

2.1. Open the eHealth doctor app.
2.2. Authenticate to eHealth doctor app using the CREDENTIAL app.
2.3. Within the eHealth doctor app, find the specific patient.
2.4. Access to patient's reports created by the diabetologist and write comments/give feedback (because previously the specialist received the required permissions from the patient).
2.5. Create new comments/feedback for the patient and upload it to the PHR (because previously the specialist received the required permissions from the patient).

Role 2: Patient.

The patient app (the patient is using the tracker devices) is automatically and continuously sending the vital data to the PHR which with the pre-conditions for giving access to other actors are described in the definition of the first use case.

Use case 3: Nutrition and activity

Brief Description: This use case focuses on the first phase of core processes of diabetes therapy. The diabetologist is responsible in this use case to help the patient to change the diet and increase daily activity. A diet specialist works in this use case with the diabetologist. The diet specialist gives an activity belt to the patient which allows her to record the number of steps she takes a day. For the new additional care goal the diabetologist updates the patient's car goal document. The patient records all the food intake in a specific period and uploads it to the PHR. The diet specialist assesses the data and provides feedback.

- Conditions: The patients and doctors have the CREDENTIAL accounts and working CREDENTIAL app installed on their devices. The patients also have the eHealth patient apps and the health records are set up and the required accesses are granted when they visited their doctors. Also tracker devices are connected to the eHealth patient app collecting the vital data. The doctors have also the eHealth doctor app.

- Goal: To change the patient's diet and help the patient to achieve the goals with the involvement of a diet specialist.
- Desired outcome: Care goal is updated and further vital data is monitored, stored and is assessed by diet specialist.

Role 1: Diabetologist.

Tasks: Update the patient's care goal document

Plan: Do 3.1 to 3.5 sequentially.

3.1. Open the eHealth doctor app.
3.2. Authenticate to eHealth doctor app using the CREDENTIAL app.
3.3. Within the eHealth doctor app, find the specific patient.
3.4. Access to the patient's records and find the specific document (because previously the doctor received the required permissions from the patient).
3.5. Download the document, update and upload it again (because previously the doctor received the required permissions from the patient).

Role 2: Diet specialist.

Tasks: Provide feedback and comments

Plan: Do 3.1 to 3.5 sequentially.

3.1. Open the eHealth doctor app.
3.2. Authenticate to eHealth doctor app using the CREDENTIAL app.
3.3. Within the eHealth doctor app, find the specific patient.
3.4. Access to patient's records and find the eating habit document (because previously the specialist received the required permissions from the patient).
3.5. Asses the data and provide the feedback and upload it to the patient's PHR (because previously the specialist received the required permissions from the patient).

Role 3: Patient

The patient app (the patient is using the tracker devices) is automatically and continuously sending the vital data to the PHR. The patient should also give access permissions to the specialist and also should attach the new device to her phone which are all the other examples of pre-condition tasks described for the patient and the doctor in the first use case. Also, the patient needs to manually add some vital data.

Tasks: Create and upload the eating habits

Plan: Do 3.1 to 3.4 sequentially.

3.1. Open the eHealth patient app.
3.2. Authenticate to eHealth patient app using the CREDENTIAL app.

3.3. Navigate to the section for manually adding vital data and create a document.
3.4. Gradually add the eating habits to that document and update it

Use case 4: Oral medication

Brief Description: This use case focuses on the second phase of the core processes of diabetes therapy. The diabetologist is responsible to assess the patient's health data and consider her ongoing changes in her lifestyle and prescribes the proper medicine. The medication plan is also created and uploaded by the family doctor (here, the diabetologist) which lists all the required medicines and gives advice on how and when to take them.

- Conditions: The patients and doctors have the CREDENTIAL accounts and working CREDENTIAL app installed on their devices. The patients also have the eHealth patient apps and the health records are set up and the required accesses are granted when they visited their doctors. Also tracker devices are connected to the eHealth patient app collecting the vital data. The doctors have also the eHealth doctor app.
- Goal: To prescribe a new medicine and create and update the medication plan.
- Desired outcome: Medication plan is created, updated and uploaded to the PHR.

Role 1: Diabetologist.

Tasks: Create and update the patient's medication plan

Plan: Do 4.1 to 4.4 sequentially.

4.1. Open the eHealth doctor app.
4.2. Authenticate to eHealth doctor app using the CREDENTIAL app.
4.3. Within the eHealth doctor app, find the specific patient.
4.4. Access to the patient's records and add a new medication plan with required notes and definitions for the patient (because previously the doctor received the required permissions from the patient).

Role 2: Patient.

The patient app (the patient is using the tracker devices) is automatically and continuously sending the vital data to the PHR which with the pre-conditions for giving access to other actors are described in the definition of the first use case.

Use case 5: Insulin therapy

Brief Description: This use case focuses on the third phase of the core processes of diabetes therapy. The diabetologist is responsible for creating a care plan that shows when the patient needs to inject how many units of insulin. Additionally, the medication plan is updated to include the insulin that is prescribed to the patient and the frequency of blood sugar measurements is adapted. The adapted plans are stored in the PHR.

- Conditions: The patients and doctors have the CREDENTIAL accounts and working CREDENTIAL app installed on their devices. The patients also have the eHealth patient apps and the health records are set up and the required accesses are granted when they visited their doctors. Also tracker devices are connected to the eHealth patient app collecting the vital data. The doctors have also the eHealth doctor app.
- Goal: To add the insulin medicine to the medication plan and to create a care plan for insulin therapy and upload it to the PHR.
- Desired outcome: Medication and care plan is created, updated and uploaded to the PHR.

Role 1: Diabetologist.

Tasks: Add insulin medicine to medication plan

Plan: Do 5.1 to 5.4 sequentially.

5.1. Open the eHealth doctor app.
5.2. Authenticate to eHealth doctor app using the CREDENTIAL app.
5.3. Within the eHealth doctor app, find the specific patient.
5.4. Access to the patient's records and add a new medication plan with required notes and definitions for the patient (because previously the doctor received the required permissions from the patient).

Tasks: Create and upload the new care plan

Plan: Do 5.1 to 5.4 sequentially.

5.1. Open the eHealth doctor app.
5.2. Authenticate to eHealth doctor app using the CREDENTIAL app.
5.3. Within the eHealth doctor app, find the specific patient.
5.4. Access to the patient's records and add a new care plan to the patient's documents (because previously the doctor received the required permissions from the patient).

Role 2: Patient.

The patient app (the patient is using the tracker devices) is automatically and continuously sending the vital data to the PHR which with the pre-conditions for giving access to other actors are described in the definition of the first use case.

Use case 6: Application for a Wearable Glucometer

Brief Description: This use case focuses on the request for the reimbursement of specific devices with the Medical Review Board. The Medical Review Board reviews the necessity of such a device for a patient. In order to do so, the patient needs to disclose different sets of treatment data to the health insurance company and the Medical Review Board. Therefore, malleable signatures will be used, to disclose the desired data.

- Conditions: The patients and doctors have CREDENTIAL accounts and the CREDENTIAL app installed on their devices. The patients also have the eHealth patient apps and the health records are set up and the required accesses are granted when they visited their doctors. Also, tracker devices are connected to the eHealth patient app collecting the vital data. The doctors have also the eHealth doctor app.
- Goal: Provide patient's care related data to the Medical Review Board
- Desired outcome: Medical Review Board receives patient's care related data. Patient receives a positive outcome of the Medical Review Board's assessment.

Role 1: Doctor

Task: Assemble a therapy summary document

Plan: Do 6.1 to 6.6 sequentially.

6.1. Open the eHealth doctor app
6.2. Authenticate to eHealth doctor app using the CREDENTIAL app
6.3. Within the eHealth doctor app, find the specific patient
6.4. Create a therapy summary document with the following patient information
    a. Diagnoses
    b. Care Status
    c. Therapy progress
    d. Selected compliance indicators
6.5. Apply a malleable signature over each of the provided information
6.6. Upload the therapy summary document to the PHR

Role 2: Patient

Task: Receive therapy summary document and mark parts of the document as accessible for Medical Review Board

Plan: Do 6.1 to 6.6 sequentially.

6.1. Open the eHealth patient app
6.2. Authenticate to eHealth patient app using the CREDENTIAL app
6.3. Find the notification about the newly added therapy summary document
6.4. Add the Medical Review Board to the address book
6.5. Disclose at least Diagnoses and Care Status from the document for the Medical Review Board
6.6. Forward the therapy summary document to the Medical Review Board

This completes the sixth and last of the eHealth use cases.

For each use case in eHealth scenario: both the eHealth app and the CREDENTIAL app should be installed on the user's device. During the setup process for the eHealth app, users are requested to give their permissions to the eHealth app to access their data in the CREDENTIAL Wallet which is handled via authorization interfaces. Also, in all use cases, some medical data are transferred between different

legitimate actors like doctors, patients and specialists. Patients should give their consents if they want to share their medical data with the doctors and specialists or other actors in eHealth use cases. Patients can give their consents to share their data with others through authorization interfaces. Moreover, doctors and patients should authenticate to their eHealth app using the CREDENTIAL app which is handled by authentication interfaces. Consequently, in the eHealth scenario authorization and authentication user interfaces play an important role and most of the actors' tasks need those interfaces to be completed.

3.3 eBusiness

InfoCert has considered three use cases for CREDENTIAL project: 1) InfoCert E-commerce login and registration, 2) Legalmail encrypted message forward, and 3) Legalmail contract form filling. In the following, we have generally analyzed the tasks users should undertake to achieve the goal of each use case.

InfoCert motivates the reliance on CREDENTIAL technology in the following way in D6.1: "Today many business processes in many market sectors can be performed online. But there is always a trade-off between security and usability: in fact, often the online services that are simple for users do not guarantee the right level of security and privacy. On the other hand, to implement safer processes companies sacrifice usability for users. Based on the above, in eBusiness pilot we analyzed the most widespread use cases related to the technologies developed under the project: among these, there are the authentication and Single Sign-On (SSO), the purchase processes and online form subscription, the use of digital signature software and web communication tools with legal value. All with the aim to show how the new technologies developed and CREDENTIAL services can meet the needs of security and privacy but also guarantee a simple user experience." (p. 51)

The following use cases have been chosen for the eBusiness pilot:

1. *User uses a web-based application for e-commerce login.* The user will be able to login to the InfoCert e-commerce using the CREDENTIAL Wallet. Some data must be imported to let the InfoCert e-commerce create a user account and bind it to the user's Wallet.
2. The user, after logging in with CREDENTIAL Wallet, can request a Legalmail mailbox. Part of the contract form can be filled with *data imported* from the CREDENTIAL Wallet.
3. *User uses a mobile application for forwarding mail*. The Android Legalmail app will request to the CREDENTIAL Android app to generate a re-encryption key and will send it to the Legalmail server, which will store it and use it, by means of the CREDENTIAL Java libraries, when a forward filter is activated. The receiver of the forwarded message will use the Android Legalmail App which requests the CREDENTIAL Android app to decrypt the session key which, when returned, will be used to decrypt the original content.

Notably, the last use case does not use the CREDENTIAL Wallet but the features provided by the CREDENTIAL mobile app and the CREDENTIAL Java libraries.

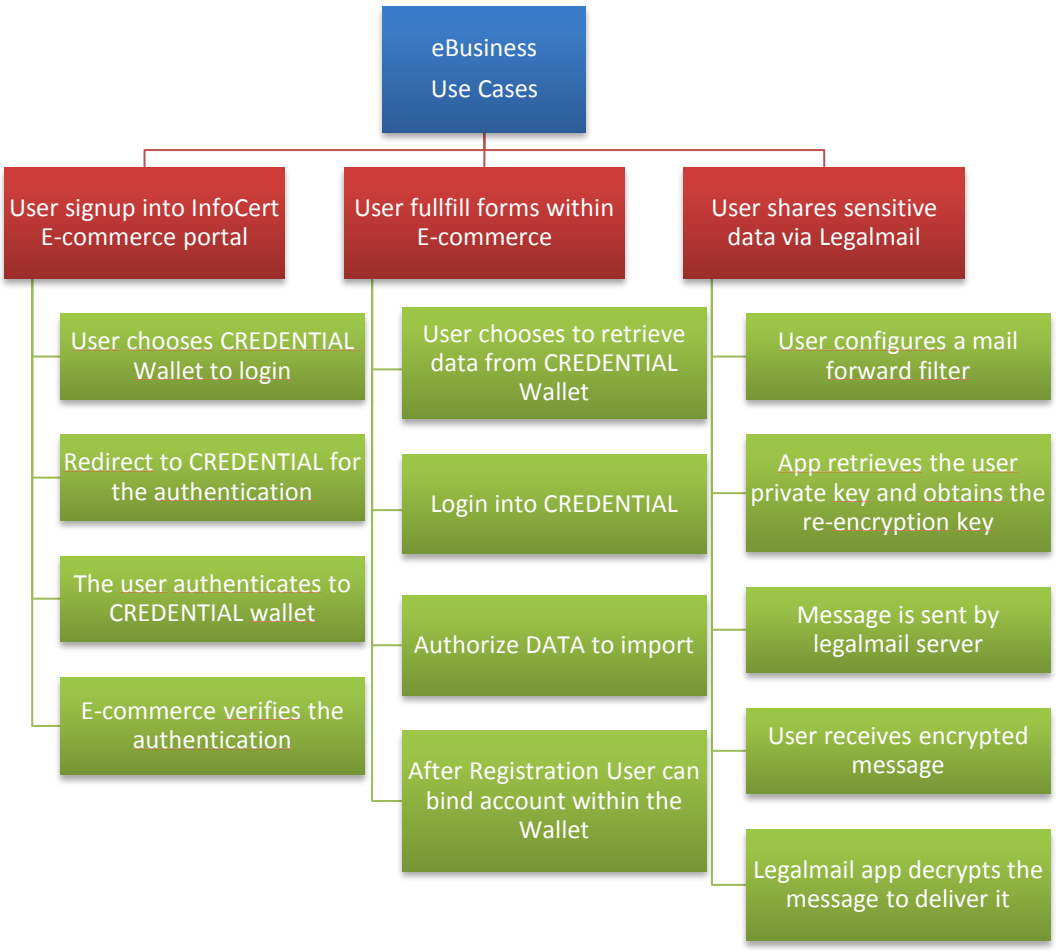


Figure 3-2: Selected use cases of the eBusiness pilot. (Figure 24 in D6.1)

For the justification of the selection of these three use cases, see section 6.3.4 in D6.1.

*

Use case 1: InfoCert e-commerce: login and registration.

Brief description: The user can login and register to the e-commerce, create an InfoCert account, without the need of an additional credential and has the ability to use the authentication and the data provided by CREDENTIAL.

- Conditions: The user has a CREDENTIAL account and a working CREDENTIAL app installed on her device.
- Goal: The user wants to login/register to InfoCert E-commerce
- Desired outcome: being authenticated/registered to InfoCert E-commerce

Tasks:

Plan: Do 1.1 to 1.3 sequentially.

1.1. Go to login/registration page of InfoCert E-commerce.
1.2. Select the CREDENTIAL Wallet to login/register to InfoCert E-commerce.
Plan: Do 1.2.1 to 1.2.3 sequentially.
1.2.1. Enter the CREDENTIAL Wallet account in the proper place on InfoCert website.
1.2.2. Run the CREDENTIAL app on the mobile device.
1.2.3. Scan the fingerprint to login to the CREDENTIAL app if it is logged out.
Plan: Do 1.2.3.1 to 1.2.3.2 sequentially or just do 1.2.3.3.
1.2.3.1. Select desired information among available data to be sent to the InfoCert from the CREDENTIAL Wallet.
1.2.3.2. Accept sharing the selected data with the InfoCert E-commerce from the CREDENTIAL.
1.2.3.3. Accept the authentication request.
1.3. Go back to InfoCert website.

The response to the login or registration request will bring the authentication result and the information required. When the authentication is successful, if an InfoCert account is linked to that specific CREDENTIAL account ID, a session will be created and the access will be allowed to the user. If the CREDENTIAL account ID has not been stored previously, an InfoCert e-commerce account will be created with the username and the new CREDENTIAL account ID attributes that just have been received.

In this use case, to help users to achieve their goals to login or register to InfoCert E-commerce, we need to provide them with two main set of interfaces for authentication and authorization. Being able to register for InfoCert, some users' personal information may be required. Users should share their information from their CREDENTIAL Wallet with the InfoCert under their valid consent which is done in authorization process. Being able to login to InfoCert, previous user's consent should be still valid and an assurance about the user's identity is needed. It means that InfoCert should be able to assure that the user is the one who claims to be which is done in authentication process. Consequently, in this use case, by proper design of authentication (1.2.3.3 task) and authorization (1.2.3.1 and 1.2.3.2 tasks) interfaces users can achieve their goals.

Use case 2: Legalmail encrypted message forward.

Brief description: Using the Legalmail encrypted messaging, the user configures a mail forward filter towards a trusted person who will be able to read the contents of the encrypted message.

- Conditions: The user has a CREDENTIAL account and a working CREDENTIAL app installed on her device. The user also has a Legalmail account, a working Legalmail app installed on her mobile device and the user is signed into her Legalmail account using the CREDENTIAL Wallet.
- Goal: To configure a mail forward filter toward a third person for the messages received by a specific sender.
- Desired outcome: A forwarding email rule successfully being set in a way that the recipient can receive and visualize the encrypted email.

Tasks:

Plan for sender: Do 2.1 to 2.3 sequentially.

2.1. Go to the email settings to set a forwarding email rule in Legalmail app.
2.2. Set the characteristics of the forwarding rule (e.g. set a recipient for the emails from a specific sender).
2.3. Confirm the changes.

When the user wants to install and run the Legalmail app for the first time, the Legalmail app may need some permissions to use the crypto library from the CREDENTIAL Wallet app to request for the proxy re-encryption key and the recipient's public key, for example. Any permissions concerning users' personal information from Wallet can be granted using the authorization interfaces. Moreover, as mentioned in the conditions for this use case, the user signs into the Legalmail app using the CREDENTIAL Wallet. Consequently, in this use case, we also need authentication and maybe authorization interfaces to help users to achieve their goals.

Use case 3: Legalmail contract form filling.

Brief description: Import data into Legalmail subscription form (e.g. Legalmail mailbox contract form. When a user has signed into the InfoCert e-commerce web application, the user can request a Legalmail mailbox. The process for a mailbox request requires a contract form to be filled.)

- Conditions: The user has a CREDENTIAL account and a working CREDENTIAL app installed on her device. The user is also signed into the InfoCert E-commerce using CREDENTIAL Wallet app.
- Goal: A user wants to import data from the CREDENTIAL Wallet to a contract form.
- Desired outcome: Data successfully imported from the CREDENTIAL Wallet to a contract form and order a Legalmail mailbox.

Tasks:

Plan: Do 3.1 to 3.4 sequentially.

3.1. Go to the contract form for the Legalmail mailbox.
3.2. Select the CREDENTIAL Wallet to import data to the contract form.
Plan: Do 3.2.1 to 3.2.5 sequentially.
3.2.1. Enter the CREDENTIAL Wallet account in the proper place on InfoCert website.
3.2.2. Run the CREDENTIAL app on the mobile device.
3.2.3. Scan the fingerprint to sign into the CREDENTIAL app if it is signed out.
3.2.4. Select desired information among available data to be sent to InfoCert from CREDENTIAL Wallet.
3.2.5. Accept sharing the selected data with InfoCert E-commerce from CREDENTIAL.
3.3. Go back to InfoCert website.
3.4. Fill out and complete the contract form.

First of all, in this use case, users should be signed into InfoCert E-commerce website using the CREDENTIAL Wallet to be able to request a Legalmail mailbox. So as mentioned in the conditions for this use case, users need the authentication interfaces to achieve this condition. Moreover, to help users to achieve their goal which is importing data from the CREDENTIAL Wallet to a form in InfoCert website, we need authorization interfaces to help them select among available data to be imported and have their consent on this disclosure.

3.4 Summary of the Task Analysis

As mentioned in section 2.4, task analysis methods focus on different levels of analysis and contribute different insights. We did hierarchical task analysis to obtain a clear understanding and descriptions of what users should do to achieve their goals in different CREDENTIAL use cases. In order to manage the resources efficiently, we wanted to highlight the users' workflow in each use case and focus on the most common tasks between different use cases.

An inspection of these task analyses show that most tasks in the different use cases of the CREDENTIAL project can be completed using the authentication and authorizations UIs in the CREDENTIAL app. So the users can achieve their goals using those principal user interfaces.

For this reason the focus was geared to designing proper interfaces for authentication and authorization tasks and conduct the user studies regarding the usability and understanding of the concepts essential to those user interfaces. The other UIs are needed to help to exert some tasks in eHealth or to fulfill the pre-conditions needed in different use cases like having the CREDENTIAL app installed and registering a CREDENTIAL account, the functionality needed to manage the accounts as well as the functionality needed to manage the permissions given using the authorization interfaces. Accordingly, in the next section, we briefly describe and present the interfaces regarding the general functionalities in CREDENTIAL and then we concentrate on the authorization and authentication interfaces, and finally present the user study conducted on those interfaces and the results and lessons learnt from that study.

4 General UIs for CREDENTIAL

4.1 UI for General Functionalities

This section elaborates user interfaces for general functionalities in the CREDETIAL project based on the definition of general functionalities described in D2.1 and considering the HCI requirements derived from focus groups and legal principles in D2.6. In particular, these included HCI requirements and principles for achieving Consciousness, Comprehension of policy information and Consent, which were derived by mapping legal privacy requirements of the GDPR following the approach by Patrick and Kenny (2003).

The interfaces were refined through incremental and iterative processes until the last version for this deliverable was reached. The design process started with a first draft of the interfaces outlined in Marlvelapp online framework,[1] and continued based on feedback from project partners to a refined version in Balsamiq wire framing software[2] because with Balsamiq, designing and communicating the prototype was faster and easier. Then after a project-wide presentation in November 2016 of several open questions, the UI prototyping group received comments during the following weeks. The general user interfaces were manipulated accordingly to form the third version. The presentation of open issues for the general UI also helped to make clear diverging opinions about what the eHealth pilot presumed. Further discussions around the eHealth mockup (an earlier version than those found in section 5) helped drive that discussion forward. Moreover, the comments and discussions during a technical workshop held in February 2017 and a user study conducted in January 2017 to evaluate some important functionality in the project helped to improve the interfaces and finalize them for the fourth version which is depicted in this deliverable.

The colour scheme was chosen to map the CREDENTIAL Wallet logo, as this logo had to be included in the size of an icon. Some graphic design patterns were followed based on similar graphical design in existing smartphone apps. Through the process described above, the project members agreed the general CREDENTIAL Wallet UI to follow this overall design. It should be noted that many minute details are the result of the Balsamiq software for rapid prototyping of graphical layout of screens. Thus, every font size, every choice of font text, background braids, etc. can be contested. Balsamiq just provides one font to be used. The inclusion of this font in the UI Prototypes V1 does not mean it should be the font in the app. Implementers should use standard and common fonts for Android apps.

However, as our first user test shows (section 4.2.4.7), there was nothing seriously hampering users in this design. On the other hand, where better performance can be wished, namely in the area of understanding and having a clear memory of consents given, text design can be questioned, but also other things, for instance how consent to disclosure is made on individual data items and how authentications is made. Our design proposal for V1 as well as for further user testing is more focused on these interaction elements rather than on details of font selection for two reasons: 1) text sizes and contrast may be set by the

[1] https://marvelapp.com/
[2] https://balsamiq.com/

individual user on her own device, and 2) the major interaction paradigms have greater transferability to other, future designs of "wallets" based on the CREDENTIAL technology, than graphic details have.

To present the user interfaces designed for general functionalities, we used the categories for general use cases in D2.1 which are data management, authorization, authentication and account management. In the following, we present the most important UIs related to data and account management while the others UI related to this are found in the appendices. However, the interfaces for authorization and authentication functionalities are illustrated attentively as we justified in section 3.4 that they are the most important and most required interfaces in the CREDENTIAL project to help users to achieve their goals.

4.1.1 Account Management

In this section, we present the UI for managing the accounts in the CREDENTIAL app. Before being able to benefit from the CREDENTIAL app's functionalities, the users need to download and install the app and register an account. To begin with, we introduce a specific user called Elsa with whom we present the UI properties. Elsa has a smart phone and wants to download and install the CREDENTIAL app. She needs to register an account first. Then she can sign into her account and enjoy the CREDENTIAL app.

When it is the first time to download and install the app on a device (or it was downloaded before but uninstalled and the user wants to install it again), the CREDENTIAL features are concisely introduced to the users. They can swipe the screen to see the features one by one or they can skip it by clicking on the two buttons provided for registration and recovering of an account. The introduction UI is presented in Appendix A.

If the user has previously registered an account on another device, the user can recover it on a new device. On the other hand, if the user does not have any CREDENTIAL account, the "Register an Account" button should be clicked. Now, Elsa has clicked on the related button to register an account in CREDENTIAL. The related prototype for registration is depicted in Figure 4-1.

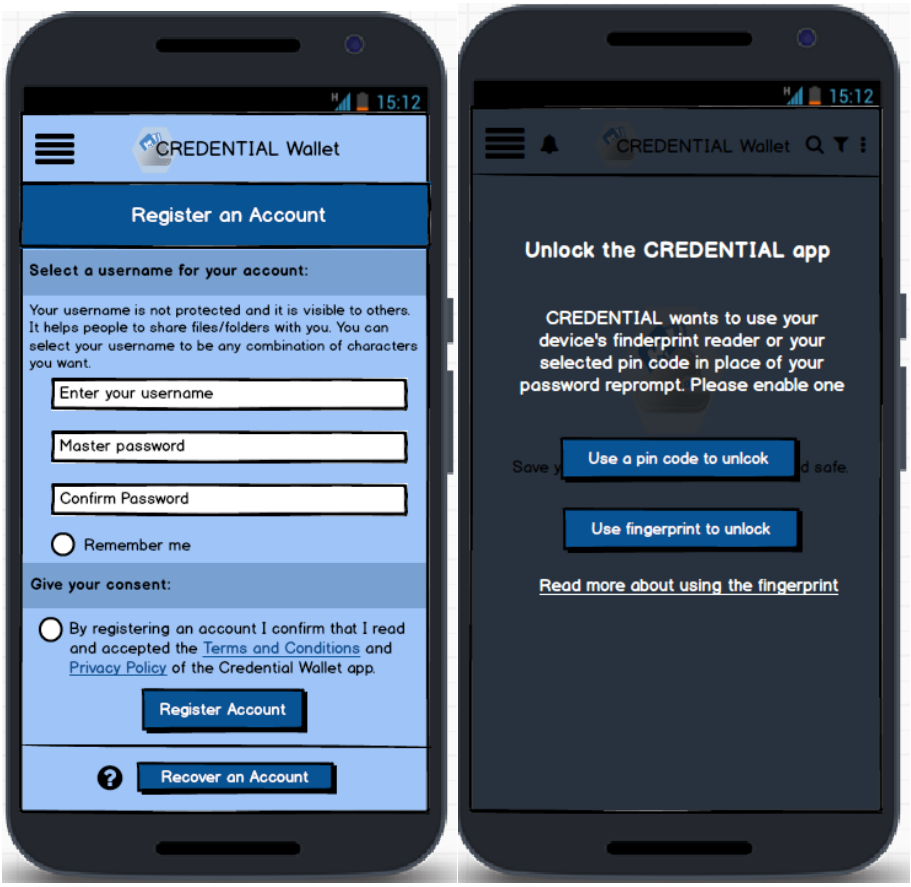


Figure 4-1: a) Register an account. b) Unlock the app

On the registration screen, Elsa should select a username which is not necessarily her email address or her name. It can be chosen from any combination of characters. Elsa should also select a password (master password) for her account and repeat it. Then Elsa needs to give her consent to the privacy policy and terms and conditions of the CREDENTIAL app. Once Elsa is done and clicks on the "Register an account" button, she is requested to select a way to unlock the CREDENTIAL app: 1) use fingerprint to unlock the app, and 2) use a pin code to unlock the app. So instead of entering master password to use the app when it is not signed in, she can use her preferred way to unlock the app.

As depicted in Figure 4-2, if Elsa selects the fingerprint, she will be requested to scan her fingerprint. If it is successful, a message is shown which conveys the current situation to unlock the app and includes a button linked to the settings (see Figure 4-15) for changing the method. On the other hand, if she is not comfortable with using her fingerprint or if her device does not support the required sensor, she can select to unlock with a four-digit pin code. If the fingerprint scanned is correct or when the pin code is set successfully, the proper messages are communicated with users because it provides more visibility (Nielsen 1994). There is a link providing more information about using the fingerprint; the content thus linked is depicted in Appendix B. If there are some registered accounts on the current device, the registration UI will have another button for signing in to an account.

When Elsa successfully registers her account (after selecting an unlocking method), she should save the recovery information for her account. She receives some instructions and she selects a pin code to protect the PDF file including the QR code of the recovery information. Then she downloads the file (see Figure 4-3). When she clicks on the button "Download the Recovery Code", the next screen shown to her is depicted in Figure 4-4. Elsa should print the PDF file or save the file safely (exactly how a user would safely store a QR code is outside the scope of CREDENTIAL, but see further discussion in Appendix F). Pressing the "Continue" button will guide her to the main page of the CREDENTIAL app (see Figure 4-7).

.

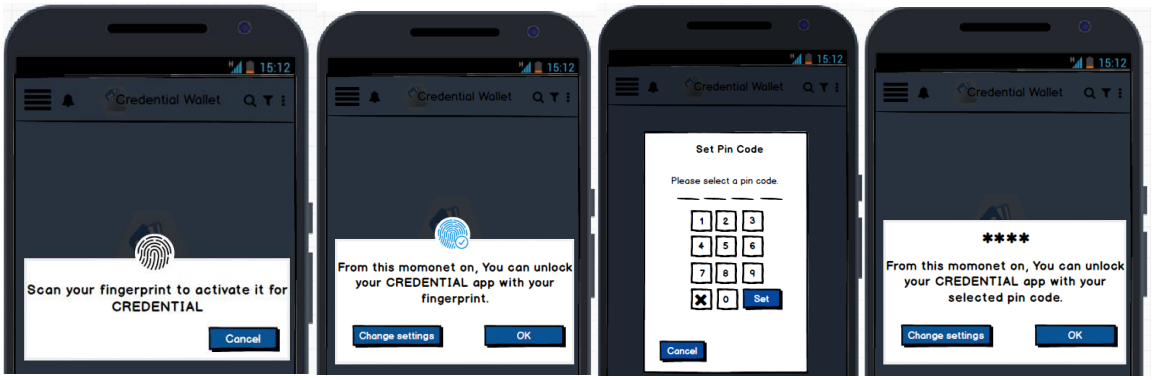


Figure 4-2 : Select the fingerprint or pin code to unlock the app

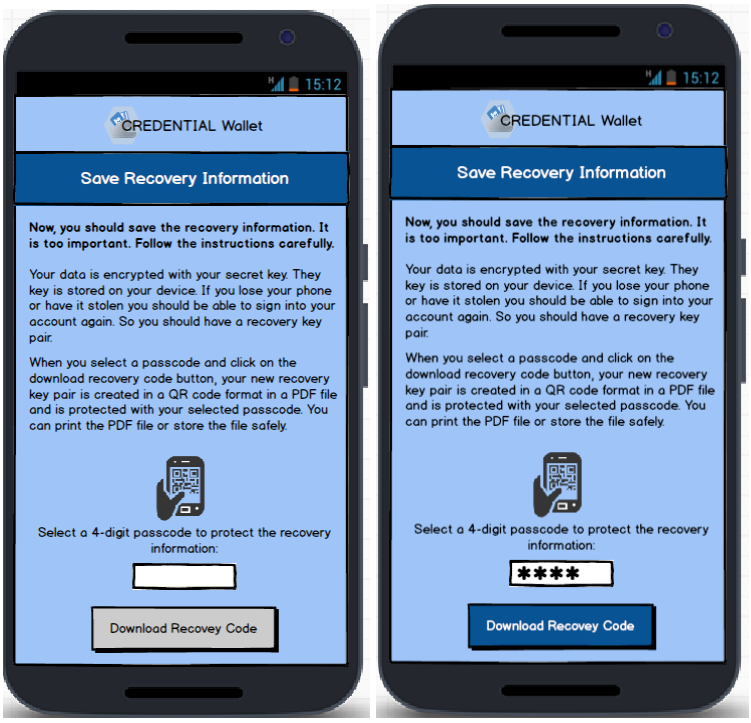


Figure 4-3: Save recovery information

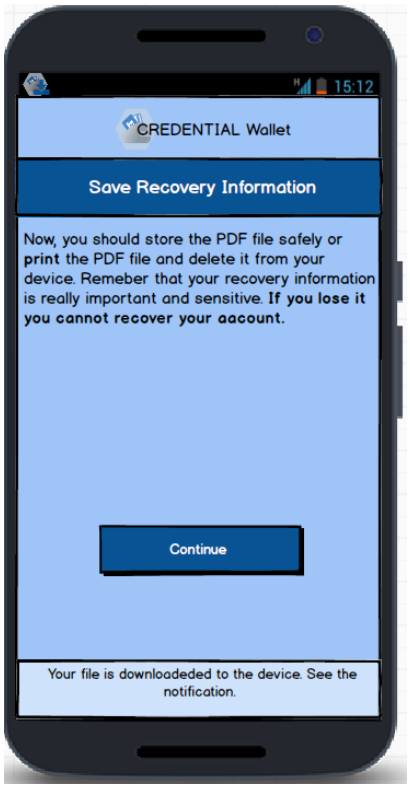


Figure 4-4: Save recovery information

If Elsa wants to recover an account, she should scan the recovery QR code given to her during the registration process of that account. Elsa scans the QR code as depicted in Figure 4-5 and then she follows the prototypes depicted in Figure 4-3 and Figure 4-4 to save the new recovery information for this newly recovered account. If there is an account registered (or recovered) on the device when Elsa opens the CREDENTIAL app to use it, she will see the related UI for signing into an account as presented in Figure 4-6.

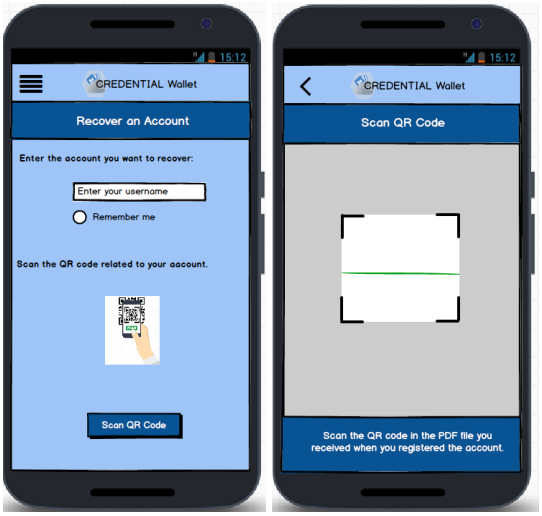


Figure 4-5: Recover an account

Figure 4-6: Sign-in to an account

4.1.2 Data Management

The CREDENTIAL Wallet is an identity provider and a file hosting service. Data management interfaces are related to the file hosting role of the CREDENTIAL. When a user uploads a file to the CREDENTIAL Wallet, the user can manage the file using different functions available in the CREDENTIAL app. The user can download, delete, define and manage the access rights to the file. Moreover, the user can view the activity logs, change the name and move the file. There is also the opportunity to search through the

available data in the Wallet and filter the data to just see the desired one. Furthermore, the user can set some notifications for the data on the Wallet and handle the requests to get access to the files from the others. In this section, we present the related user interfaces for each of the mentioned functionalities. Again, we present these functionalities with specific scenarios with a user called Elsa to make it clearer. Elsa has installed the CREDENTIAL Wallet app on her device and has a CREDENTIAL user name. So Elsa is registered in the CREDENTIAL. For now, we assume that Elsa is signed in to the CREDENTIAL Wallet app using the interfaces described in section 4.1.1.

The first view that Elsa can see is depicted in Figure 4-7. This view serves as a home view and by default she can see all the files and folders she owns in her CREDENTIAL Wallet which are sorted based on modification time in ascending order. The order to see the files can also be altered using the vertical ellipsis sign available in the header bar. Elsa can change the view to see the files and folders the others have shared with her as is shown in Figure 4-7. Also, she can select to see both. The prototypes for other types of view are depicted in Appendix C. For each of the available file/folder, Elsa can see the modification time, name and the status of sharing directly in the main view.

From this view, Elsa can access to all parts of her CREDENTIAL Wallet. We describe each of the elements in this view and how the elements can be mapped to the general functionalities concerning the data in the CREDENTIAL Wallet.

File/Folders Properties

Elsa can see what functions are available for each individual file/folder. If Elsa clicks on the vertical ellipsis sign shown in front of each file/folder, she can see the list of actions she can use for her files as depicted in Figure 4-8.

As depicted in Figure 4-8, for each file/folder, Elsa can see some properties of the files like the owner of it, if it is shared with others, modification and creation times and the size. In other words, there are some metadata available for each file/folder. Moreover, if Elsa wants to see the history of access to this file, she can click on the “view activity logs” and she can see the activity logs for a file chronologically. If Elsa herself has done something on the file, the device model is also shown to help Elsa better remember and realize the modification she made, because Elsa can access to her account from different devices. She can use the search and filtering functions available on the header bar to customize the access log view.

If Elsa wants to share the file with others or change the given access rights for the file, she can click on “Manage access rights” (Figure 4-9). Elsa can see who has access to the file and what the access type is. Also the date of authorization (first time to give permission to access the file) and the date of validity of the authorization are available. We have two kinds of authorization validity: 1) default validity date, and 2) being valid until it is revoked. For the files requested individually by doctors, the validity of access right is defined by default. So the user cannot revoke the permission before that time and after the validity date, the permission is revoked automatically. For the files and information requested by other service providers, we have two options. If it is mandatory information, it is not possible to cancel the access to a specific file if it is a part of a permission including other data as well. Instead the whole permission given to that service provider should be revoked. But if it is optional information it can be revoked easily by clicking on the recycle bin icon.

Also showing in Figure 4-9, if Elsa wants to share the file with more people, she can click on the icon located at the left bottom of this view and start adding new people to get access to the file which is shown in Figure 4-10. In Figure 4-10, Elsa can enter the usernames of the people with whom she wants to share the file and by clicking on the "Edit" icon below the input form, she can define different type of access rights to be granted to different users. To make the process more visible for the user, the previously granted access rights are shown at the bottom. Moreover, when users enter the new people's names to grant them access rights, the new names besides the type of access are shown.

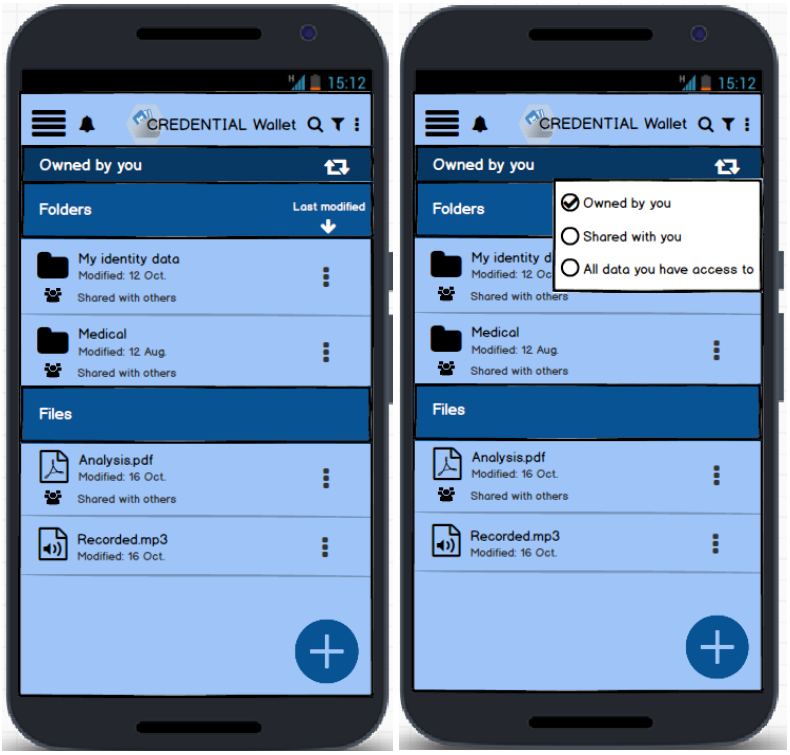


Figure 4-7: The main view of CREDENTIAL Wallet app

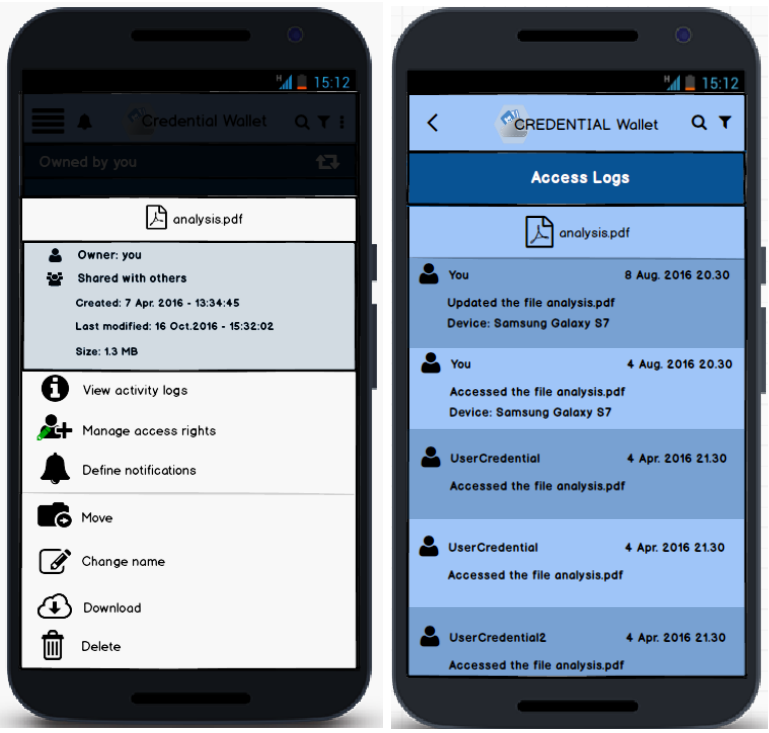


Figure 4-8: Functionalities for each fil (left) and Activity logs on a file (right)

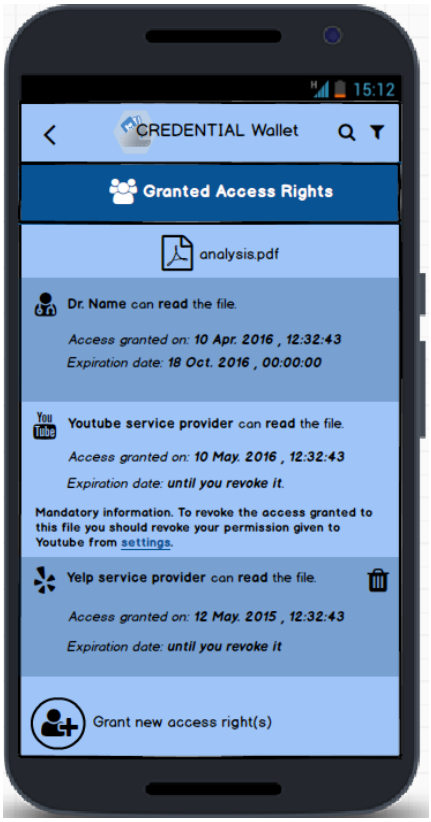


Figure 4-9: Granted access rights for a file

Furthermore, besides different general notifications available in CREDENTIAL, Elsa can define specific notifications for each file and it can be done by using the "Define notifications" for the target file. This is depicted in Figure 4-11. For each individual file, Elsa can define to receive notifications if it is edited or accessed. It is useful when the notification settings for being informed about changes and access to all shared files are not set. If Elsa wants to have more granular notification she can use advanced settings as shown in Figure 4-11. She can define to receive notifications when the file is accessed by a specific person, on special days in a week or special times or she can define a very specific date. Besides these functionalities, Elsa can also change the file path (move the file), rename, download or delete the file from her Wallet which is presented in Appendix D.

Create a New Folder or Upload Files: Plus Button

If Elsa wants to create a new folder or upload some files she can click on the plus button at the bottom of the main page and the select the desired functionality as shown in Figure 4-12. When Elsa selects the upload function, she should navigate through her files or folders on her device and select the ones she wants to upload. If she is done with selecting the desired files/folders, she will see what is depicted in Figure 4-13. The selected items are listed and there is an opportunity to define some access rights on the files selected if it is required. Moreover, Elsa is briefly informed about what is happening when she uploads some files. The steps to define the access rights are the same as the steps depicted in Figure 4-10.

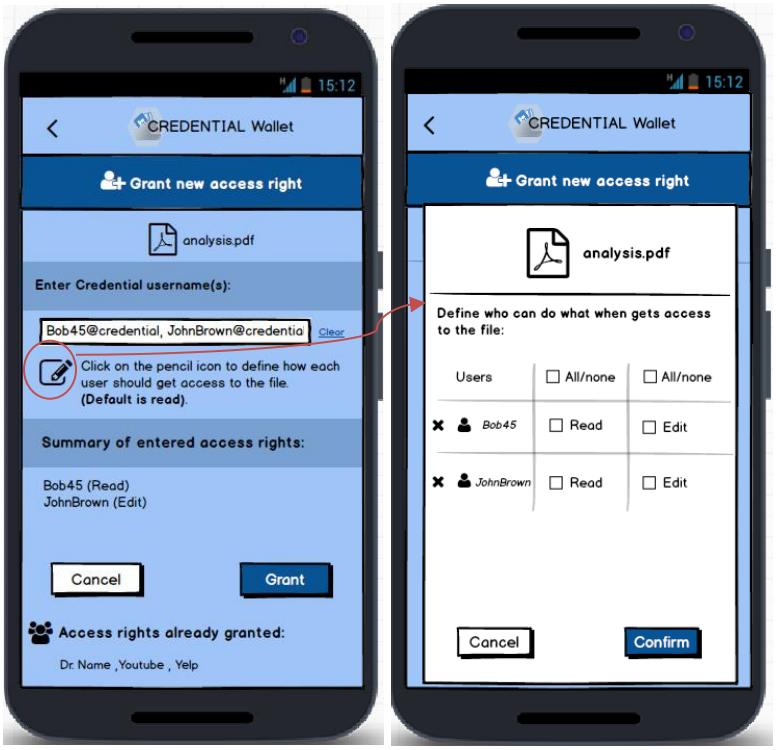


Figure 4-10: Granting new access rights on a file

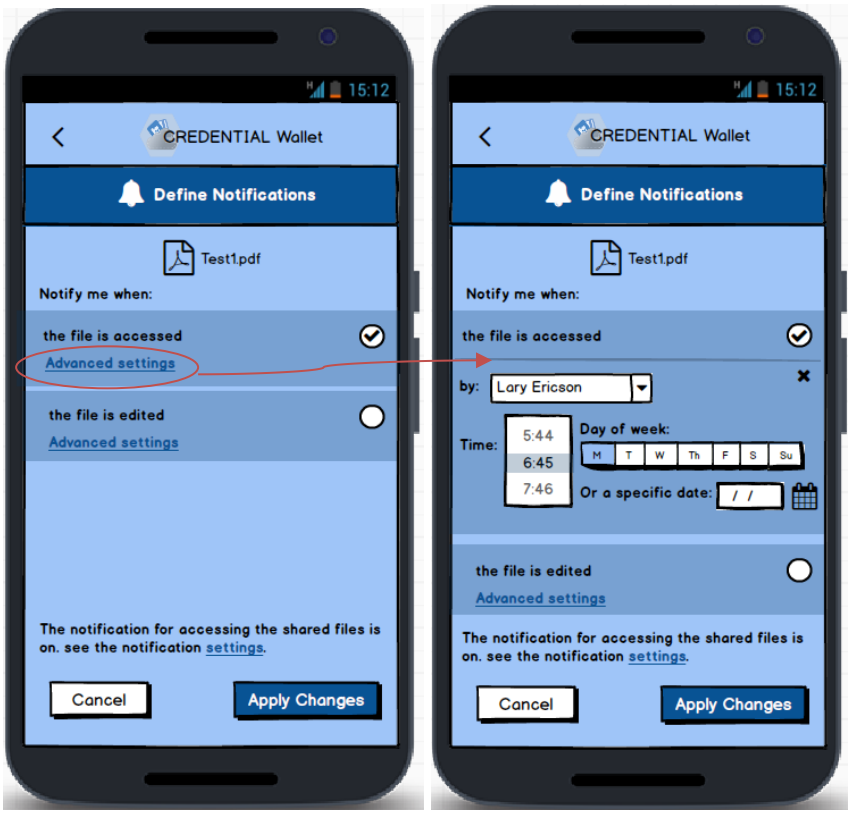


Figure 4-11: Define notifications for a file

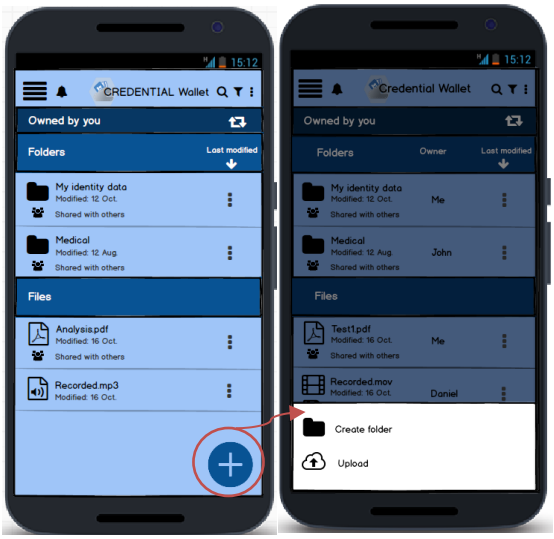


Figure 4-12: Button to upload files or create folders

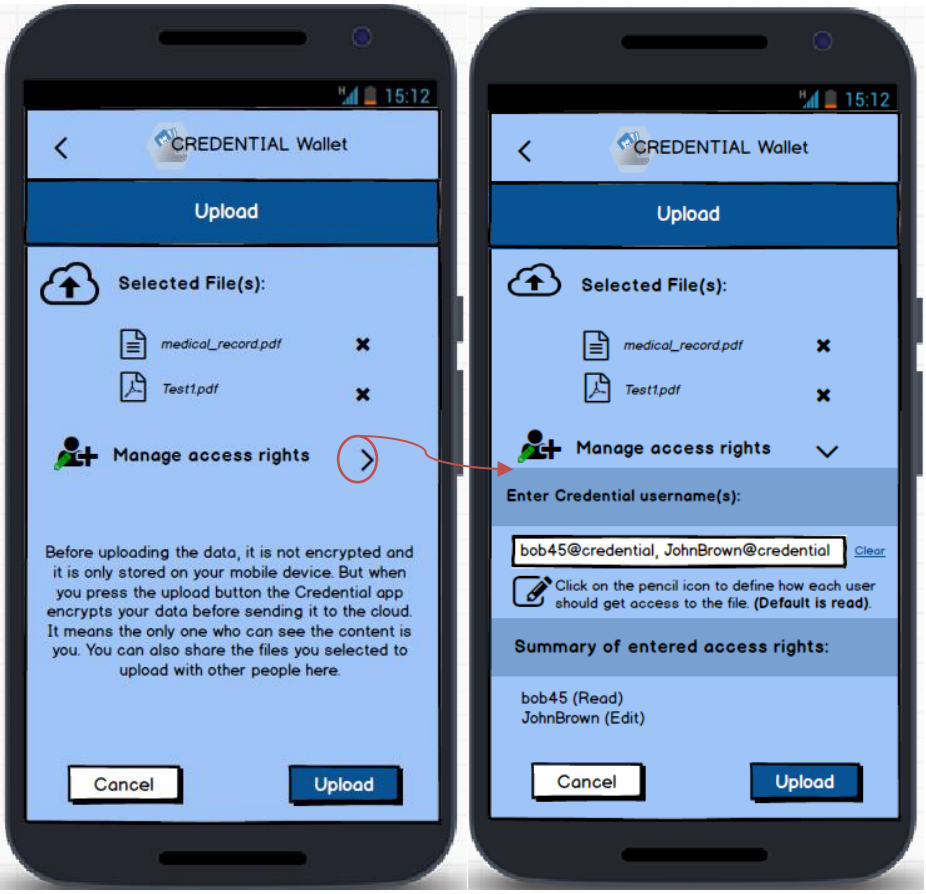


Figure 4-13: Upload files and define access rights if needed

Header Bar

On the header bar of the CREDENTIAL Wallet app, as shown in Figure 4-7, searching, filtering and some view functions are defined. These functionalities help users to limit the number of files and folders they want to see. For example, they can define to see the files being modified on a specific time or see the files based on their types. They can also search for a specific file/folder or they can select multiple files/folders to do the same actions on them. These functionalities are depicted in Appendix E.

Moreover, there is a menu icon on the top left of the header bar as shown in Figure 4-7 and if the user clicks on it, the list of items in the menu will be shown (see Figure 4-14). As depicted in Figure 4-14, the current account being singed in is also shown on the top. There is an "angle" icon to change the view easily between different accounts on the device as shown in Figure 4-14. If Elsa wants to change the view to see the content of the Wallet for another account, she can select the account from the available list and then the screen is changed to the "Sign into an Account" and she should provide her password. Needless to mention, when Elsa is not signed into her account or the app is locked all the settings items in the menu and sign-out functionality are deactivated.

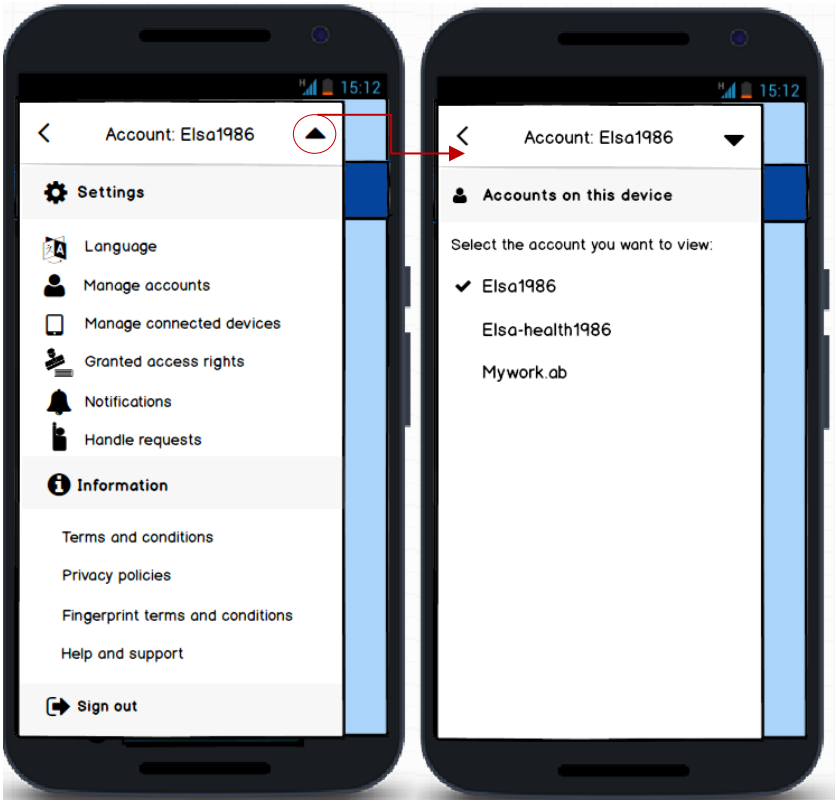


Figure 4-14: Menu items

On the menu list as shown in Figure 4-14, we have three different sections: 1) Settings, 2) Information, and 3) Sign out functionality. Under the "Settings" section, we have a "Language" option. CREDENTIAL Wallet should provide its services in different languages based on the targeted users. So Elsa can select her preferred language from the list when she clicks on the "Language" item. Moreover, in order to see the current account logs or to de-register the account from the CREDENTIAL Wallet, Elsa can click on the "manage accounts" item from the menu list. Represented in Figure 4-15, Elsa can change her preferable way to unlock the app and define how often she wants the app to be unlocked or signed out. The account logs are also accessible from the prototype illustrated in Figure 4-15. For each access log for the current signed in account (Elsa1987), the exact date, time, the mobile device, and the type of action are presented. So Elsa can see when she signed into her account from a specific device. By using the filtering and search icons mapped to related functionalities Elsa can find the events happened from a specific device or on a specific time, for example. If Elsa wants to de-register her account from the Wallet, she can clicks on the related link on the bottom of the prototype as depicted in Figure 4-15.

If Elsa wants to see from which devices she signed in to her current account (*Elsa1986*) she clicks on the "Manage connected devices" from the menu. List of different devices in conjunction with the access logs from each device and the ability to remove each device are available in the prototype depicted in Figure 4-15. If Elsa does not want to be able to sign in to her account from a specific device anymore, she can

remove the device by opening the “Connected Devices” screen by clicking the “De-register the account” link in the lower right corner, and then click the corresponding “Remove” button. When this is done, the account is no longer available from that device. If she wants to use her account on a removed device, she should recover the account again on that device.

Figure 4-15: Manage accounts screen

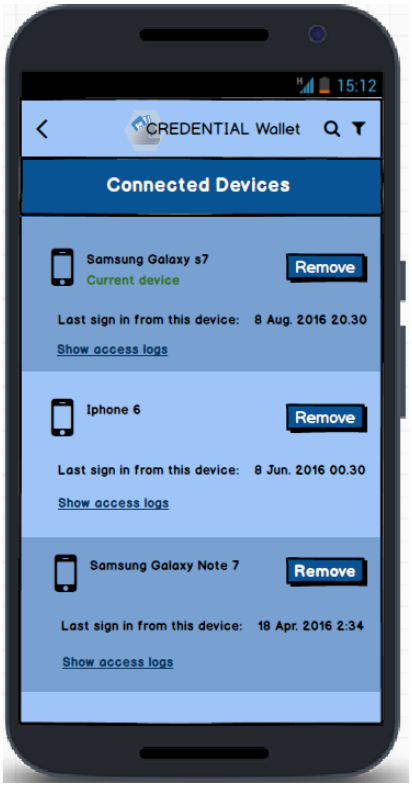


Figure 4-16: Connected devices

If Elsa is wondering to which entities she has granted access rights for her files and folders she can click on the "Granted access rights" item from the menu. As presented in Figure 4-17, Elsa can revoke any of the permissions she has granted previously. We have two types of granted permissions. One group are the permission given based on a request from a party and another group are the permissions given to a party initiated by Elsa herself without an explicit request from the receiver. In the figure, first the permissions granted to the first group are shown and if Elsa scrolls down the other permissions are also presented. Some requests require mandatory information like some request from service providers. As previously mentioned, mandatory information cannot be revoked one by one. On the contrary, if Elsa wants to revoke them, she should revoke the whole permission. But she can remove the access to optional information individually if she wants. For each receiver of the information, date of authorization and the type of access right are also presented. Moreover, there is a link to see the access logs for each entity. As shown in Figure 4-17, for the permissions given to the other CREDENTIAL users to have access to some files from Elsa's Wallet, the access type could vary from read to edit or the other type of access and it can be changed by clicking on the edit icon beside the type of access right. Finally, using the filtering and search functionalities, Elsa can find a specific receiver of her information and manage the permission given to it as she wants.

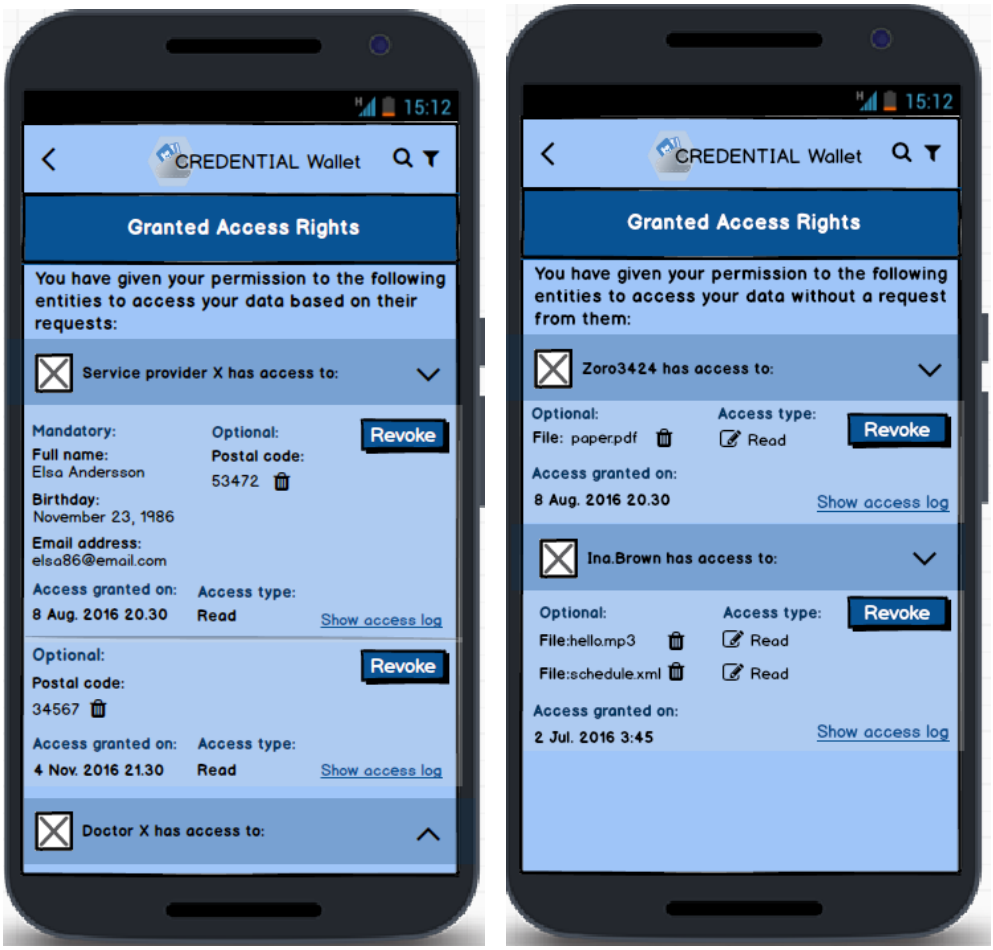


Figure 4-17: Granted access rights to different entities

Under the "Settings" section of the menu, users can also see the "Notifications" and "Handle Requests" items. If Elsa wants to see the notifications, she can clicks on the bell icon on the main page of the CREDENTIAL app as depicted in Figure 4-18 or she can clicks on "Notifications" from the menu. Based on the settings for notifications and granular notification settings for files/folders, notifications for the related events are listed with the detail about time and the event as shown in Figure 4-18. If the notification is a request from a third party like a doctor to access to a file, there is a direct link with which Elsa can handle the request immediately and if it is clicked it shows the authorization screen to have Elsa' consent. To change the notification settings, Elsa can click on the gear wheel icon at the right bottom of the prototype in Figure 4-18 which will lead her to a new prototype as shown in Figure 4-19.

Depicted in Figure 4-19, there are some general notification settings which Elsa can switch *on* or *off*. The notification for requests to access the data from her CREDENTIAL Wallet is always *on* by default, because it is important to notice and handle those requests.

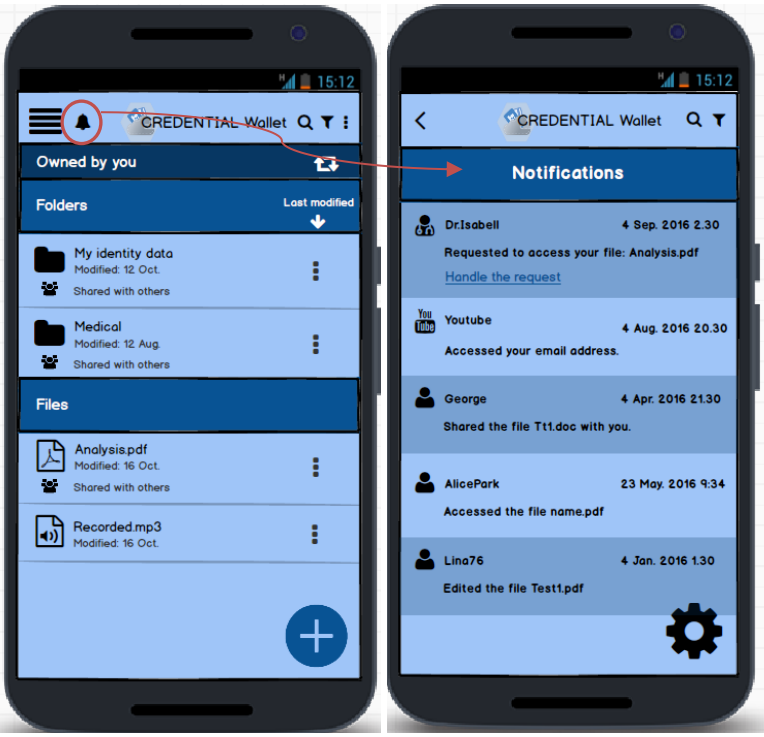


Figure 4-18: Show the notifications

Elsa can decide to receive general notifications when: 1) someone shares a file with her, 2) someone revokes the access previously granted to her for a file/folder, and 3) someone gets access to the files/folders she shared with them. She can also define granular notifications for files as described previously and depicted in Figure 4-11. She can review the notifications she has defined for files/folders by clicking on the related link in Figure 4-19. As illustrated in Figure 4-19, Elsa can review the notifications defined for files/folders and she can edit or remove the defined notifications.

Finally, if Elsa wants to see the list of all waiting requests for accessing her data from her Wallet and to handle them she can clicks on the “Handle Requests” item from the menu. As depicted in Figure 4-20, Elsa can see all the requesters with their full identity and contact information. Besides that the purpose of the request is mentioned briefly and the remaining time to handle the request is also shown. The requests are sorted based on their remaining time to be handled. If Elsa clicks to handle a request the authorization screen is shown to her (see).

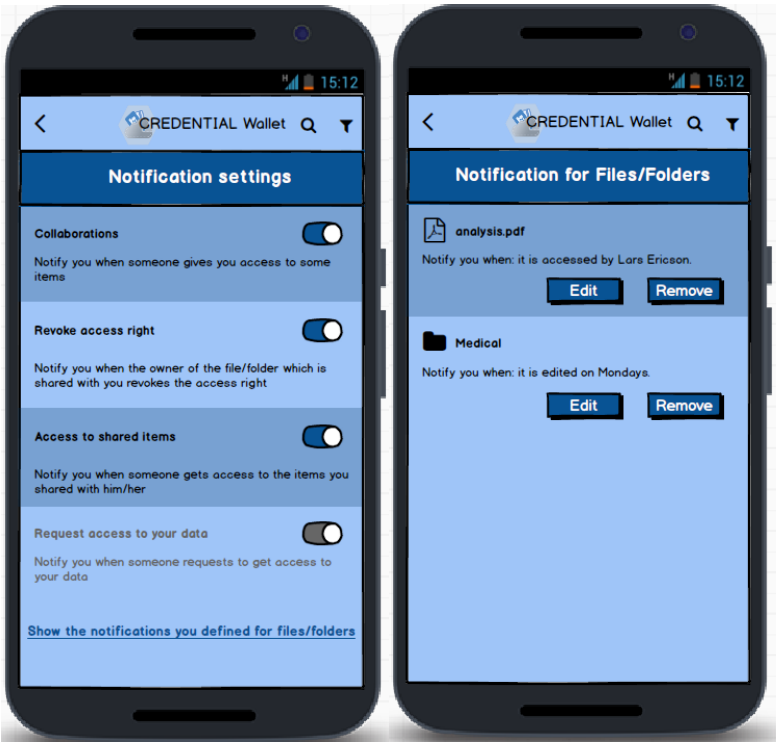


Figure 4-19: General notification settings (left) and notifications for files/folders (right)

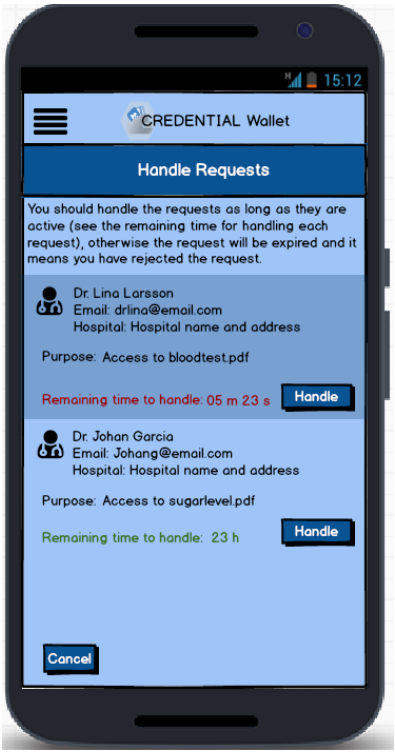


Figure 4-20: Handle requests

4.1.3 Authorization

Elsa wants to sign up for a service provider using her CREDENTIAL account or she wants to handle the request from a doctor to access her data from her Wallet. Generally speaking, when there is a request to access the data from the Wallet, the authorization functionality is needed. During the authorization process Elsa reviews the information being requested and in most cases she can benefit from the selective disclosure functionality. She is informed about the receiver of her personal data and the purpose of data requesting. To begin with, when a request is made, either the CREDENTIAL app opens automatically on her phone or she opens it herself, she should first unlock the account using her preferable method she set previously (based on her account settings she may need to sign into the app instead of unlocking the app). So as depicted in Figure 4-21, she sees a message telling that she has to unlock the app first. Obviously, for whatever reason that she opens the app she will see the message shown in Figure 4-21 based on her account settings before being able to benefit from any other functionality in the CREDENTIAL app.

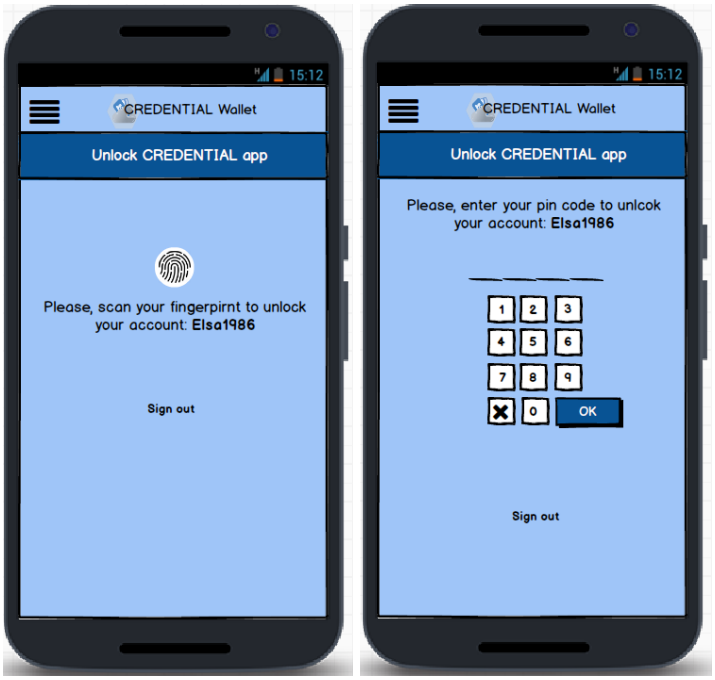


Figure 4-21: Sign into the account to see the request

When Elsa scans her fingerprint or enters her pin code and this is successful, she sees the authorization screen as shown in Figure 4-22. In this figure, the identity of the requester beside the contact information and its logo (or in some cases a picture of the person who asks for an access) is explicitly available for Elsa's attention. Mandatory and optional requested information are also shown distinctively. The exact personal information requested is also shown beside its title. For example, in Figure 4-22 not only the full name is mentioned but also the exact full name of the user is shown. The incorporation of end-user's personal information examples in the application authorization dialogues has recently been claimed to be effective in communicating the security risks associated with authorizing an Android application's requested permissions. For example, displaying a stored photo along with the read SD card permission to communicate the user's personal data which the developer can access (Javed and Shehab 2016). Harbach et al. (2014) state that users take longer to install applications when presented with personal information

examples along with the permissions. Similarly, Egelman (2013) explored the display of user information verbatim on the Facebook connect dialogue.

At the time of writing, the structure of attributes in the CREDENTIAL was an open issue. There was a discussion that attributes should be file-based and derived from the files stored in the Wallet. Here, we have assumed we have both attribute-based and file-based authorizations as shown in Figure 4-22. However, the final prototype for authorization screen depends on the results of ongoing discussion about the structure of attributes and some to-be-done research and user studies about users' perceptions, understandings and difficulties dealing with file-based authorization in the authorization dialogue which is completely different from what people experience in today's single-sign-on systems (e.g., single sign on using social networks).

Figure 4-22: Authorization screen

If Elsa wants to continue and accept the request she should select at least all of the mandatory information. She can do it one by one or click on the "All/none" option to select all of them at once. When Elsa selects all the mandatory information, the "Continue" button in Figure 4-22 will be active. If she presses the "Continue" button to go further, the screens depicted in Figure 4-23 according to her account settings will be shown (either the pin code or the fingerprint request to accept the request).

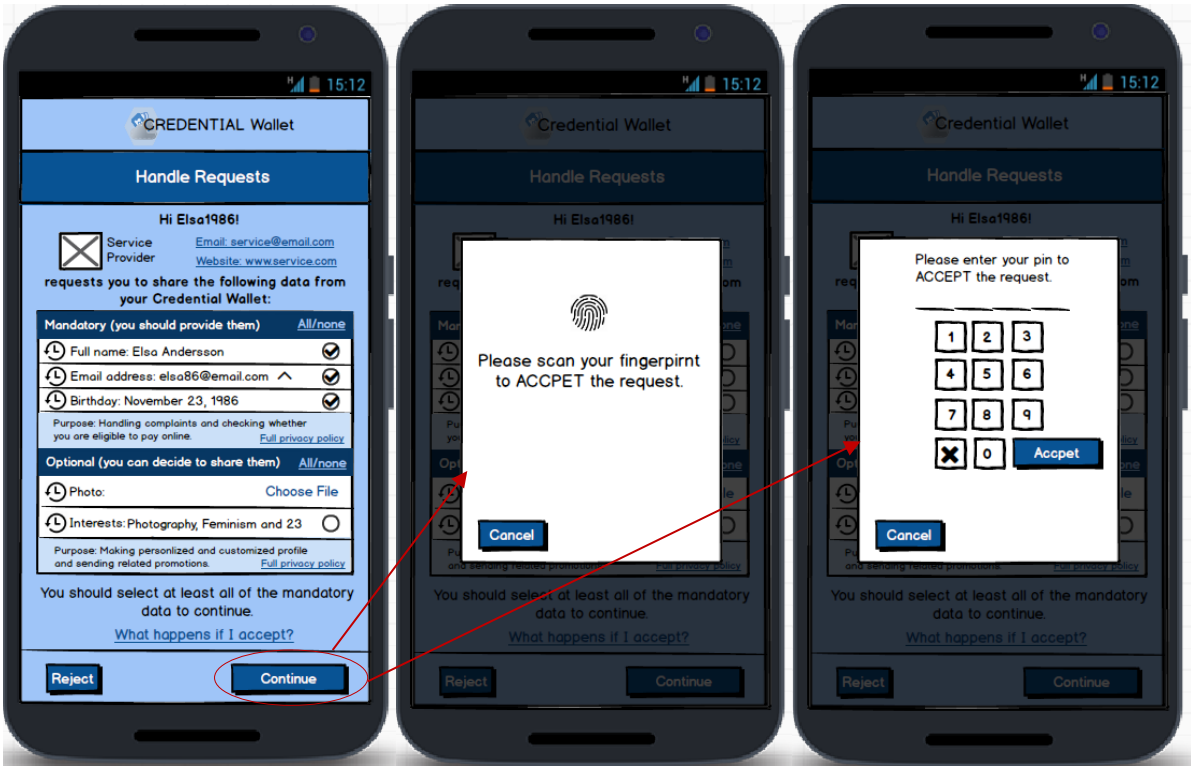


Figure 4-23: Accept the request

For each of mandatory or optional information, the purpose of data collecting is also depicted in a short sentence. If Elsa needs more information she can clicks on the "Full privacy policy" link. For some of the requested information, if there are more than one option available in her CREDENTIAL Wallet, like the email address or her photo, an angle icon is available in front of them to help Elsa to select the desired option.

Hence, we use a multi-layered design of privacy policy information as recommended by the Art. 29 Data Protection Working Party (2004), which displays only the identity of the controller and data processing purposes along with the data that can be selected to be disclosed by the user, while detailed policy information can be viewed by clicking on the "Full privacy policy" link. As discussed in D2.6, presenting policies in multiple layers instead of a long text is a mean for enhancing the end user's consciousness and comprehension of the essential policy information. Consent is obtained by requiring that the user actively selects data items to be shared, i.e. no data is pre-selected by default.

Furthermore, besides each piece of requested information, there is a history icon that shows the access logs for requested data in a timeline view if it is clicked as shown in Figure 4-24. The timeline view for the access logs shown in Figure 4-24 presents what entities on what date and time have accessed the Elsa's email address, for example. The access logs are shown chronologically and Elsa can use search and filtering options to limit the logs she wants to see. Moreover, if Elsa clicks on the logo or the picture of the requester she can see the related access logs of the requester. As shown in Figure 4-24, the logs are also

shown chronologically and they show exactly when the requester has accessed personal data from her Wallet.

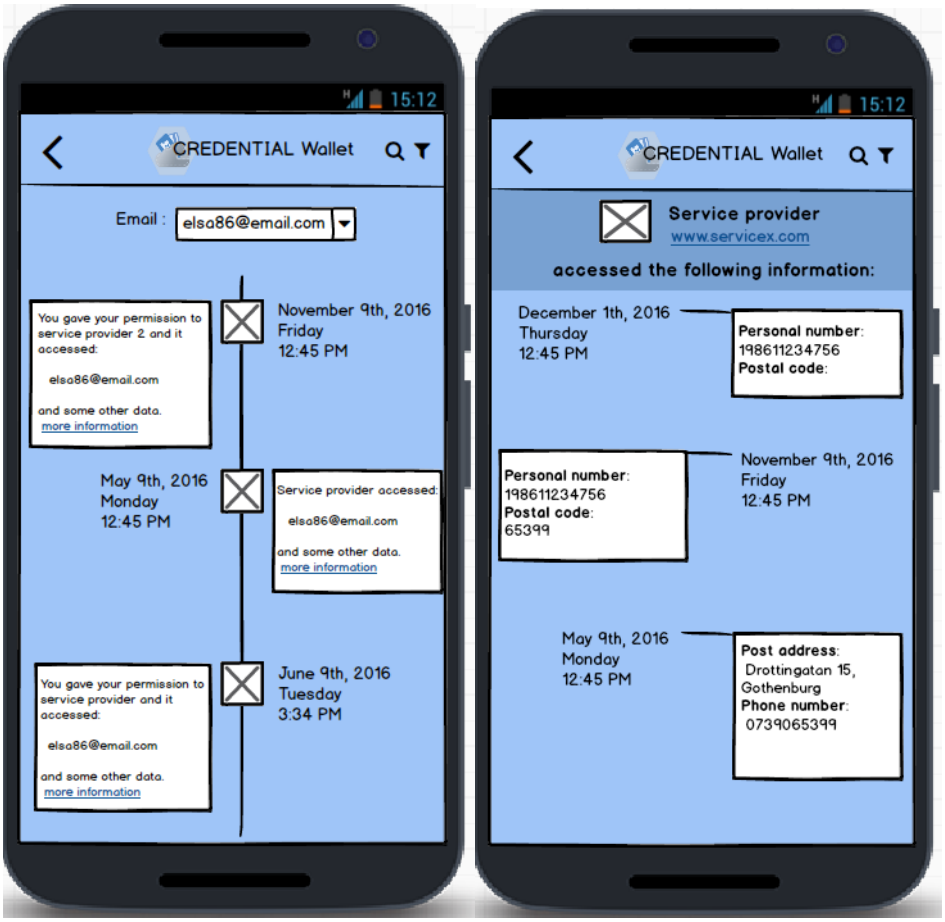


Figure 4-24: Access logs for requested information (left) and access logs for the requester (right)

Depicted in Figure 4-22, there is also a link that gives Elsa more information about what happens if she accepts the request and the exact information she receives is shown in Figure 4-25. Based on HCI requirements derived from legal principles in D2.6, Elsa should be informed about the expiration date of the authorization, how she can revoke her consent, how the service provider can access her data if she gives her consent and other detailed information. So considering the characteristics of the protocol being used for authorization, proper information should be conveyed to the user.

When Elsa scans her fingerprint successfully or enters the correct pin code to accept the request or when she rejects the request, the proper message is shown to her as presented in Figure 4-26. We have two buttons in the prototype depicted in Figure 4-26. If Ela wants to go to the main page of her CREDENTIAL Wallet app she can clicks on “Explore My Wallet” which shows the main page as it is depicted in Figure 4-7. Also, if she wants to handle the other requests avaibale in the waiting list she can

clicks on “Handle Requests” which shows her all the requests waiting to be handled as depicted in Figure 4-20.

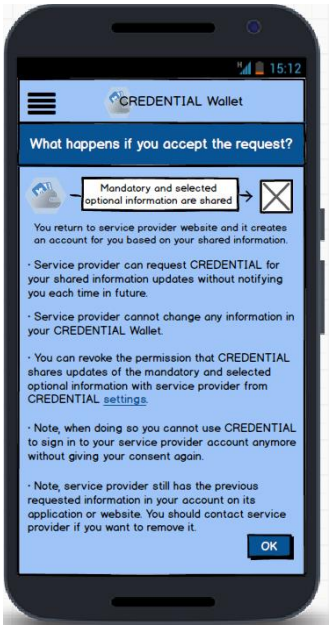


Figure 4-25: What happens if the user accepts the request

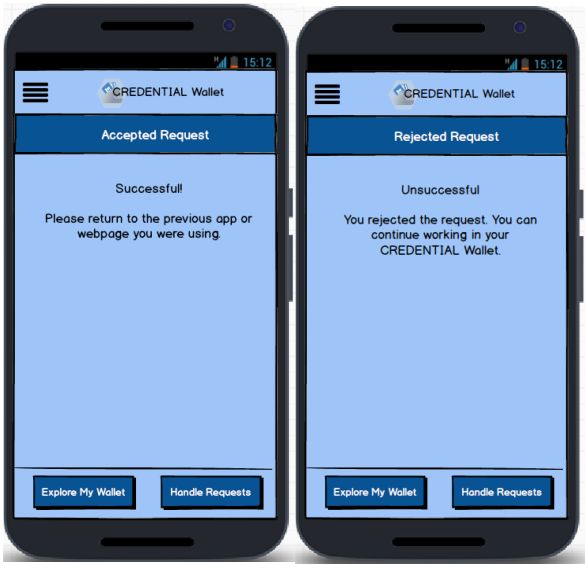


Figure 4-26: Messages shown after accepting (left) or rejecting (right) the request

4.1.4 Authentication

Elsa wants to sign into a SP using her CREDENTIAL account. Elsa may have been previously signed up to the SP and shared some of her personal data with the SP (see Figure 4-27), or it may be the first time that Elsa wants to use her CREDENTIAL account to sign up to the SP, and the SP does only need to know that she has a CREDENTIAL account, not any of her personal data from her Wallet at this stage (see Figure 4-27). Generally speaking, when there is a request to assure that Elsa is the owner of a

CREDENTIAL account that she claims, the authentication functionality is needed. To begin with, just like the authorization process, when a request is made, either the CREDENTIAL app opens automatically on her phone or she opens it herself, she should sign into her account first (if she is not already signed in). So as shown in Figure 4-21, she sees a message telling her that she has a new request and she can scan her fingerprint to see sign into her account to see the request. In Bauer's et al. study (Bauer 2013) participants expressed a strong desire to be kept better informed about the information that was being sent to the SP on the subsequent logins, during which IdPs typically send the information to SP without giving any notice or control to users. So in the authentication screen of the CREDENTIAL app, for every subsequent login we inform users about the previously shared data and the ability to revoke the permission.

If previously some data was shared from her Wallet with the SP Elsa can see what information was shared and can review and revoke this information by clicking on the link "CREDENTIAL app settings" as depicted in Figure 4-27. If she clicks on this link she will see the "Granted Access Rights" screen as shown in Figure 4-17 with a focus on the SP from which she just received the request. Otherwise, as also depicted in Figure 4-27, if previously no information was shared Elsa can just decide to authenticate to the SP using her CREDENTIAL account by scanning her fingerprint (or entering her pin code) or reject the request. The screens to convey the proper messages for the result of handling the request, whether being rejected or accepted, are similar to what we have for authorization as shown in Figure 4-26.

Importantly, the menu bar is omitted from authentication and authorization screens because the users should not navigate through the app when the focus is on handling a request and should not be distracted because otherwise they might miss the request and it will time-out (i.e., the request will be rejected due to no answer from the user.)

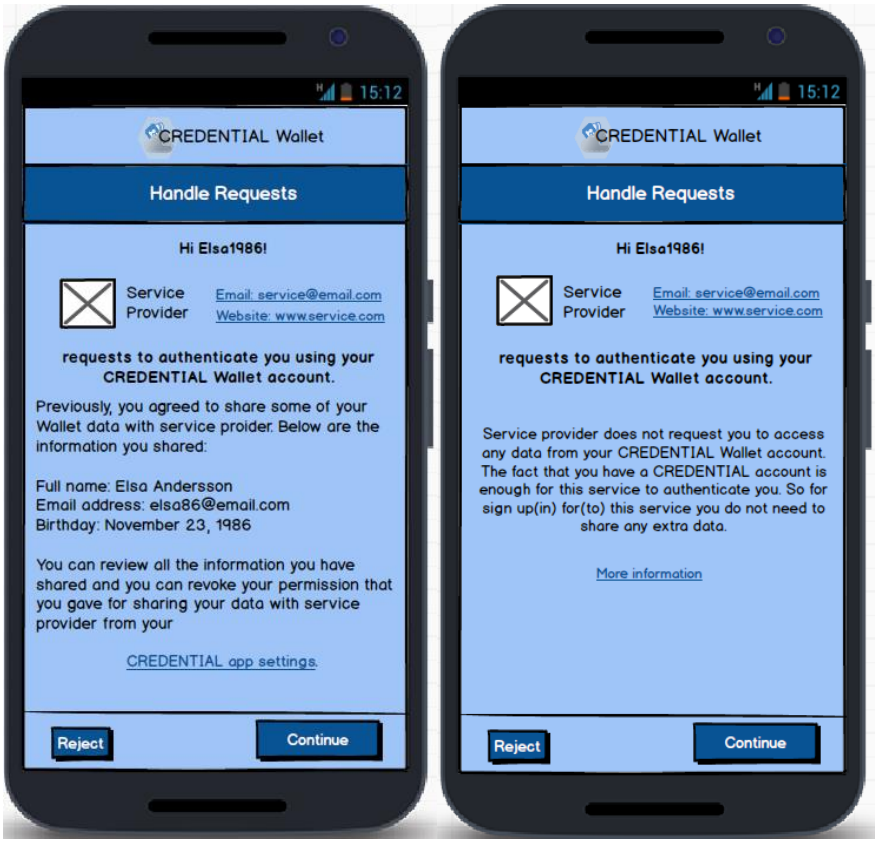


Figure 4-27: Authentication with or without previously shared data

4.2 Evaluation with Users

We conducted a user study with 20 participants recruited at Karlstad University with the objective to evaluate the usability of authorization and authentication screens while participants try to sign up/sign in for/to a service provider using the CREDENTIAL Wallet app. The results highlight certain problematic features and will be used to improve the interfaces. Also, the user study itself will be developed in order to be conducted in more varied contexts. Furthermore, we also used this first user study to evaluate the users' consciousness and comprehension of personal data disclosure and flows, and in particular to deepen the investigation into users' mental models in regard to the concept of "sharing" and in regard to how their fingerprint is used when giving consents.

Our study is both qualitative and quantitative using questionnaires and interview, which allows to ask some questions based on participants' answers on the questionnaires for more clarification, and a thematic analysis approach (Braun and Clarke, 2006) to surface key themes that arise in our interviews.

Before the user study, we conducted a pilot study with 3 participants. The reason to conduct the pilot user study was twofold: 1) to test, fine-tune the task and adopt the timing, and 2) to tailor and manipulate the questions we ask during the study for better achieving the study goals.

It is noteworthy to mention that the prototypes used in the user study were part of the third iteration prototypes so there are some minor differences between the prototypes presented in section 4.1 and the prototypes studied in this section.

4.2.1 Recruitment of Participants

The participants were recruited using stratified sampling in regard to sex and age. Stratified sampling means that all participants are recruited to create a sample that is equally distributed in regard to some, presumably, important criteria, in this case age and sex. Thus, we set out to have 10 men and 10 women, as well as to find participants with a wider age range than the ordinary student, why we included both students and personnel in the sample. We were careful not to include students with a computer science major, as this sample would represent a more external view of user requirements and comprehensibility.

4.2.2 Study Procedure

The user study was conducted using the interfaces of authentication and authorization screens (slightly earlier versions than those found in section 4.1) made interactive in Axure prototyping tool[1] on an Android mobile phone and a prototype of a fictitious website for which the participants pretend they want sign up. To begin with, a study plan was written to serve as the main communication vehicle as well as a blueprint for the study. A study plan is a summary of all the containing documents needed for the user studies (Rubin and Chisnell, 2008). To avoid an active researcher (study moderator/interviewer) bias which includes mannerisms and statements made by the researcher that provide the participants with information about the researcher's preferences (Onwuegbuzie and Leech, 2007), the procedure was standardized.

During the study, each participant received the same instructions and followed the same blueprint. The study took 20-40 minutes based on how much each participant wanted to communicate, and consisted of five parts: 1) a welcome session in which we thanked them, briefly talked about what they were expected to do, and obtained informed consent from all of participants. The informed consent imparted that participants agreed to have their screen and audio recorded, alongside with their answers. Consent to the recording was not required, though all participants agreed to be recorded; 2) a role-playing task with a fake CREDENTIAL account to sign up for a website using the CREDENTIAL app (Task 1); 3) a post-task questionnaire (cf. Appendix G), and comments for Task 1; 4) a role-playing task with the fake CREDENTIAL account to sign in to the same website from Task 1 using the CREDENTIAL app (Task 2), 5) a post-task questionnaire (again, cf. Appendix G0), and comments for Task 2; and 6) a general questionnaire asking for demographic information and some follow-up questions about fingerprint and sharing concepts in the app (found last in Appendix G). Two researchers, one as an interviewer (moderator) and one as a note keeper, were present during the testing.

Participants' own personal information was not used in the study. Instead, they were given the role of a persona, with made up personal information on the CREDENTIAL app that they used for Task 1 and Task 2 (i.e, for signing up and signing in, respectively). By using a persona, the participants could feel secure that they were not compromising their own personal details for taking part in the study. Moreover, it

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

allowed full control of what each participant encounters, avouching a standard experience that can be compared between participants (Karegar, Pulls, and Fischer-Huebner, 2016). The persona details included a username for the CREDENTIAL app and the personal information related to that username shown in authorization screen to be shared with the website from the CREDENTIAL Wallet, such as, the full name, email address, and date of birth.

Participants were shown a prototype of a fictitious website (the service provider) and they had three options to sign up/register to the page: 1) using the Facebook login button, 2) manually fill a form on the website, and 3) using the CREDENTIAL app to sign up. They were asked to use the Credential button to sign up. Our focus was not on how they would have preferred to sign up if they could select between different methods, we merely wanted to illustrate the function and utility of the service provided by CREDENTIAL and therefore put it in a context that would be familiar to web users (cf. section 6.5).

Then, while still on the website of the SP, they were asked to enter their CREDENTIAL username and run the CREDENTIAL app on their phone. We made an icon for the CREDENTIAL app on the home screen of the test device as depicted in Figure 4-28.

To measure the usability, we measured the effectiveness, efficiency and satisfaction. For the measurement of efficiency, we timed each participant's actions, from the moment they started to enter their usernames on the service provider side to the moment when they saw the return message on the app and they again checked the website to see that they were indeed signed up. For effectiveness, we counted the number of participants who finished the task without any problem or questions/interruptions. Finally, for satisfaction we used the System Usability Scale, SUS (Brooke, 1996). The SUS has been used in hundreds of usability studies (Bangor et al. 2009), which made it possible to get an estimate of user satisfaction for the key screens of the UI Prototypes V1 – a key concern at this stage of UI development as this graphic design will be used in the implementation starting when this report is delivered. (For a short discussion on other scales, see 6.2.)

In addition to measure the effectiveness, efficiency and satisfaction, we requested participants to answer some questions in regard to advantages and disadvantages of the CREDENTIAL app for each task, potential difficulties and their comprehensions of "sharing" and fingerprint.

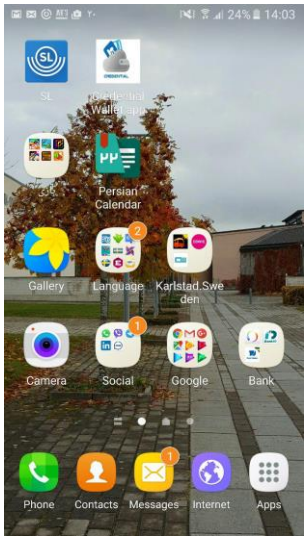


Figure 4-28: Home screen icon for the CREDENTIAL prototype

4.2.3 Description of Tasks

During the test, participants have two tasks: Task 1) we asked the participants to sign up for the website using CREDENTIAL Wallet app; Task 2) we asked the participants to imagine that some hours had passed and that they had been signed out of both the CREDENTIAL app and the website, and that they now wanted to sign in to the website again. For Task 2, they needed to use the app again, to sign in to the website.

The prototype of the website used in the study is depicted in Figure 4-29. It is a fictitious web service called "PhotoHex". When participants clicked on the "sign up using the Credential", they were asked to enter their CREDENTIAL usernames and then they saw a message telling them to run the Credential app on their devices to continue. For both Task 1 and 2, the first step is the same, except the exact interface of the website. For Task 2, participants used the sign-in prototype and "sign in using the Credential" button.

The screen to sign in to the CREDENTIAL Wallet app to see the request, the authentication screen, the screen to inform users about the result of their actions (accepting the requests, for example), and the authorization screen depicted in Figure 4-30 and Figure 4-31, respectively, are used for the tasks (which are slightly different from the related prototypes depicted in section 4.1).

The name of the fictitious website, PhotoHex, appeared on the authorization and authentication screens. We did not use the "history" icon besides each requested information for authorization screen because we did not want to test the functionality of that. Also, the participants were supposed to *sign in* to their accounts scanning their fingerprints. Because for the test, we could not use the real fingerprint sensor, we asked participants to click on the fingerprint sign to pretend they were scanning their fingerprints. So instead of just saying to scan the fingerprint it said "click to scan". We did not use a popup for fingerprint scanning but tried to make a solution that was as slimmed as possible. We also removed the "handle requests" button (as found in Figure 4-26) from the screen conveying the success or failure of the request

as shown in Figure 4-30. This simplification was made as we had no waiting lists of requests outside Task 1 and Task 2.

In this test only attribute-based authorization figured, because at the time when the user study was conducted, file-based authorization was an open issue and needed more discussion from a technical point of view. Indeed, file-based authorization from users' points of view and the users' understanding, perceptions and their difficulties handling the file-based authorizations could be subjects of future studies.

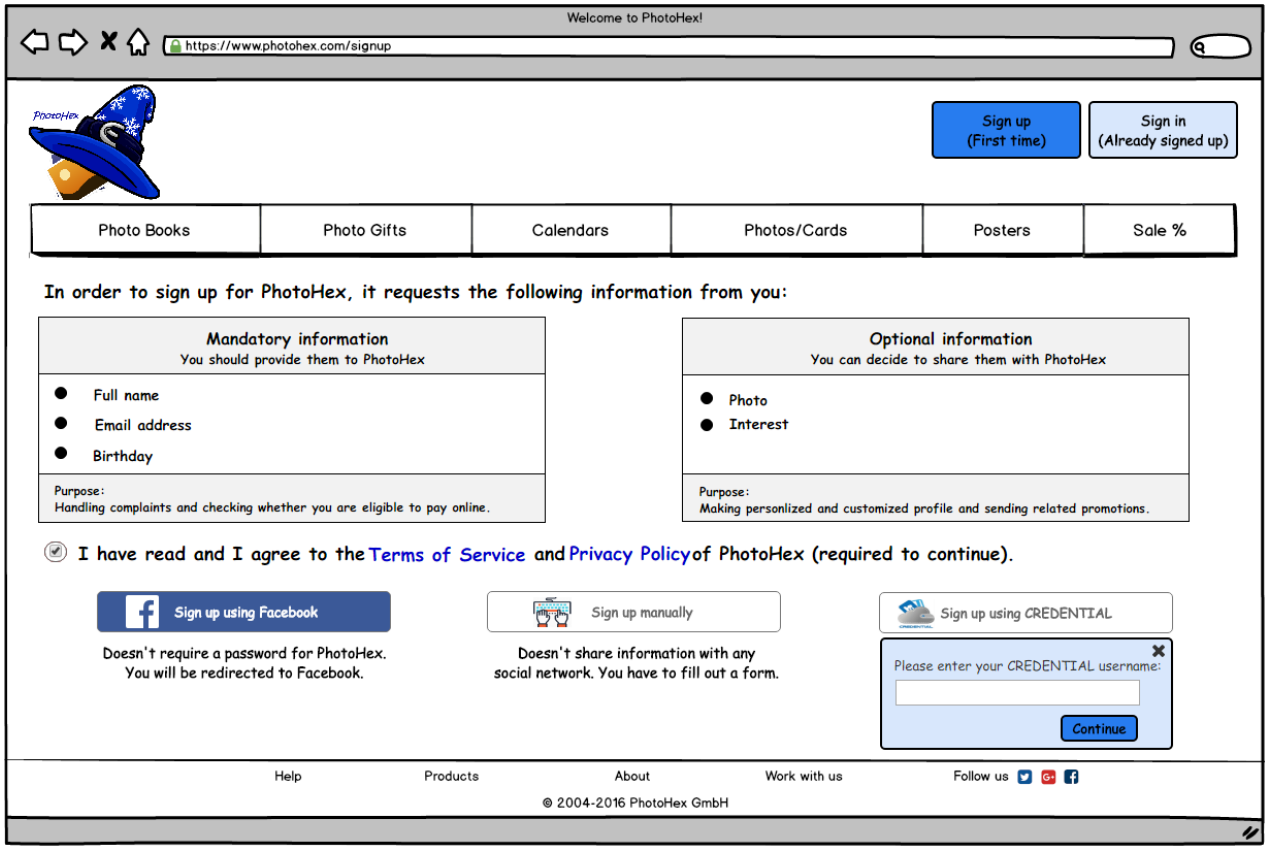


Figure 4-29: Prototype for the website used in the user study

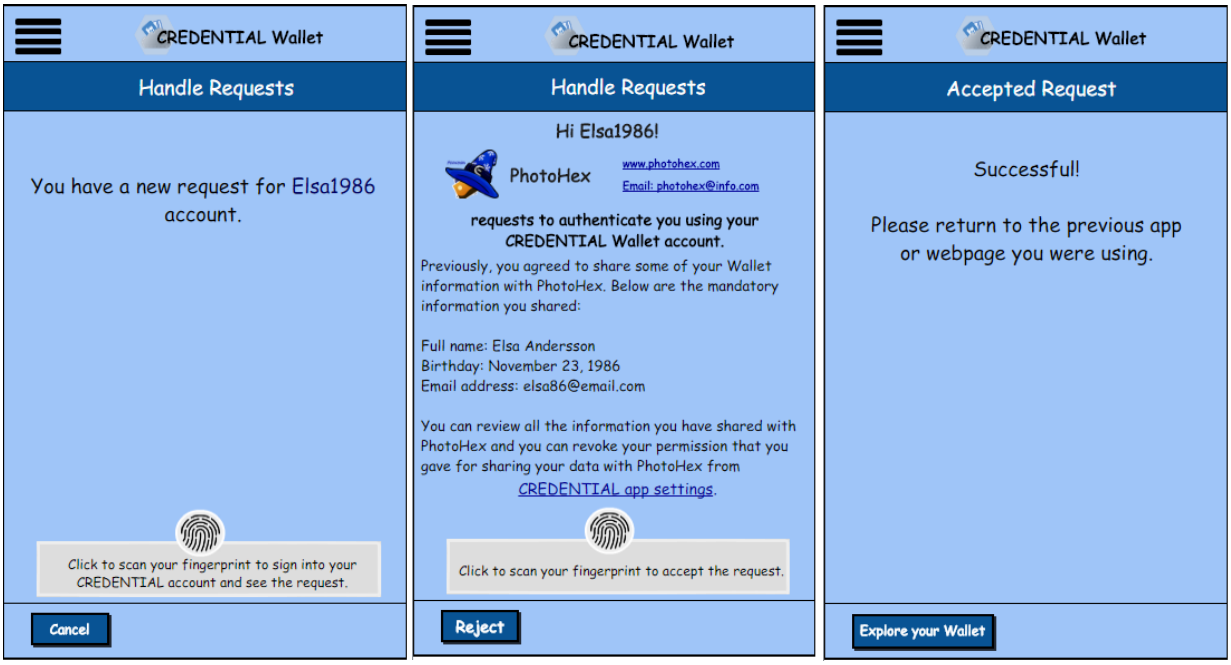


Figure 4-30: Sign in to see the request (left), authentication screen as used in the study (middle), and the success message

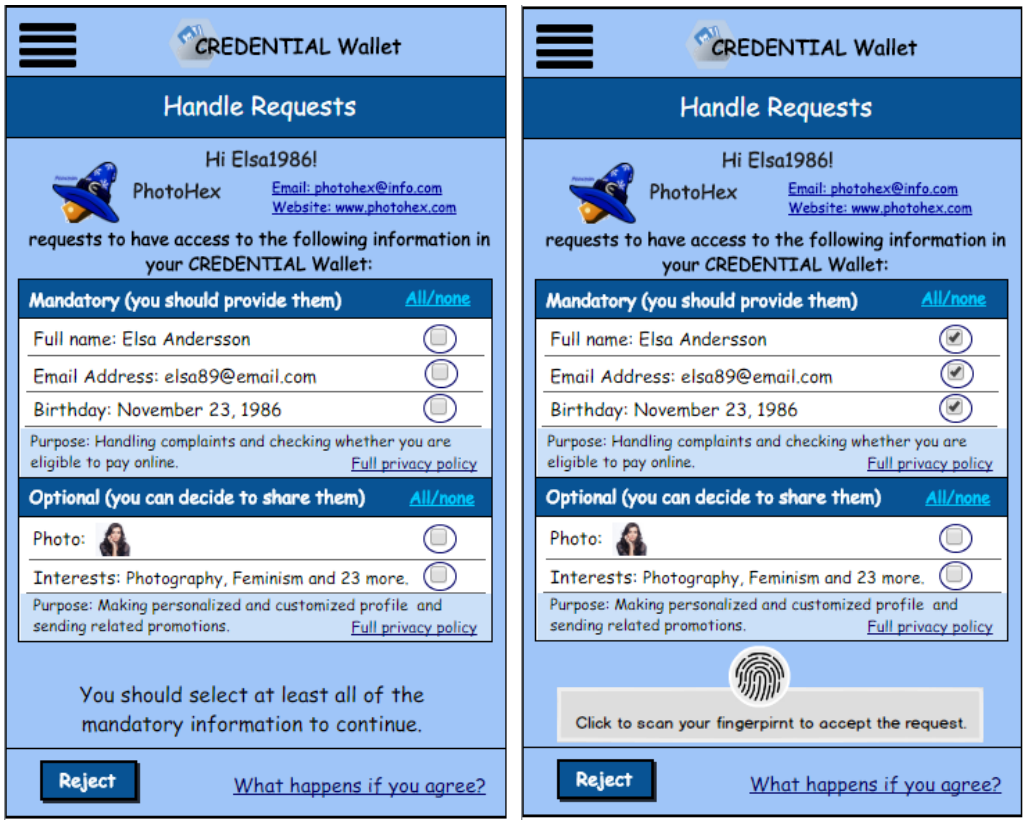


Figure 4-31: Authorization screen as used in the study

4.2.4 Results of the User Study

Twenty non-IT experts were recruited for the first user test outside the project group. The evaluation concerned only the Authorization and Authentication part of the general UIs. In line with other studies we found people not paying sufficiently attention to details of data releases and settings for disclosure policies. However, the participants showed a desire to have control over their data and wanted to select the mandatory information manually. This can be a way of slowing users down, and make them reflect more. Of course, people should not feel obstructed, but the design should make people more actively see or chose the data to be disclosed and the conditions for the disclosure.

Most participants seemed to understand that they used the CREDENTIAL Wallet mockup to authenticate, but this probably depends on their previous experience with a similar solution. This might bias the conclusion about technology acceptance if not other subjects, for instance from other countries, are included in the further user testing.

In addition, some participants were worried about the security and thereby also the privacy because they could not really figure out how it worked. Moreover, the single point of failure, as it is called in the literature, that is if the one and only IdP goes down, the user is at loss.

Using the fingerprint for giving consent (at the same screen requesting for the personal information in authorization dialogue, for example) was from a simple usability question not a problem, but we observed that most of the participant had not a correct view of where it is stored and who have access to it. Our UI contains now a suggestion for a simple alternative, a pin code. Of course, this can be elaborate further. For instance, the results indicate that the very way the fingerprint scanning was presented might have contributed to the confusion. Thus, our UI V1 includes a separate pop-up for fingerprint scanning.

On the multi-layered approach to present the necessary data for informed consent, the results are like other studies showing that people in general would not bother for clicking such links. The only participant actually opening the full information actually did not show any remembrance of this when answering the questionnaire afterward.

In sum, further evaluation is needed concerning how people would understand what data is needed, how to select these, and what data are actually sent. Also, user evaluation should be wanted of file-based authorization requests and potential solutions to guide people to select the proper files from their Wallet like the file tag system discussed presently within the project.

The following paragraphs give details on the recruitment of test participants and their familiarity with IdPs and then discussions on test results from the questionnaires are presented as concern the participants':

- opinions and understanding of the authorization task in the CREDENTIAL app,
- opinions and understanding of the authentication task in the CREDENTIAL app,
- general opinions and concerns for using the CREDENTIAL app,
- perceptions of the fingerprint,
- perceptions of sharing their personal data,

and, finally, some simple usability metric results are presented.

4.2.4.1 Demographic Information and Familiarity with Identity Providing Functions

Twenty participants were recruited for the user study, equally distributed between men and women. The average age of the participants was 32.2 years old, with eleven participants between the ages of 20 to 29, three participants between 30 to 39, five participants between 40 to 49 and one participant above 50 years old. All participants but one were pursuing their higher education or they had their higher education degrees already, and none of them were from Computer Science and Informatics System Departments.

To be aware of the participants' familiarity with the concept of identity providers, using a third party website/app to sign up for a service, we asked them whether they had used social login buttons or Swedish Mobile BankID[1]. All of the participants stated that they had seen social login buttons previously, and half of the participants expressed that they use the social login buttons on some multimedia websites like Spotify, SoundCloud and online TV providers. Only three participants stated that they do not use the Mobile BankID.

4.2.4.2 Participants' Opinions and Understanding of the Authorization Task in the CREDENTIAL App

As mentioned previously in section 4.2.2, after each task, participants completed a task-specific questionnaire in which they gave their opinions about SUS statements, and answered to the questions regarding their understanding of each task, pros and cons of the CREDENTIAL app and the potential difficulties or unclear words, instructions or any elements in the interfaces.

For Task 1, signing up for a website using the CREDENTIAL app, we asked participants whether they needed more information on the authorization screen that could help them make better decision. In other words, we asked them to state if they though they required more clarification about each of the requested information which could help them to decide better. Nine participants explicitly expressed that they did not need extra information and the available information was enough for them. Analyzing the answers from whom needed extra information, clarification about security of data, the reasons to share the data and benefits of sharing, who can see the data and how the data is used surfaced. Moreover, one participant mentioned that clearer feedback to select all mandatory information in the authorization screen is demanded.

To receive feedback for how the selection works in current version of UI, we asked participants whether they preferred to select the mandatory information manually or they wanted them to be selected by default. Because if they want to accept the request, they should select all the mandatory information anyway. Among the participants, 15 stated that they prefer to select the information manually.

To further being informed about participants' problems concerning Task 1, we asked them about difficulties they encountered during the task and whether something was unclear. Most participants (n = 13) stated that they did not have any difficulties and nothing was unclear for them. However, five participants expressed their ideas and experiences regarding the checkboxes. One believed that it was not clear where they should click at the first time. Another one expected an "Agree" button and it took a while

[1] https://www.bankid.com/en/om-bankid/detta-ar-bankid

for him to find where to check boxes and continue. Furthermore, one participant mentioned that he needs a clear feedback if someone misses to check one of the mandatory information.

To receive feedback about pros and cons regarding using the CREDENTIAL app in Task 1, we asked participants to state their general experiences of the app. Eleven out of 20 expressed that it was easy, clear and quick. They supported their statements by stating that it did not need a special skill, it was less time-consuming than using username and passwords and there was no much information to read. On the other hand, two participants mentioned it was pretty advanced and it is always hard for the first time to work with an app. For disadvantages, two participants expressed their concerns regarding trust and security. Two described their feelings regarding sharing their data and the fact that they were not comfortable to share the mandatory information and they wanted to know the reason for sharing their data. Moreover, three participants mentioned they wanted the app to be more visually appealing. For example, they wanted the checkboxes for mandatory information to be more distinguishable with a different colour and desired bigger texts on the screen. Interestingly, one participant stated that using the CREDENTIAL app was too easy, that it made him not read anything and not pay attention to anything but just continue.

In sum, participants found the authorization task easy, quick and clear. However, as we discuss in the following sections, participants did not understand all the concepts behind sharing their information from CREDENTIAL Wallet with a SP, and the task may have been too easy making them not pay attention enough, as mentioned by one participant. They showed a desire to have control over their data and wanted to select the mandatory information manually like the way it is in the current interfaces. Although most participants did not require any more clarifications for information requested in authorization task, some were interested in knowing more about the security of data, reasons to share and benefits of sharing besides the facts about the receiver of the data and how it is used. Moreover, for some participants at the very first time it was hard to understand how they should proceed. The fact that all mandatory information should be checked so they can proceed should be conveyed in a better way.

4.2.4.3 Participants' Opinions and Understanding of the Authentication Task in the CREDENTIAL App

For Task 2 (signing in to a website using the CREDENTIAL app) we asked participants about the reason of not being requested to give their consent again to share their information in the authentication screen. In other words, we wanted to know if they understood that they gave their consent once in sign-up process, and they could sign in to the service without being asked again for their consent. The majority of participants (n = 16) expressed that they were not asked again to select and share their information because they gave their consent before and the information were shared already. Two participants did not have any opinions, and two others answered incorrectly.

In the authentication process, if you have disclosed your information previously, whether you accept the request for authenticating you to the SP or reject it, the SP will still have access to the information you shared with it before. To find out if people have the correct understanding of how data flows between the SP and the CREDENTIAL app, and to see what they think of "sharing" their information, we asked them to answer whether the SP would have access to their shared information if they rejected the request in the authentication process. Surprisingly, eight participants said that the SP could not access their information if they rejected the request in the authentication task. Even some of the participants who correctly stated

that they were not asked about their consent again because they gave their permission before answered this question incorrectly.

To further being informed about participants' problems doing Task 2, we asked them about difficulties they encountered during the task. Almost all participants (n = 17) stated that they did not have any difficulties and nothing was unclear for them. Only one participant mentioned it is always a bit unclear when it is the first time you are using an app and another one expressed that she needed more instructions to use the app and to do the task.

To receive pros and cons feedback using the CREDENTIAL app in Task 2, we asked participants to state their ideas about general experiences of the app. Eight out of 20 expressed that it is easy and fast and two mentioned that it is easy to learn. One participant stated that it was really good to see what was shared previously. On the other hand, four participants expressed that it could be better typographically. Also, the need of clear information about data protection, clear instruction about how to use the app, no need of immediate requirement for using the app and finally being too easy that makes you forget and do the tasks fast were among the other comments.

In sum, most of the participants understood that during the authorization process they were not asked for their consent to share the information because they did it before. However, some participants had difficulties to understand that whether they accept the authentication request or reject it, the SP would have access to their personal due to previous sharing. Comparing the comments on authorization task with the authentication task (i.e., Task 1 and Task 2, respectively), it is obvious that authentication task was easier and clearer for participants because most of them explicitly stated that they had neither any difficulties nor anything that was unclear for them. Furthermore, the easiness to execute the tasks made them forget about what happened in the task; more required information about data protection and more visually appealing interfaces were among participants' comments on authentication and authorization screens.

4.2.4.4 Participants' General Opinions and Concerns for Using the CREDENTIAL App

To begin with, we briefly talk about the Swedish BankID[1] which is used widely by people in Sweden. The BankID is the leading electronic identification in Sweden. The BankID has been developed by a number of large banks to use by members of the public, authorities and companies, and have 7.5 million active users. Many services are provided where citizens can use their BankID for digital identification as well as signing transactions and documents, a signature made with a BankID is legally binding, and the bank issuing the BankID guarantees the customer's identification. The services vary from online and mobile banking, and e-trade to tax declaration, and are provided by government, municipality, banks and companies. The BankID is available on smart card, soft certificate as well as mobile phones, iPads and other tablet devices. Due to its easiness, lots of people use the mobile version of BankID. Because for smart card version, they need the card reader and a laptop (or a desktop computer) which are not available every time you need them. Using the Mobile BankID to authenticate to different services is similar to the

[1] https://www.bankid.com/en/om-bankid/detta-ar-bankid

concept of using the CREDENTIAL app to authenticate. For Mobile BankID people have a six digit pin code and when they want to authenticate to a website using the Mobile BankID they provide their unique national personal number on the website and then they run the Mobile BankID app on their devices. They see the name of the website to which they want to authenticate and they enter their pin code and return to the website. For Mobile BankID there is no selective disclosure functionality, and there is no information about what kind of data flows between different entities, the BankID is only meant as a digital identification.

After completing each task, participants were asked if they had any comments about the task and the application. In the general questionnaire after the Task 2, one question regarded participants' concerns regarding using the app. Here, we present their general comments and concerns about the CREDENTIAL app.

Half of the participants explicitly mentioned that the Mobile BankID and the CREDENTIAL app are similar, although the CREDENTIAL app is more complex. Despite the similarity, they expressed that they like it more when they can select their information and decide to share them or not in the CREDENTIAL app. They also mentioned that the CREDENTIAL app could be a good replacement if it worked in different languages (as it is supposed to work in different languages for different people). During the study, we observed that participants mentioned this similarity from the beginning when they were introduced briefly to the CREDENTIAL app.

Four participants mentioned that the word "revoke" is a hard word and they cannot understand it. We used the word "revoke" in the authentication screen (see Figure 4-30) to clarify they can revoke their permissions they have given previously. But people had difficulties understanding the meaning of the word.

Five general comments had trust and security concerns. Two participants wondered how they could be sure that the tool was secure. They wanted more information to trust the app. Among the comments, two mentioned they prefer to use usernames and passwords to the CREDENTIAL app. To support their opinions, they mentioned that it is a single source of lots of personal data and they are afraid to use it. Moreover, they expressed that when there are more steps to login, they feel safer and more secure and they think that using the Credential app is not easier than using the usernames and passwords for websites.

Other general concerns about using the app that were mentioned were: security, loss of control over the data, no real need of usage and forgetting how to use it. Security was the most common concern, participants were concerned about their security if the CREDENTIAL app is hacked and the level of access the hacker can get over their information. Some of the participants also mentioned their concerns regarding fingerprint theft. After security, concerns about the control over the data were the most common one. Participants stated that they were hesitant to share their data via another app to register for websites because they feel they will have no control over their data.

In sum, using the CREDNETIAL app, participants are concerned about the security of the app and loss of control above their data. According to Ruoti's et al. study (2015), transparent authentication systems like single sign on systems are usable from users' points of view but simultaneously lead to confusion and lack of trust from users. Our results, aligned with previous studies (San-Tsai et al., 2013; San-Tsai et al., 2011), indicate that users are concerned about security and privacy of their data when using a federated IdP: the

single point of failure feeds their concerns. Most of our participants were familiar with the concept of using an application to authenticate to a website (like the Swedish Mobile BankID), even if they considered the CREDENTIAL app to be more complex than the BankID. We need more participants from other countries who are not using a BankID or similar apps to repeat the study and see the difficulties those participants encounter during doing the tasks.

4.2.4.5 Participants' Perceptions of the Fingerprint

In order to sign-in to the CREDENTIAL app and accepting the request in the authorization and authentication screens, users should scan their fingerprints. Fingerprint pattern is sensitive personal information. Consequently, it is very important to learn what people think about the fingerprint and what their concerns regarding using their fingerprints are. Also, it is important to know about people's understanding of where their fingerprint is stored, who has access to it, and whether it is sent to the SP with other personal information when they give their consents to share the information by scanning the fingerprint or not.

Among participants' comments about their concerns for using fingerprints, security was the most mentioned subject. For example, two participants stated explicitly that it is risky to use their fingerprints. They were afraid that their fingerprint patterns could be sold to other parties. Two participant also mentioned about the availability of the technique. They mentioned about their previous problems using the fingerprint, like some technical issues on their devices or being rejected because of dirty hands.

Moreover, two of the participants expressed explicitly that they feel the fingerprint is safer than passwords and five expressed that it is faster and easier. However, one the other hand, four participants did not like to use their fingerprints and they said they prefer passwords. For example, one participant said that it was not pleasant to give the consent with the fingerprint because it might be saved and used in unwanted ways. Six participants expressed that they do not have any concerns regarding using the fingerprint.

Answers to the question about where the fingerprint pattern is stored are summarized in Table 6-1. Eleven participants stated that it is stored on the CREDENTIAL app. To justify their answers, most of them mentioned the use of the fingerprint on the app and that it was the app which asked them to use it. Also, one mentioned that the app is the place where all the personal information is saved. Four participants said that the fingerprint is stored on the mobile device. To justify their answers, they said that because it is a hardware taking care of that and they registered their fingerprints on their devices previously. Two participants mentioned both the mobile device and the CREDENTIAL app have access to the fingerprint pattern. Two other participants also mentioned that both the CREDENTIAL app and the website have access to the fingerprint because all of them are connected and because the CREDENTIAL app was accessed from the website. Interestingly, one participant expressed that fingerprint is accessible by the website, the CREDENTIAL app and the mobile device because all of them need the fingerprint to let her login to the website and to the app.

Table 4-1: Where the fingerprint is stored?

Number of Participants	Where is the fingerprint stored?

11	CREDENTIAL app
4	Mobile Device
2	Mobile Device and CREDNTIAL app
2	CREDENTIAL app and the Website
1	Mobile Device, CREDENTIAL app and the Website

In sum, although some participants mentioned that using the fingerprint is easier, quicker and safer than using the passwords, others were afraid of the security of their fingerprints and how the fingerprint could be used and stored in unwanted ways. Moreover, most of our participants did not have a correct understanding about where the fingerprint was stored, or who had access to it. Based on participants' answers, the fact that they were asked to scan their fingerprints on the CREDENTIAL app and the way they should sign into the app contributes to their misunderstanding about where the fingerprint is stored.

4.2.4.6 Participants' Perceptions of Sharing their Personal Data

When users give their consents to share their personal data with different SPs, it is imperative to help them to make an informed consent. Authorizing permissions without reading and consenting to them raise the risk of unintentional information disclosure to third parties, and cause a privacy issue. Thus, we investigated if participants paid attention to what personal information they shared with the website from their CREDENTIAL account during the authorization task. We asked about 14 different personal information including the mandatory and optional information and fingerprint pattern. Moreover, we investigated to what extent the participants noticed the informative links in the UI to receive more information about what happens if they share their data with the website from their CREDENTIAL app. Also, we were interested to see to what extent the participants' mental models and the way they think are compatible with what is happening nowadays when they use an IdP to share their data with other parties.

None of the participants could correctly state what information was shared from the CREDENTIAL app with the website. In the UI prototype of the app, the mandatory information were full name, birthday and email address. All participants accepted the request in the authorization task so all of them shared the information with the website (PhotoHex in the study). However, five participants said "no" or "not sure" when they were asked to state if they shared their full names. Three participants said "no" or "not sure" when they were asked to state if they shared their email addresses, and seven said "no" or "not sure" when they were asked to state if they shared their birthdays. Interestingly, people did not notice that when they shared their birthdays, they implicitly shared their ages: 7 participants did not have consistent answers for their birthdates and ages. While three participants stated that their birthdates were shared, they believed their ages were not shared or they were not sure about it. On the other hand, two who were not sure if the birthday was shared stated that the age was shared. Finally, two participants who were not sure if the birthdate was shared mentioned that the age was shared.

For optional information, six of participants selected to share all the optional information when doing the authorization tasks but not all of them remembered properly what they shared. Also, some of the people who did not share the optional information did not remember correctly if they shared a photo or their interests. Regarding the photo, just two participants answered incorrectly and for sharing the interests five participants were not successful to correctly answer the questions. We also asked participants whether they shared their fingerprint pattern with the website or not. Surprisingly, only two participants said "no"

and all the other either said "yes" or "not sure". In Table 4-2, numbers of participants who said YES, NO or NOT SURE for each piece of information in question are shown.

Table 4-2: Distribution of YES, NO and NOT SURE answers for each piece of information

Information	YES		NO		NOT SURE	Sum
	Correct	Incorrect	Correct	Incorrect		
Your post address	N/A	4	9	N/A	7	20
Your full name*	15	N/A	N/A	4	1	20
Your email address*	17	N/A	N/A	1	2	20
Your educational background	N/A	0	16	N/A	3	19†
Your fingerprint pattern	N/A	17	2	N/A	1	20
Your home town	N/A	1	11	N/A	8	20
The city in which you live	N/A	1	11	N/A	8	20
Your birthday*	14	N/A	N/A	3	3	20
A photo of yours**	6	2	12	0	0	20
Your phone number	N/A	2	12	N/A	5	19†
Your interests**	4	2	10	3	1	20
Your credit card number	N/A	1	16	N/A	3	20
Your age (* by implication)	14	N/A	N/A	3	3	20
Your mobile device model	N/A	1	10	N/A	9	20

* Mandatory information.

** These were presented in the UI as optional choices. Six participants chose to share both photos and interests and one participant shared only the interests. The remaining thirteen selected just the mandatory data.

† One participant forgot to answer.

N/A Not applicable.

Besides asking for recapturing what mandatory and optional information the participants shared, we included items that were not on the CREDENTIAL authorization screen, such as hometown, credit card number and educational background; to ensure that participants were truly answering the questions. Interestingly, some people incorrectly stated that this listed information was shared with the website. Among all the information being asked that was shared or not, people were most successful at remembering about sharing the photo and were most unsuccessful at understanding if they shared the fingerprint with the website.

To better report the awareness of participants of personal data being shared we measured the relevance of responses using precision and recall. Ronen et al. (2013) used these measurements to report people's awareness of data exposures when using the federated IdP to sign in to websites. Ronen and co-workers defined the precision (P) as the ratio between the number of data types a participant named correctly and the number of data types the participant named (correctly and incorrectly) and defined the Recall (R) as the ratio between the number of data types a participant named correctly and the number of data types that were actually transferred to the website. In Table 4-3, the related average, standard deviation, minimum and maximum for recall and precision are reported. Two participants did not answer to all the questions

for data being shared so they are excluded from this measurement. Regarding the averages in Table 4-3, P = 0.72 and R = 0.76, approximately one-fourths of the participants' answers were incorrect (incorrectly mentioned that the information was shared with the service provider) and participants identified three-fourths of the data types that were shared with the service provider. Although the average numbers are not very low, it shows a rather limited awareness of the data types being transferred and needs improvements especially for specific data types like fingerprint pattern. Aligned with our study, Bauer's et al. (2013) study shows that participants' precise understanding of what is sent is not significantly affected by the consent dialogues (instead, as that study indicates, it is affected by their privacy concern level and that they have some preconceptions about what is going to be sent). Egelman's study (2013) also showed that participants did not read the authorization dialogues and they did not pay attention to the details of the dialogues during the test.

Table 4-3: Precision and recall values

	Precision	Recall
Average	0.72	0.76
Standard deviation	0.16	0.20
Min	0.43	0.50
Max	1	1

To see to what extent people's mental models are compatible with what is happening when they use an IdP to share their data with other parties, and to see if they click on the links available in the UI to receive more information, we asked the participants some questions regarding sharing concept. Based on the implementation of authorization protocol, the authorization validity could be one-time, limited or unlimited until revoked. Moreover, the SP (requester) can request to access the updates of shared data either when the user is signed in, or when the user is not interacting with the SP and is offline. Our results showed that people's understanding and expectations of what should happen differ from the actual data flow between the SP and the IdP.

Just one participant clicked on the link that informs users about what happens if they agree to the request (see Figure 4-31). Consequently, we should not expect people to click on the links when we use layered interfaces. That information should be more visible and mandatory to read if it is required. Still the participant who clicked the link could not answer the questions and he did not remember about the content he read. So if we provide important security and privacy information in the form of pretty long texts on the mobile device, users may not be able to comprehend it as we expect.

Participants in our study expect that even if they have shared their information previously with a website they should be informed again if the SP requests from the IdP to access to the update of shared information. However, in current implementation of authorization protocol like OAuth, when the information is shared and as long as the authorization date is valid the SP can implicitly request to have updates of shared data without users being informed or involved to get new consents. Also, seven participants though they could not revoke their permissions and five of them though the website gets access to write into the CREDENTIAL app.

Our results are aligned with the Bauer's et al. study (2013) in which they found out that some specific preferences of the participants appeared to be out of sync with the current implementation of single sign-on process. For example, most of our participants expected to receive a consent form and being involved in subsequent updates of data sharing. Moreover, in the Bauer's et al. study participants expressed a strong desire to be kept better informed about the information that was being sent to the SP on the subsequent logins, during which identity providers typically send the information to service providers without giving any notice or control to users. Although in authentication screen in CREDENTIAL app, for every subsequent login we inform users about the previously shared data and the ability to revoke the permission, few participants read the screen carefully and paid attention to the given information.

Most computer security warnings and authorization dialogues lack effectiveness in attention switch and maintenance; the very first stage of Communication Human Information Processing (C-HIP) model proposed by Wogalter and co-workers (Conzola and Wogalter 2001). The end-users are more focused on accomplishing the task at hand, than switching their attention towards the warning dialogue and assessing the associated risks. Since access control is not the primary goal of users, many users simply click through the notices, ignoring the one important piece of information that alerts them about giving away their personal information to the third parties (Javed and Shehab 2016). There are various works on users' awareness of data types they share on authorization dialogues and several suggestions to help them make informed consents (Bauer et al. 2013; Wang et al. 2013; Javed and Shehab, ibid.; Egelman 2013; Ronen et al. 2013).

In sum, the results from the user study in this deliverable which showed people to not spend enough time on authorization dialogue to see the details, and to not pay attention to different elements in this dialogue are in accordance with previous works on consent dialogues in the context of identity providers. Considering our results and the reported problems in the literature, including the habituation and preconception of authorization forms, we need to do more research to reveal what methods for communicating with the users are most effective in this context. Moreover, in the context of using identity providers to sign up/in for/to service SP, clear and proper information about how and when the SP can access the users' information after giving the consent and what is exchanged during the authentication and authorization process should be conveyed to the users without endangering the usability.

4.2.4.7 Usability Results

To measure the usability, we measured efficiency, effectiveness and satisfaction. We timed people when they were doing the tasks, as well as observed and kept note of any major difficulties or interruptions during the tasks. We also used the SUS to measure the satisfaction. As part of an empirical evaluation of SUS, Bangor et al. (2009) paired SUS scores against objective measurements of the various systems' success in order to derive adjective-based ratings for SUS scores. These ratings and their correlation to SUS scores and acceptability ranges are given in Figure 4-32. In the following, we will compare our results with these.

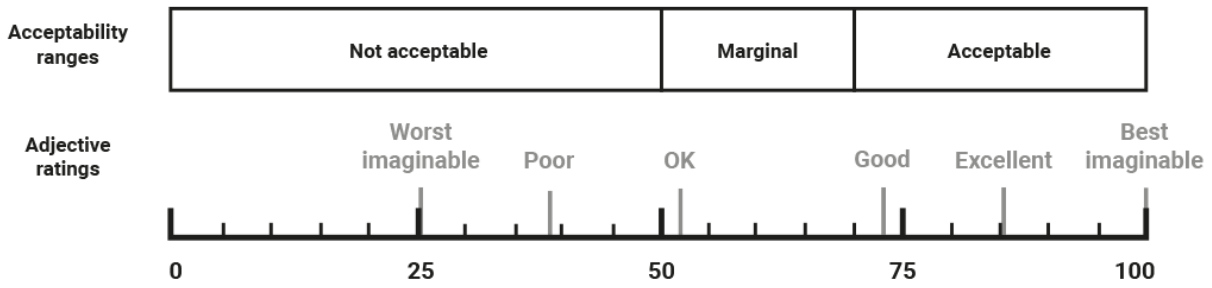


Figure 4-32: Adjective-based ratings to help interpret SUS scores (adapted from Bangor et al. 2009)

Table 4-4 shows the related average, standard deviation, minimum, and maximum, for the required time to finish each task. Table 4-5 presents average, standard deviation, minimum, and maximum, for the SUS score for each task. For Task 1, one participant missed to rate one of the SUS statements, and for the Task 2, two participants missed to rate one of their SUS statements. We replaced the missed values with the mean value of the series of that statement ranked by all participants; this way the imputed value would not affect the group difference. The average SUS value for the first task is 75.88 which is above the "good" level, under the "excellent" level, and classified as acceptable. The average SUS value for the second task is 81.98 which is also above the "good" level, near the "excellent" mark and classified as acceptable. As shown in Table 4-5, the SUS score of the authentication task in the CREDENTIAL app is bigger than the one for authorization which was predictable from comparing users' comments on both tasks.

Ruoti et al. (2015) have studied the usability of seven authentication systems including federated single sign-on systems like Google OAuth 2.0 and Facebook Connect. In their study, they defined three groups of authentication techniques and the method which won in each group was also compared and tested for SUS score with the winners of the two other groups. Finally, Google OAuth was the winner between different technologies with the SUS score of 75. Our average SUS scores for the CREDENTIAL app, both for authentication and authorization task, align with Ruoti's study.

Table 4-4: Time to conduct the tasks

	Task 1 (Authorization)	Task 2 (Authentication)
Average	1m 40s	57s
Standard deviation	39	14
Min	42s	40s
Max	2m 50s	1m 40s

Table 4-5: SUS scores for the tasks

	Task 1 (Authorization)	Task 2 (Authentication)
Average	75.88	81.98

Standard deviation	11.74	11.68
Min	47.50	57.50
Max	95.13	97.50

Two participants had difficulties with finding how they could continue in the authorization screen. So they asked the moderator how they should proceed. Except for the problem of not finding how to continue at their first time for these two participants in the first task (authorization task), participants were successful at finishing the tasks without any questions or interruptions.

Comparing the time it took for doing Task 1 and Task 2 shows that most participants needed more time for Task 1 than for Task 2 (Figure 4-33, left, and Table 4-4). During the study some participants mentioned that it is always hard for the first time when you are using an app. We believe that the work of selecting the information in authorization screen and being the first-time user when doing the first task contributed to the higher numbers for time. Considering the fact that it was the first time participants were working with the CREDENTIAL app, we assume in future when they are using the app in different scenarios they get more acquainted to it and the timing will improve together with the understanding.

Moreover, comparing the SUS values for the tasks, as depicted in Figure 4-33 (right), shows that most participants (*n*=15) scored the authentication task higher or equal in SUS value. The same reasons as mentioned for the time comparison of the tasks can also be discussed for SUS values. But the changes between Task 1 and Task 2 were not big for most participants, and as already pointed out, the average values in Table 4-5 show that the graphic and interaction design as well as the general concepts behind the UI Prototypes V1 are acceptable as a working basis for the CREDENTIAL project.

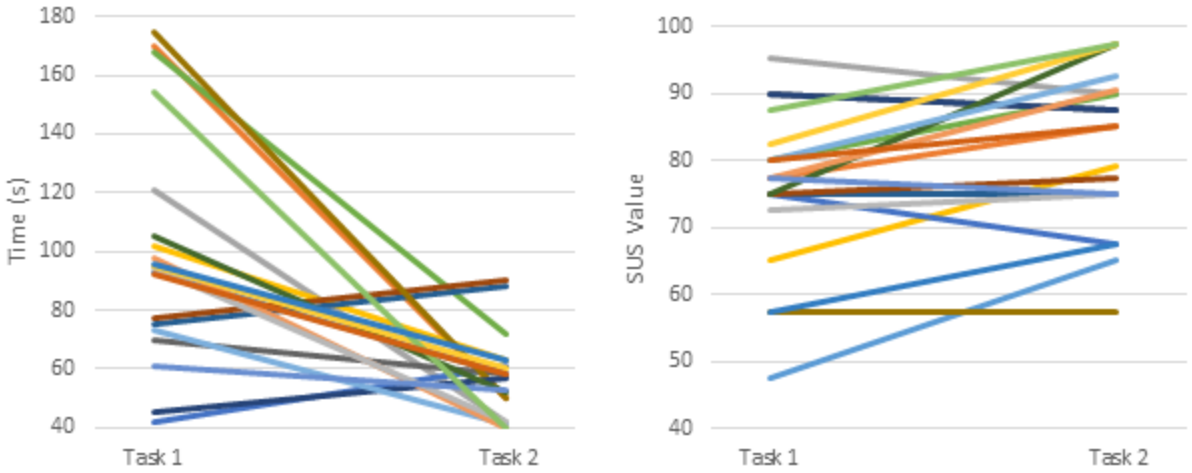


Figure 4-33: Tendency of priming effect between Task1 and Task 2

5 eHealth-specific UI

Independent from the general app for the CREDENTIAL project, the eHealth pilot aims to develop use case specific apps for patients and healthcare practitioners. In the eHealth use cases in section 3.2, the general CREDENTIAL app (the general Wallet) is used only to authorize access by these other apps. Since interfaces have to be different for patients and healthcare practitioners, we describe UIs for an eHealth Patient CREDENTIAL mobile app and UIs for eHealth Practitioner CREDENTIAL tablet app (for the sake of simplicity, we use only "doctor" as practitioner here). These UIs are graphically sketchier than the general ones, and as they anyhow might be issued by some special eHealth developer, they are not given the same colour scheme as the general UIs.

We divide the description of the eHealth specific UI in a patient section and a healthcare practitioner section. We do not use the same persona as introduced in section 4.1 but instead *Alice* for explaining the eHealth Patient CREDENTIAL app. We introduce *Paul* as the user for the eHealth Practitioner CREDENTIAL app.

The UI design process has multiple steps with a couple of iterations. The process is depicted in Figure 5-1. Two of these steps have already been completed and the results are described in the present report. The remaining steps will be performed in the future.

The definition of the use cases builds the basis for the design iterations. The use cases describe what functionality needs to be realised and covered by the UIs (cf. section 3.2). The following step was the first design phase covering an initial description of the views for the UIs. Transitions between those views were defined and thus give the developer an understanding of the process flows between multiple interfaces. This first stage of the UI designs was made on whiteboard or PowerPoint presentations, and have been put into this report in order to document this first phase of the design work. Figure 5-1 is somewhat simplified as the explication of dependencies and necessary steps in these designs have furthered the detailed description of the use cases.

These very first sketches presented here will be transformed in the second design phase where abstract designs were put in a consistent design with pictures, icons and forms. The mockups will be made with design tools like Photoshop and Marvelapp. The next step will be the prototyping step. It is a first clickable iteration of the previous designed interfaces. A "user" can navigate through the different views and thus get a first impression about the look and feel of the UI as well as give feedback to the designer. From here on the design can enter in a feedback loop by collecting the feedback and restart the process with new improved design concepts in the first design steps. Thus, through multiple iterations a satisfying UI design should be accomplished after leaving the prototype phase. The next step is the development (programming) of the UI. All design elements are transitioned in a development framework for apps. Thus, a first version of a clickable and usable application for smartphones is made. The last phase is the integration of the interfaces with the pilot functionality and the CREDENTIAL libraries in order to finalise an app with all the necessary functionality.

The following design concepts for the eHealth pilot are the artefacts created in the first design phase for the patient application as well for the doctor application. They can be found in section 5.1 and section 5.2.

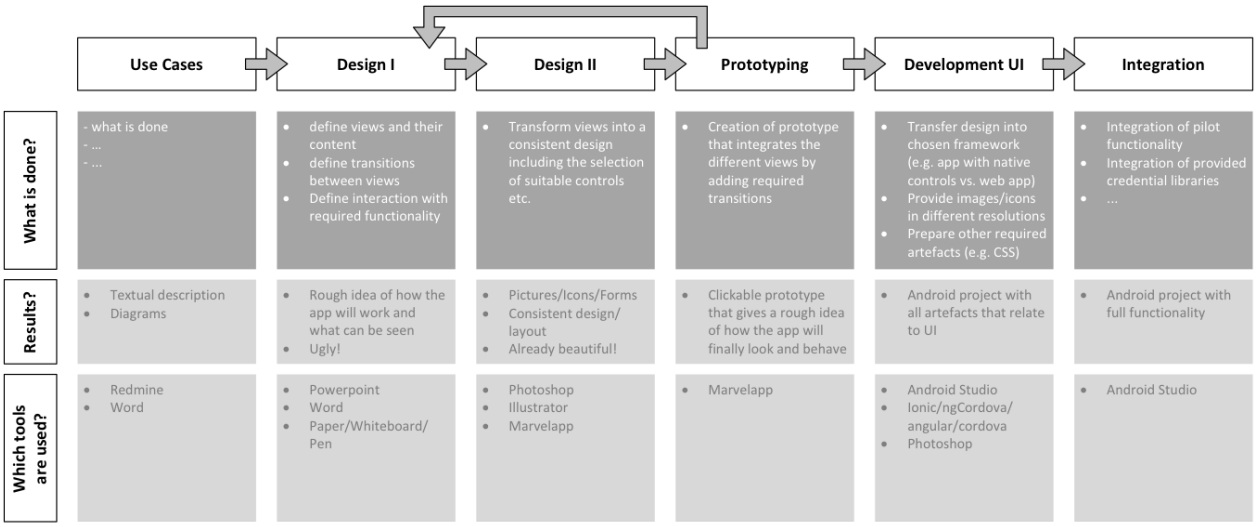


Figure 5-1: UI design process in eHealth

5.1 Patient

The interaction screens for the eHealth Patient CREDENTIAL app can be broken down in the following scenarios:

1. Register a new Patient Health Record
2. My HealthRecord
3. My Data

They are described in the following subsections.

The main screen of the eHealth Patient CREDENTIAL app is depicted in Figure 5-2.

5.1.1 Register a new Patient Health Record

After installing the patient eHealth CREDENTIAL app, Alice has the only option to setup a new Health Record showing in the main screen of the app. Every other functionality in the app is deactivated as depicted in Figure 5-3. Setting up a new Health Record is a task that the patient has to make when she visits her doctor.

By clicking on the Setup Health Record button, she is navigated to the screens depicted in Figure 5-4. The first option she has is to scan a QR code which she receives from her doctor. A Patient Health Record (PHR) is always initiated by the doctor but needs to be confirmed and registered with the patient consent. In order to do so, Alice needs an already active CREDENTIAL account and the generic CREDENTIAL app installed. If she does not have any yet, she has to install the CREDENTIAL app and create her CREDENTIAL account as described in chapter 4.1.1.

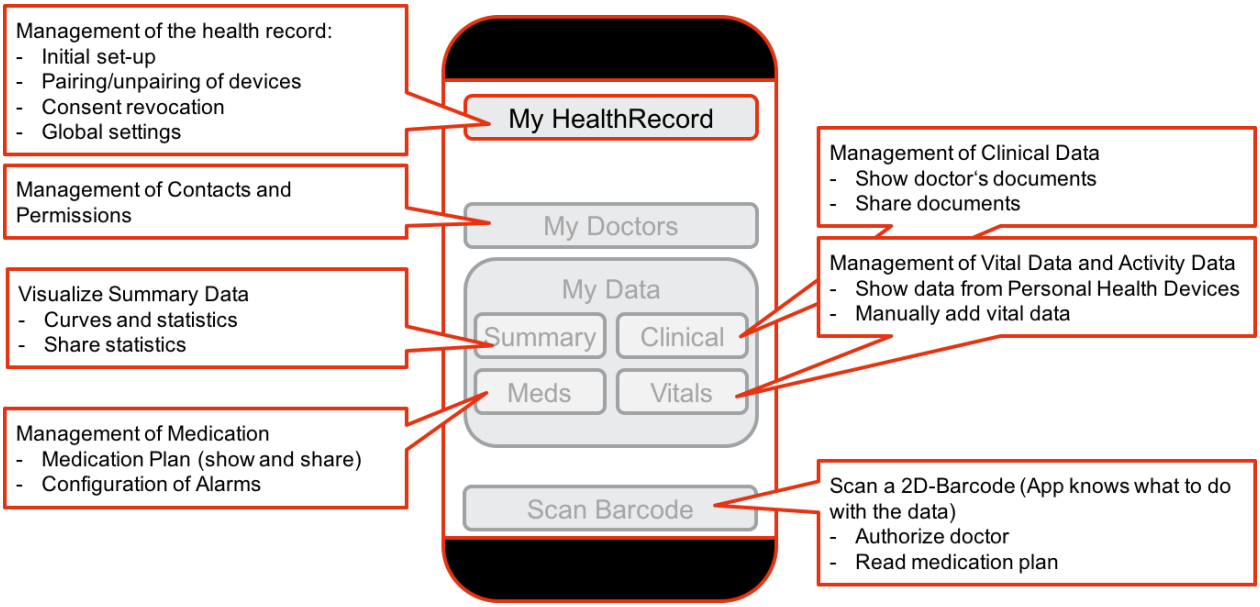


Figure 5-2: Main menu of the eHealth Patient CREDENTIAL app

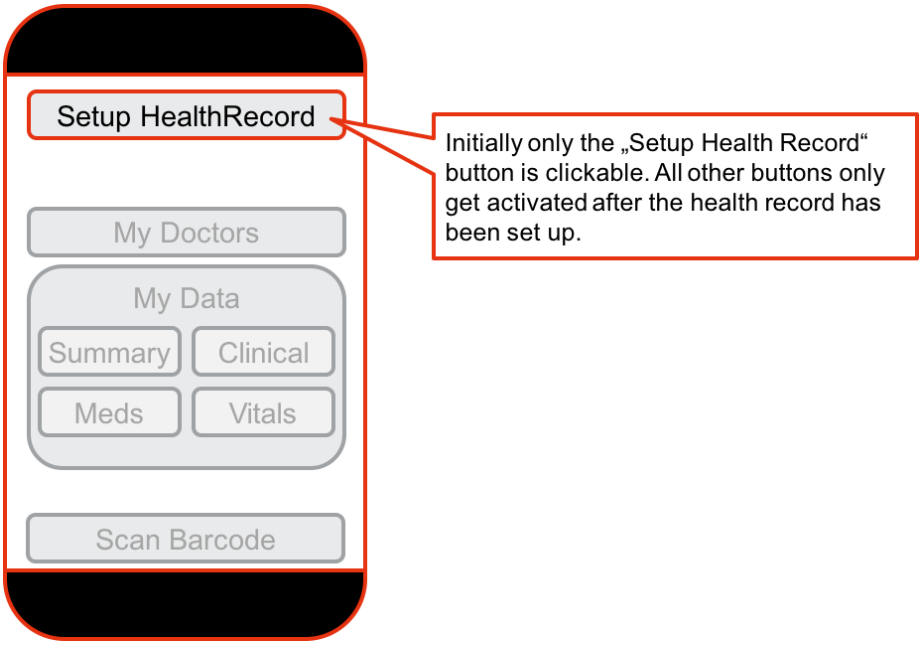


Figure 5-3: Setup a new Health Record

After scanning the QR Code in Figure 5-4 she is navigated to a register form where she is prompted to provide personal data and her health insurance number. After clicking the "OK" button, the internal processes for activating the PHR for Alice are triggered. The app sends an authorization request to the CREDENTIAL Wallet and she is forwarded to the generic CREDENTIAL app (which user interface is in blue colours as in the previous section on the general UIs).

The “CREDENTIAL Wallet” opens with a notification about the request from the doctor who wants to have full access to her PHR directory. After accepting the request (compare Figure 4-23), she is navigated back to the eHealth Patient app and can proceed.

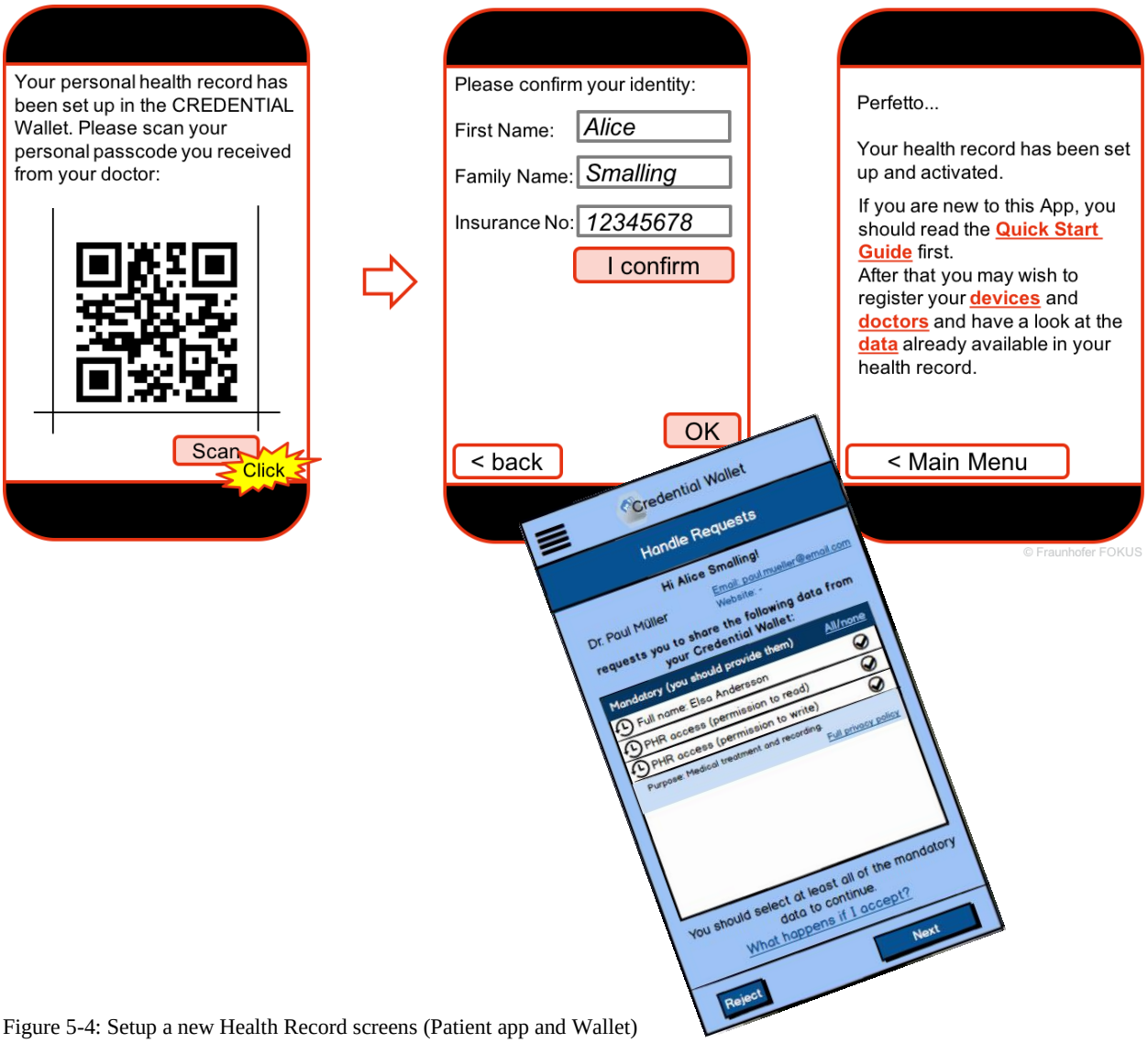


Figure 5-4: Setup a new Health Record screens (Patient app and Wallet)

5.1.2 My Health Record

When Alice wants to configure her health record she can click on the “My HealthRecord” Button in Figure 5-5. She is presented with three different options. The first one is to open an event list where the recent events can be viewed. The second option is the protocol about all actions that have been made in the past related to the PHR of Alice. For example, accessing or changing data in Alice’s PHR. The eHealth pilot does not specify own interfaces for the views since similar functionality is already described for the generic UI. Therefore, the UI designs described in section 4.1 where the notification and access log screens are described.

Furthermore, Alice has the option to configure the settings for her Health Record and to revoke her consent to all practitioners having access to her Health Record. By clicking on "Configuration" she is navigated to the configuration screen as depicted in Figure 5-5. There, she can activate the option if she wants to receive notifications about new data that is added to her PHR. For example, she can receive a notification when her doctor adds or modifies a medication plan for her. The common behaviour of the eHealth Patient App when adding new data requires an explicit authorization decision by Alice. If she wants to shortcut these decisions, she can confirm, that every contact in her personal address book can add new data to her PHR. She can do this by activating the "Registered contacts may add data without explicit authorization" button.

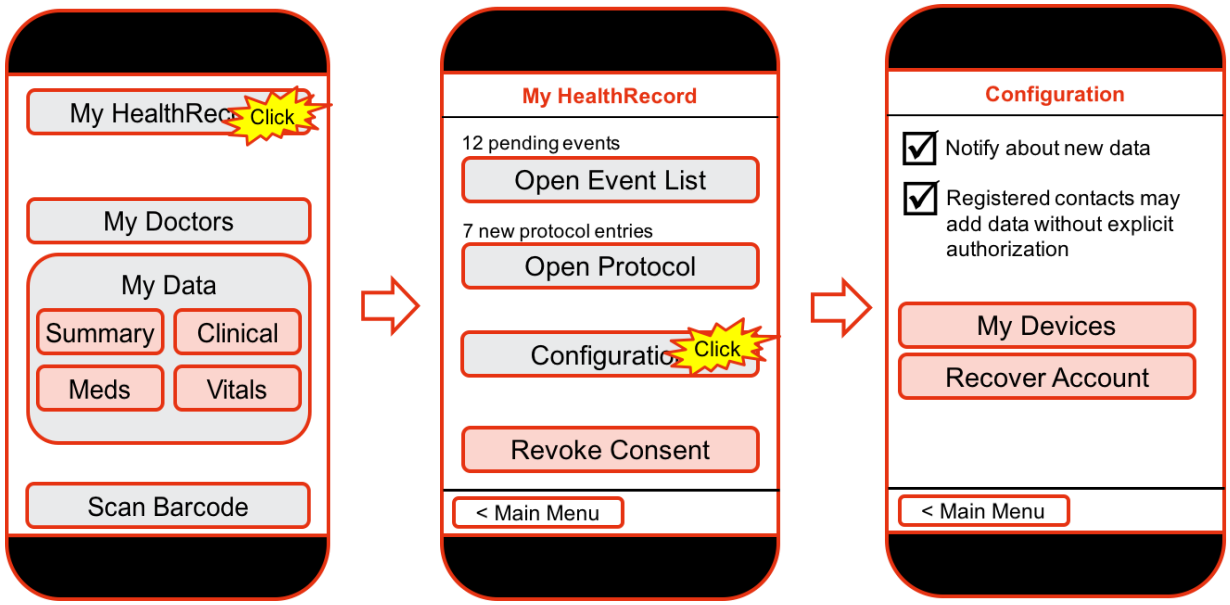


Figure 5-5: eHealth Patient app configuration screen

Two more buttons give Alice the option to view her paired devices with the eHealth App as well the possibility to recover her account. The option to recover her account is already explained in section 4.1.1 and thus will be integrated in the eHealth Patient App. The view of the connected devices is also described in section 4.1.2. The eHealth pilot however, will extend it a little bit to give the connected devices more context information. Thus, Alice can connect a specific Glucose meter, a certain digital scale, and a step counter to the eHealth app. The process is depicted in Figure 5-6.

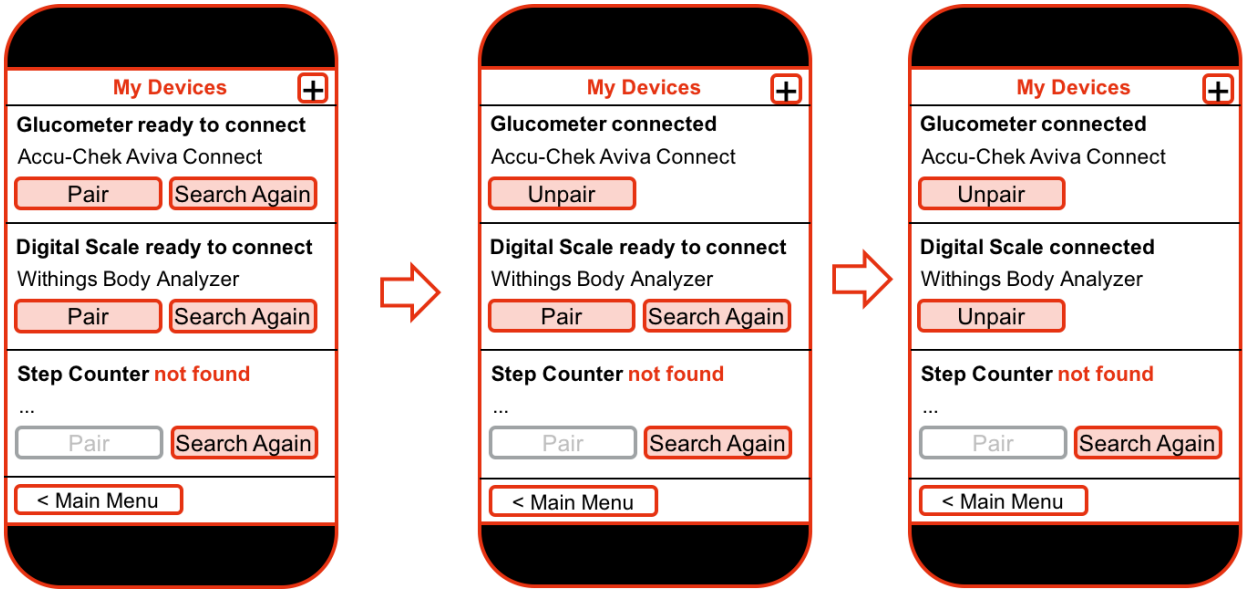


Figure 5-6: eHealth Patient app's My Devices screen

5.1.3 My Data

The data screen is divided into four subscreens, viz.:

1. Summary
2. Clinical
3. Medications
4. Vitals

The following four sections summarizing and explaining how the subscreens are looking like and how the interaction by clicking on certain items is performed.

5.1.3.1 Summary Screen

By clicking on "Summary", Alice is guided to the Summaries and Curves view of the eHealth Patient CREDENTIAL app. The view is depicted in Figure 5-7. She sees a split screen with two statistical views on her average blood sugar level as well as the HBA1c measurements over the last few months. By clicking on the screen, a new view is shown with a detailed view on a specific time frame of the selected medical data.

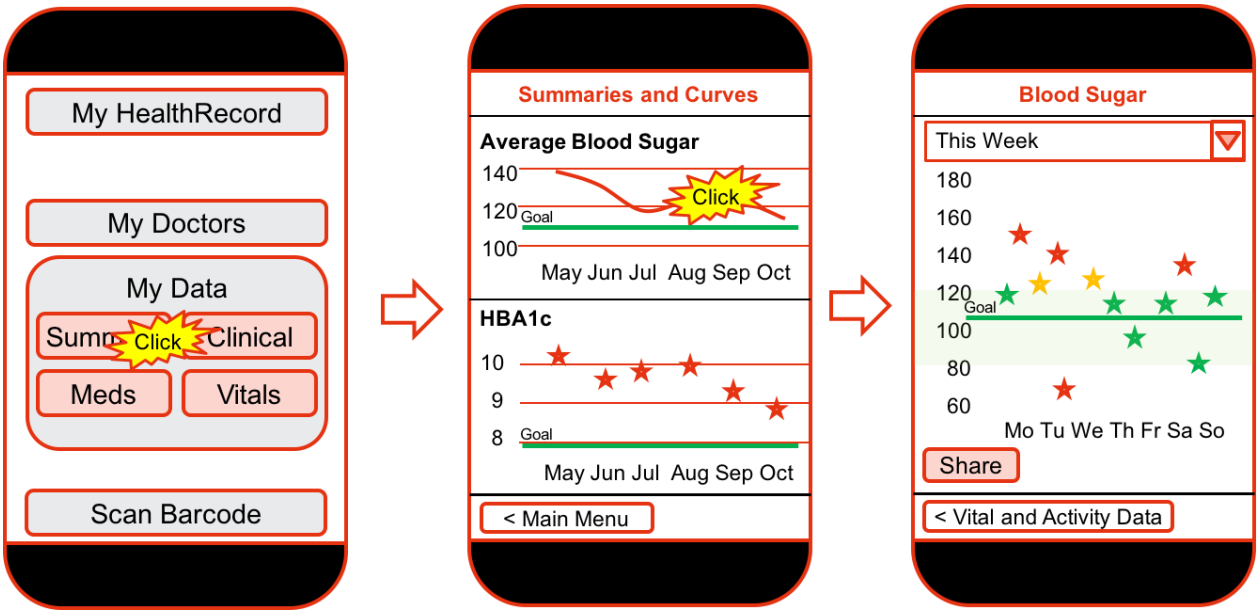


Figure 5-7: Summaries and Curves screen

5.1.3.2 Clinical Screen

If Alice wants to view her clinical data she can do so by clicking on the "Clinical" button. The app navigates to a view with all the clinical documents registered in her PHR. Each clinical document is represented in a list entry showing the relevant metadata for the document. This contains the name of the document, the creation date and the name of the healthcare practitioner who created it. By clicking on one of the entries, the app navigates Alice to rendered view of the clinical document. The example mockups are depicted in Figure 5-8.

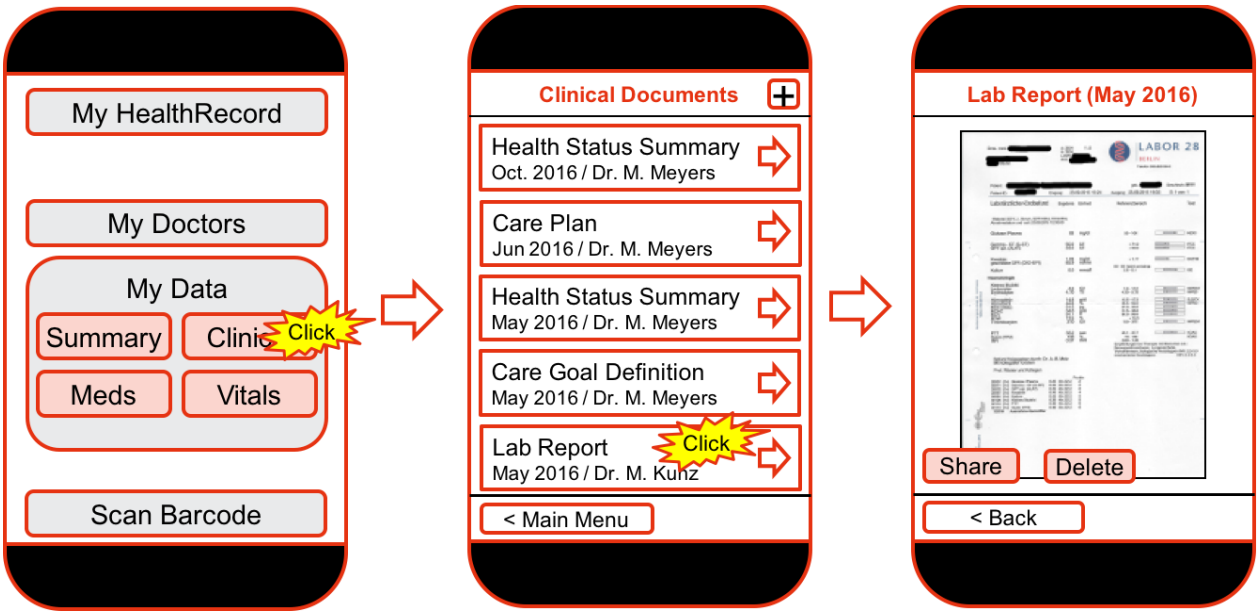


Figure 5-8: Clinical Documents screen

5.1.3.3 Medications Screen

Alice needs to be informed about her medications she has to take. In order to keep track of it she can click on the “Medications” Button. The app navigates her to the “My Medications” screen. Every medication of her medication plan in her PHR is listed with metadata information. She can click on a medication and the app navigates to a screen showing the medication information and when she has to take the medication. She can configure an alert whenever the medication has to be taken. The screens are depicted in Figure 5-9.

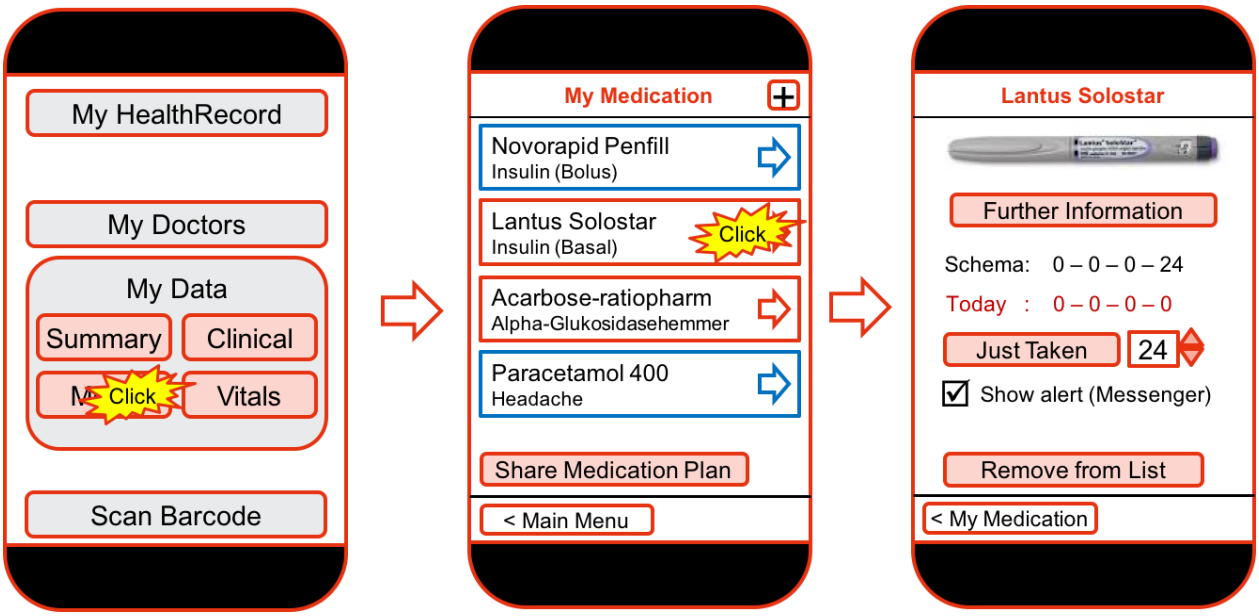


Figure 5-9: Medications Screen

5.1.3.4 Vitals Screen

If Alice needs to view here last vital and activity data collected by her smartphone or connected activity tracker devices, she can click the “Vital” button in the main screen. The app navigates her to the vital and activity data split screen showing her a statistic overview about her body weight and performed steps over the period of the last half year. By clicking on the graph, she is navigated to a detailed view about her vital data showing a particular week. The screens are depicted in Figure 5-10.

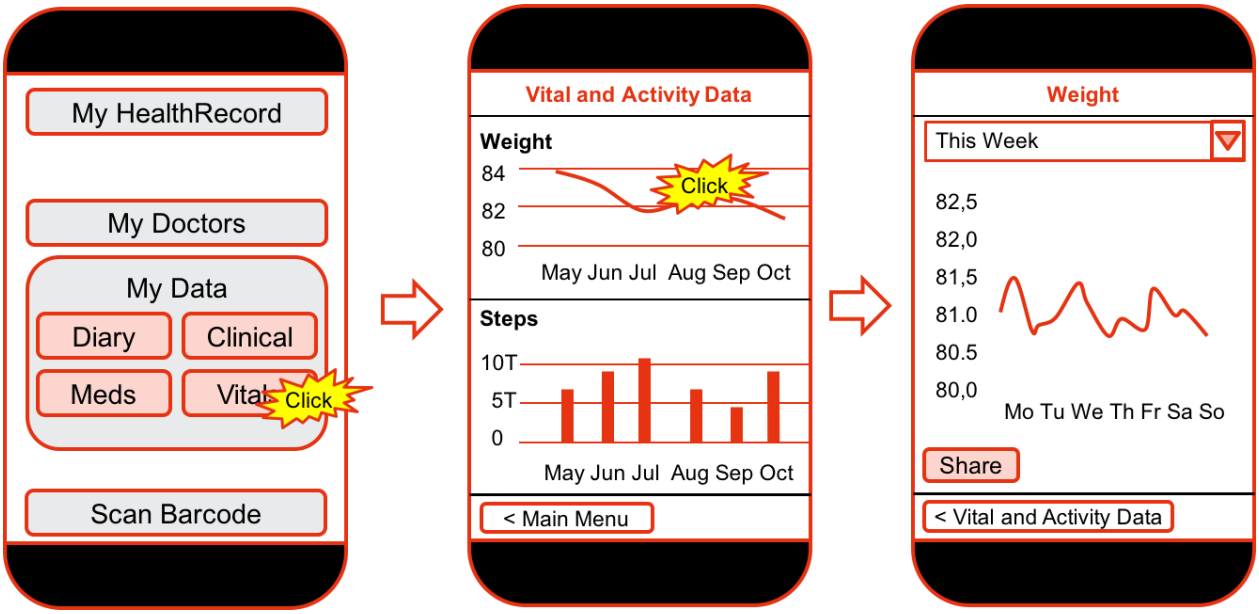


Figure 5-10: Vital and Activity Data screen

5.2 Doctor

In the pilot, the prototypical eHealth worker will be a doctor. We call the doctor Paul. Paul runs his CREDENTIAL eHealth app on a tablet, not on a smartphone, as we imagine health workers to have a need for a better overview. including The interaction screens for the eHealth Doctor CREDENTIAL app can be broken down in the following scenarios:

1. Patient Registration
2. Patient Search
3. View Notifications
4. View Documents
5. Edit Medication Plan
6. View Patient Diary
7. View Vitals and Lab
8. Add Alerts
9. Create Therapy Summary

The main screen of the eHealth Doctor CREDENTIAL App is given in Figure 5-11. The interface is kept rather simple but unfolds more functionality by clicking on the buttons. On top of the screens are icons to view the patients that the doctor has added. A notification icon signals if new alerts or notifications have arrived. Paul, the doctor, has in addition a drop-down search field where he can select already added patients or search for them by a detailed search functionality. If a new patient needs to be added, Paul can do so by clicking the “+” button.

The following sections explain the different interaction screens for each of the above-mentioned functionalities.

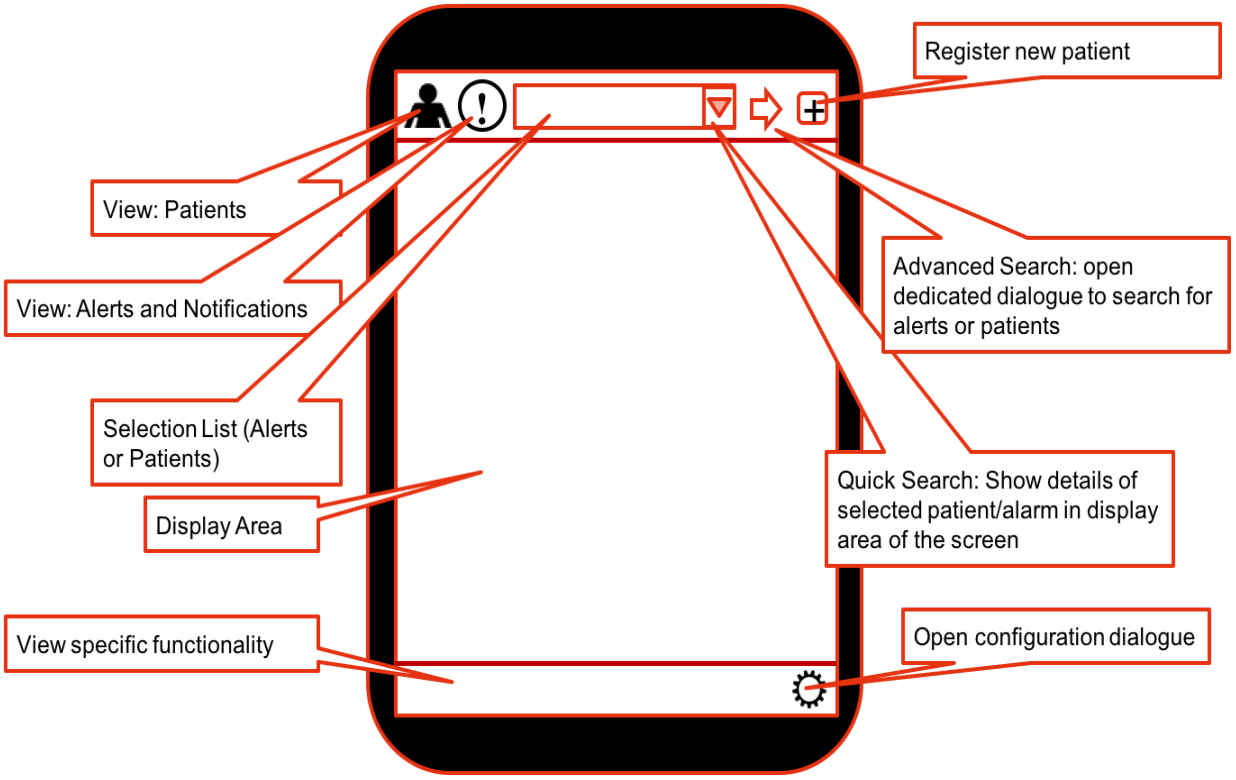


Figure 5-11: Doctor app main screen

5.2.1 Patient registration

When Paul wants to introduce a new patient to the CREDENTIAL eHealth system, he can do so by clicking on the "+" button to add a new patient. The app shows him the form "Patient Registration" as shown in Figure 5-12 where basic patient identity information can be added. Gathering that information can be short-cut by reading these data from the patient's electronic health card. Paul requests a written consent from Alice, the patient, and confirms that he has fully informed her. He clicks on the "Register Patient" button and receives a notification with detailed instruction how to activate the patient's PHR.

Figure 5-12: Doctor app's Patient Registration screen

5.2.2 Patient Search

The app supports Paul by finding records for his patient Alice Smalling. He clicks on the "Patient Search" button and the app navigates to the "Patient Search" view (Figure 5-13). He can provide basic patient information like the name or family name of the patient. He can further refine the search to filter only patients with new documents or pending alerts. By clicking on the "Search" button a list of all patients, their number of alerts, and number of documents are shown. Paul can click on a patient entry and the app sets the context for this patient.

5.2.3 View Notifications

After Paul set the app context for a particular patient, he can view the pending alerts and notifications for this patient. They are shown as a drop-down list under the pending alerts and notifications entry. Alerts are marked as red entries and notifications about new data or new documents are highlighted as blue. Thus, he can immediately see which types of new information about the patient are available. By clicking on one of the entries he sees more detailed information. The pending alerts and notification screen is depicted in Figure 5-14.

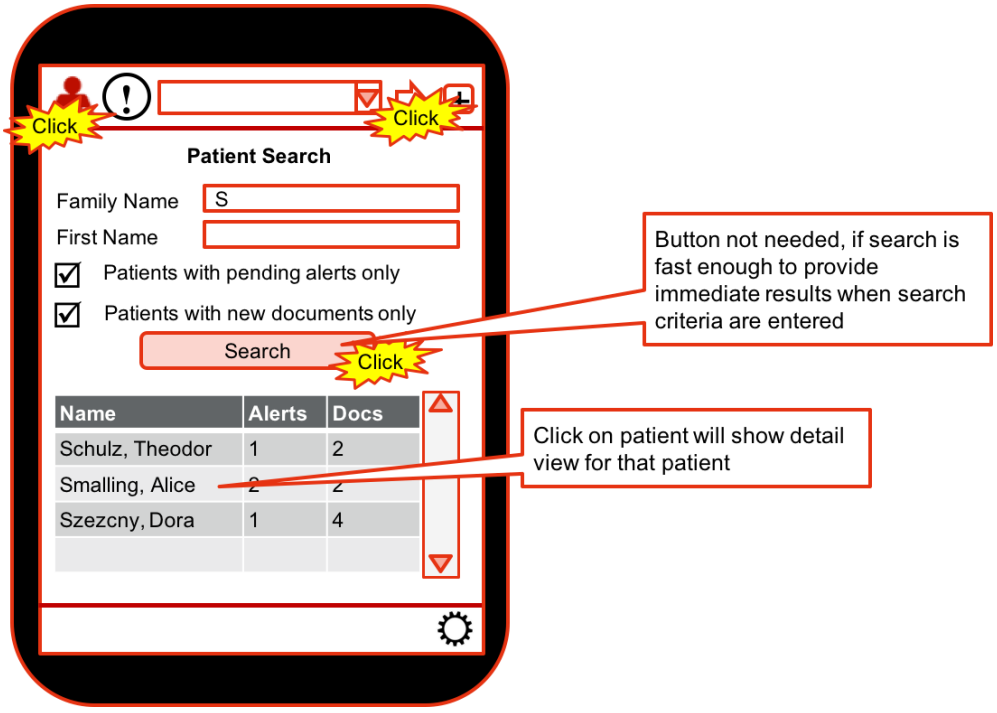


Figure 5-13: Doctor app's Patient Search screen

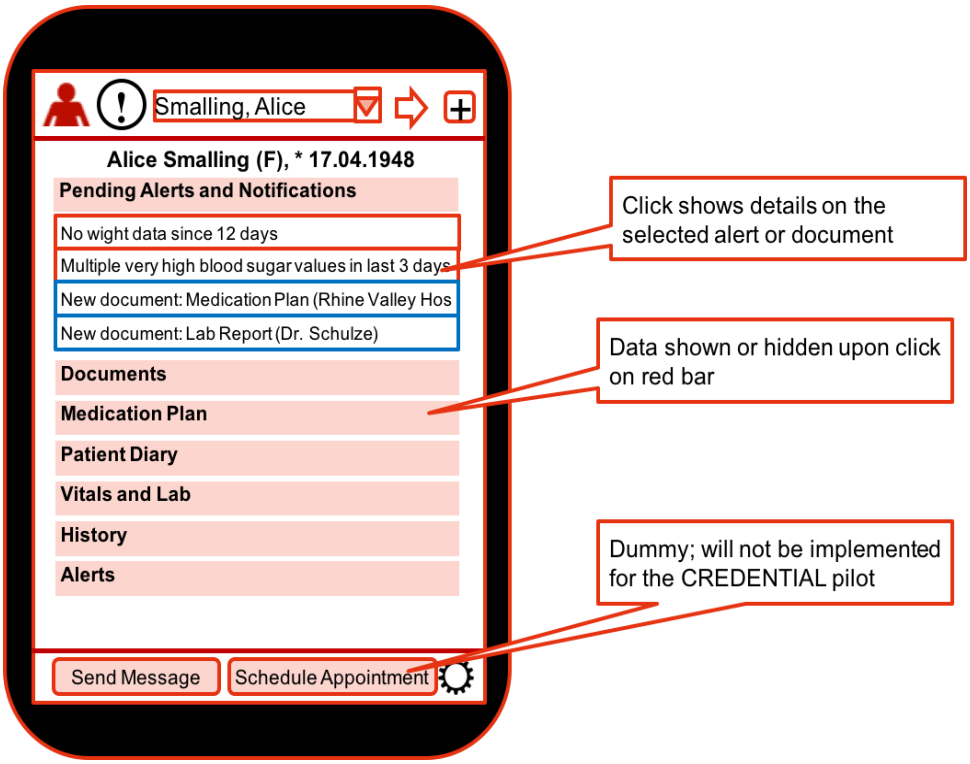


Figure 5-14: Pending Alerts and Notifications screen

5.2.4 View Documents

Paul can view all documents for the selected patient by browsing through the documents drop-down list in Figure 5-15. The documents are ordered by their creation date. The documents in this list are marked with colours to represent certain states of them. New documents are indicated by a red colour, documents created by Paul himself are grey marked and documents created from external doctors or the patient herself are blue. If Paul needs a certain type of document or data from the patient, he can request these by clicking on the respective button. New documents for the patient can be created by either select and uploading an existent document or by creating a complete new document.

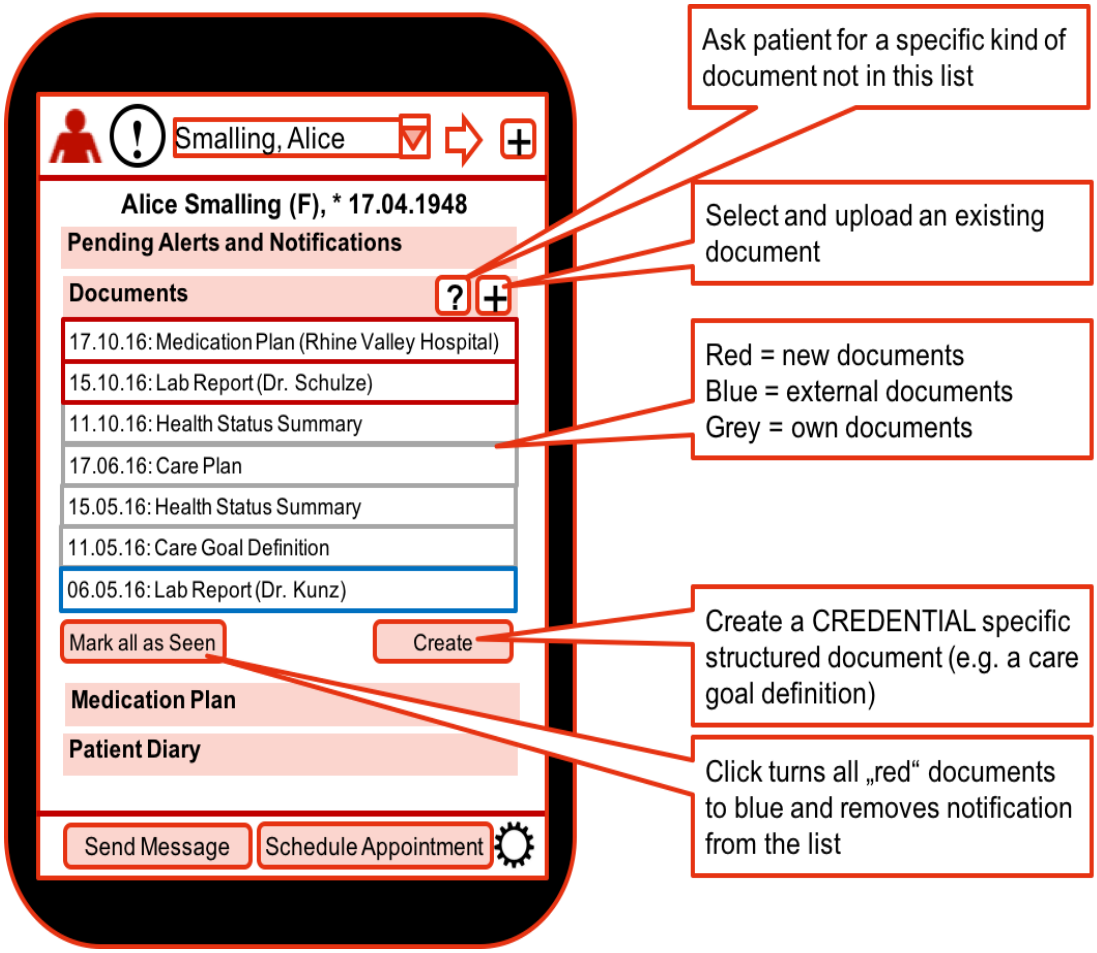


Figure 5-15: Patient documents screen

If Paul wants to see the document's content, he can do so by clicking on the document entry. The app navigates to the show document content view. PDF documents are rendered within the app. If it is a structural document, the app renders a HTML view and shows it to Paul. This interaction is depicted in Figure 5-16.

When Paul requests a certain type of document or data from the patient, the app navigates to the request document view. He can select a predefined document type from a drop-down list and enter a note that will be included in his request. By clicking on the "Request Document" button a notification is sent to the patient via the CREDENTIAL notification system. This process is depicted in Figure 5-17.

When Paul wants to add a new document the app navigates him to the create document screen as depicted in Figure 5-18. He can select a document type from a drop-down list. The document details are shown in the bottom half of the screen. The content and which fields he can add depend on the document type. If the document should be a new version of a previous document, he can initialize it with the data from the last document with the same type.

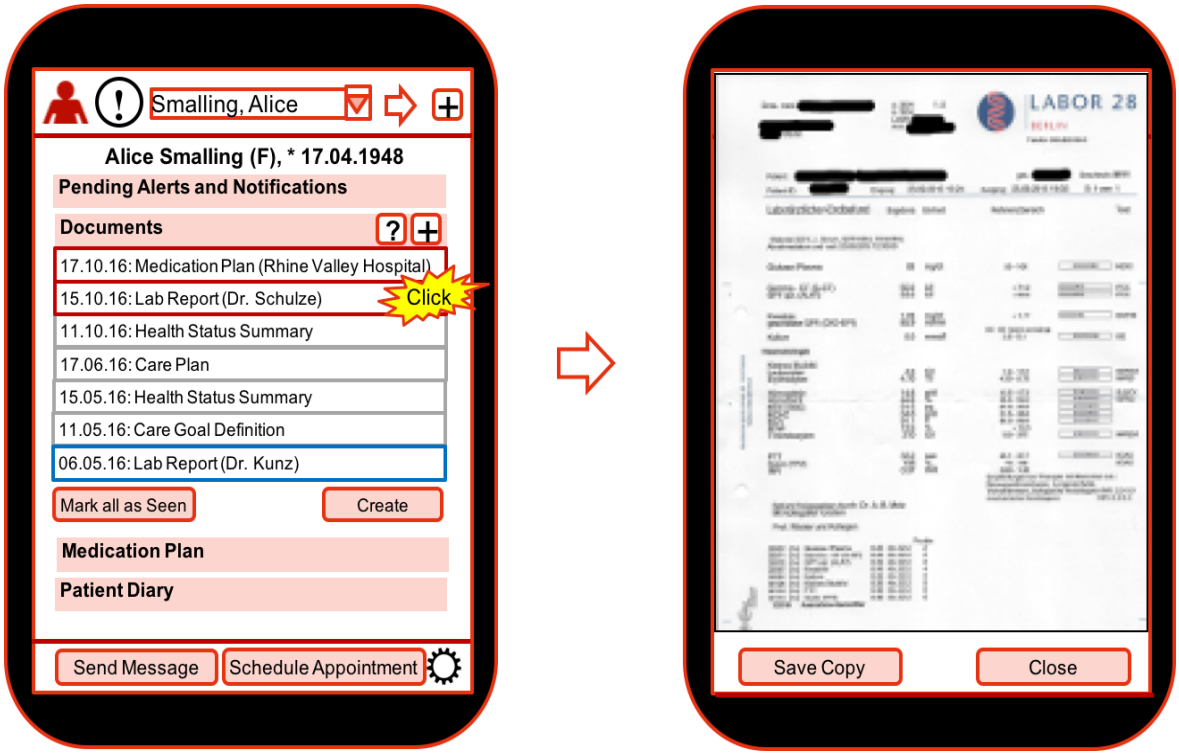


Figure 5-16: How to show document content (Doctor's app is run on a tablet, not a smartphone)

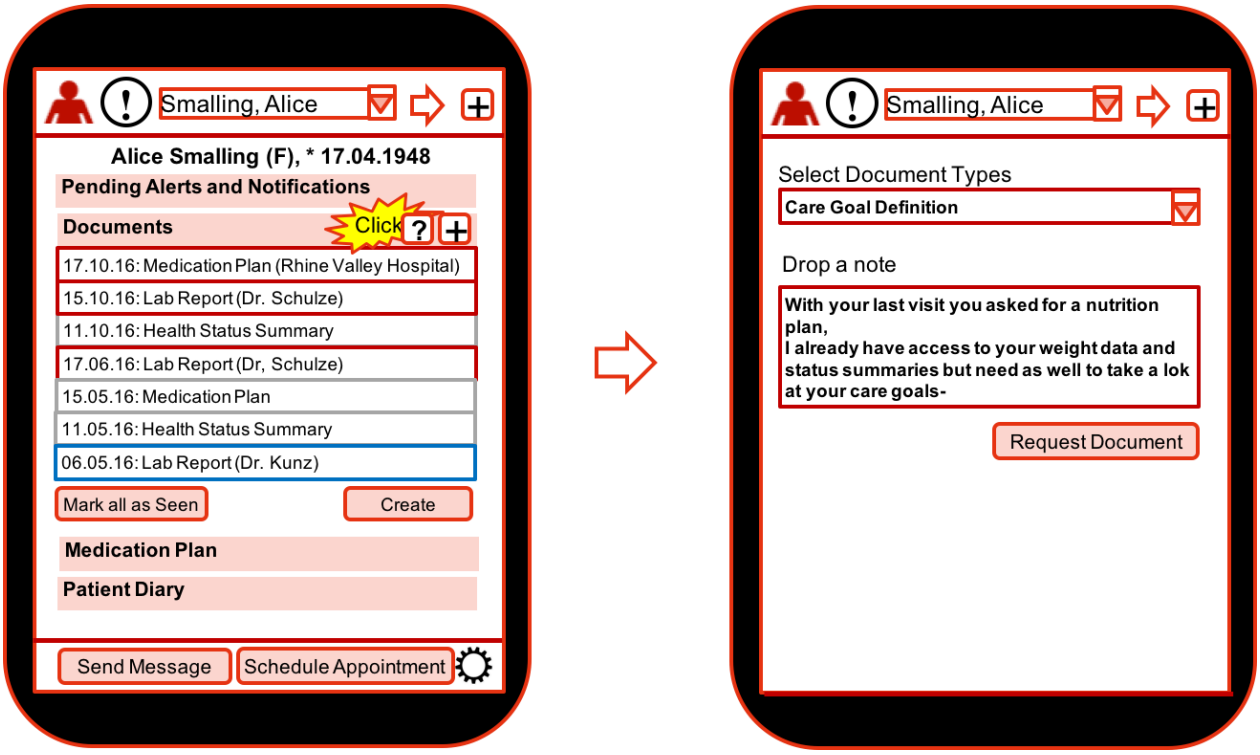


Figure 5-17: Doctor requests a document from a patient

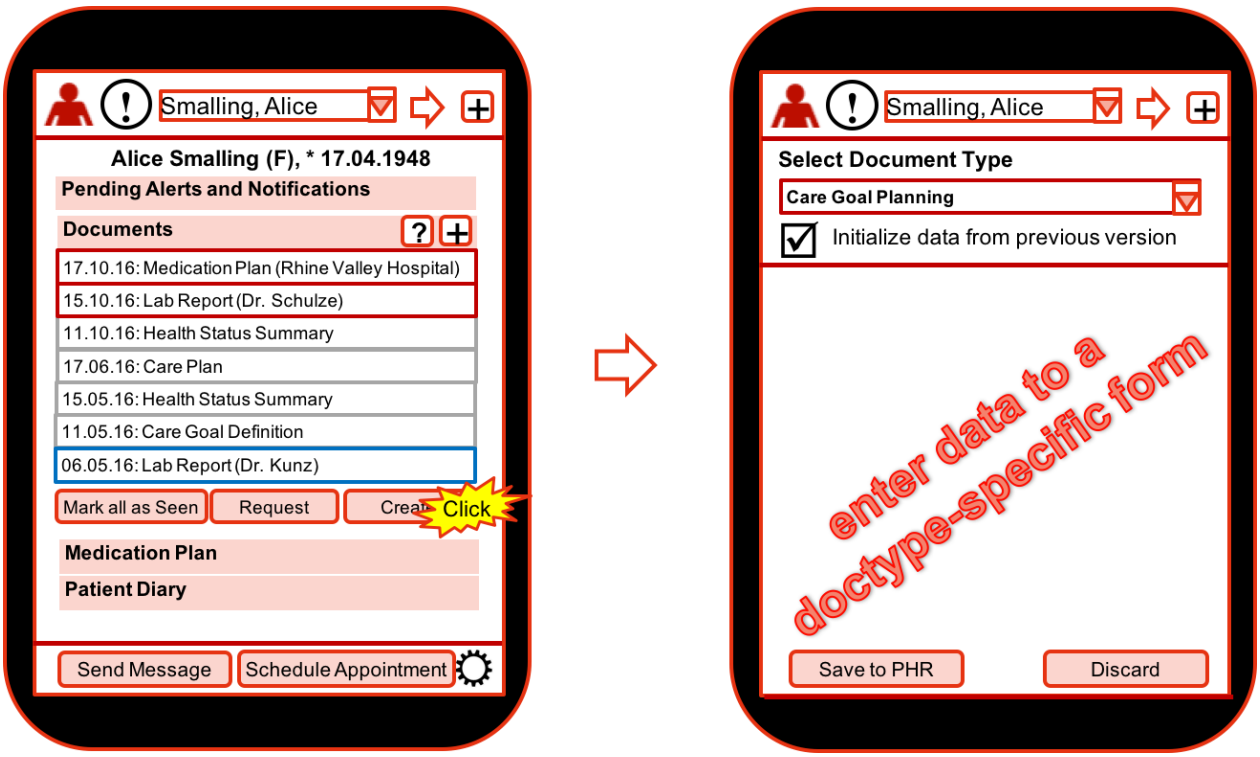


Figure 5-18: The screen for creating a new document for a patient

5.2.5 Edit Medication Plan

The medication plan for a patient contains all the medicinal products she has to take. The medication plan screen is shown in Figure 5-19. Paul can view all the medications in one drop-down list. If he has not already access to the patient's medication plan he can request access to it.

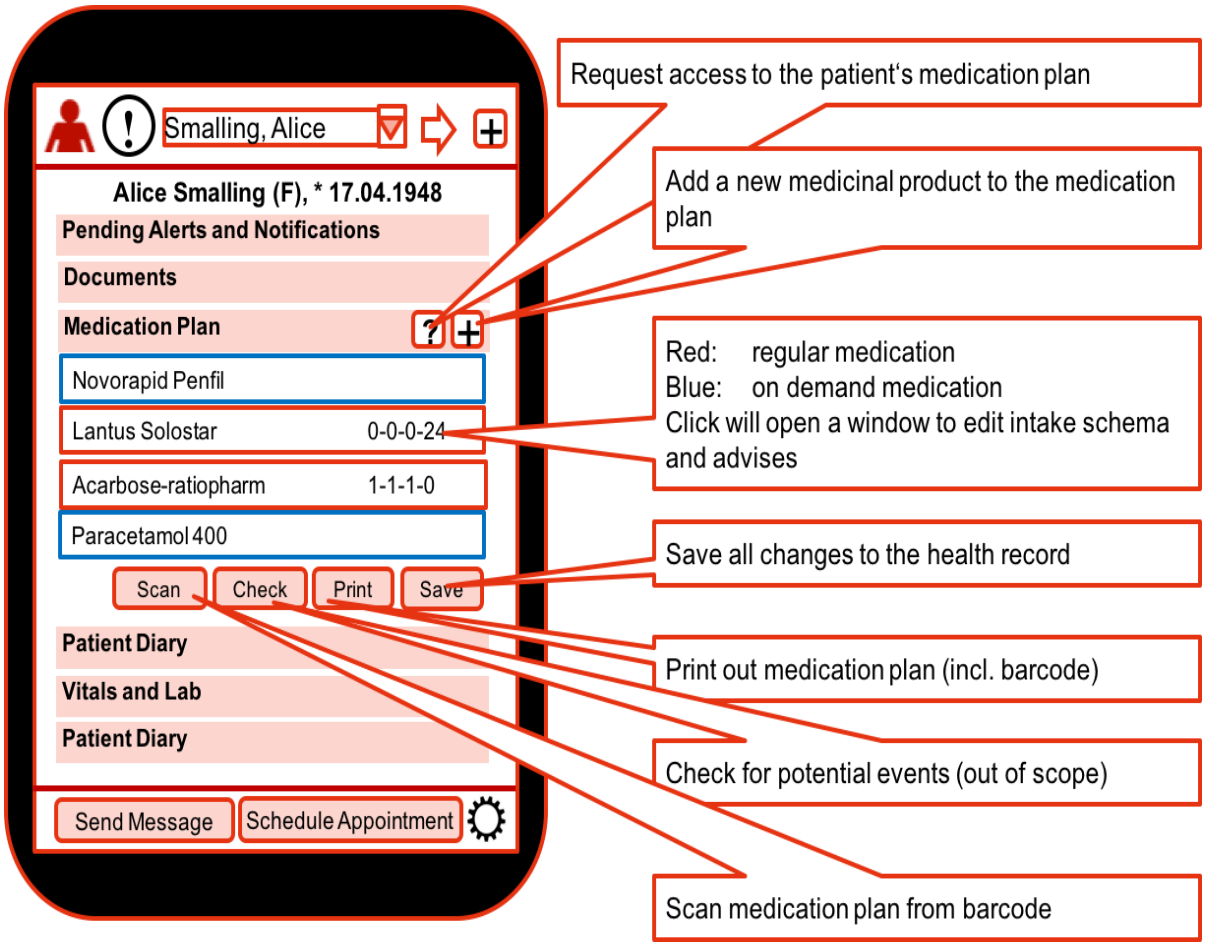


Figure 5-19: Doctor's screen for patient's medication plan

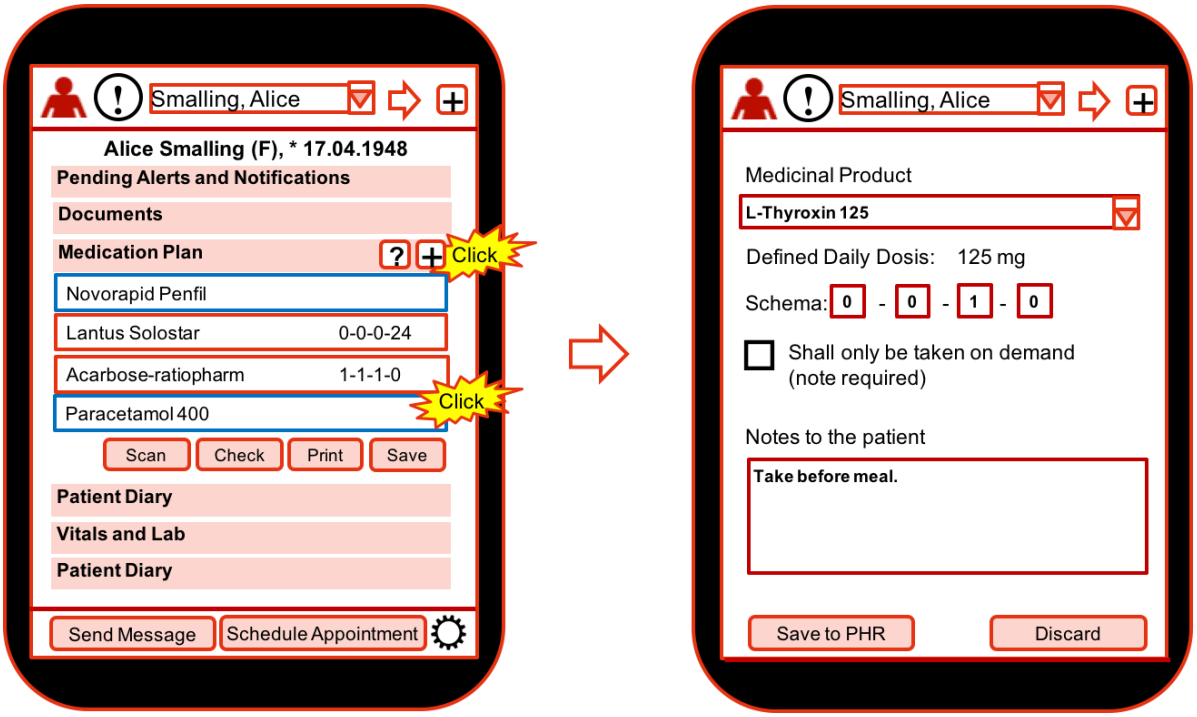


Figure 5-20: Doctor's screen after clicking on Medication Plan

5.2.6 Add Alerts

Dr. Paul can manage the alerts he wants to receive for a particular patient. In order to do so, he can click on the Alerts tab as depicted in Figure 5-21. The doctor is presented a view with the recent occurred alerts of the selected patient, Alice, within a preselected timeframe of the last 6 months. The timeframe presents events about regular data that have not been provided by the patient as well as exceeding thresholds for the Hyperglycemia and Hypogycemia values that were measured by the patient.

When Paul clicks the "+" button he opens the "Add a new alert" view depicted in Figure 5-22. There he selects thresholds for the values he wants to be notified about:

- If the patient does not provide data for a given timespan
- If the value for hyperglycemia exceeds the given threshold
- If the value for hypogycemia exceeds the given threshold

After clicking on the OK button the new alert is added and Paul is navigated back to the main screen.

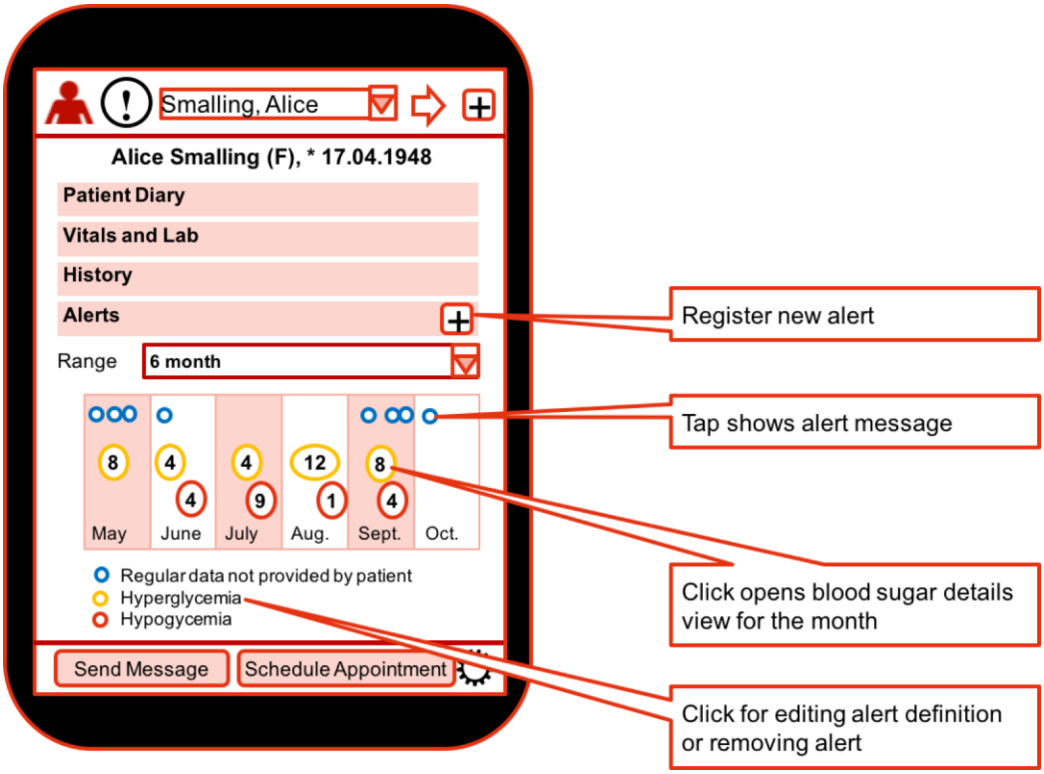


Figure 5-21: Manage alerts

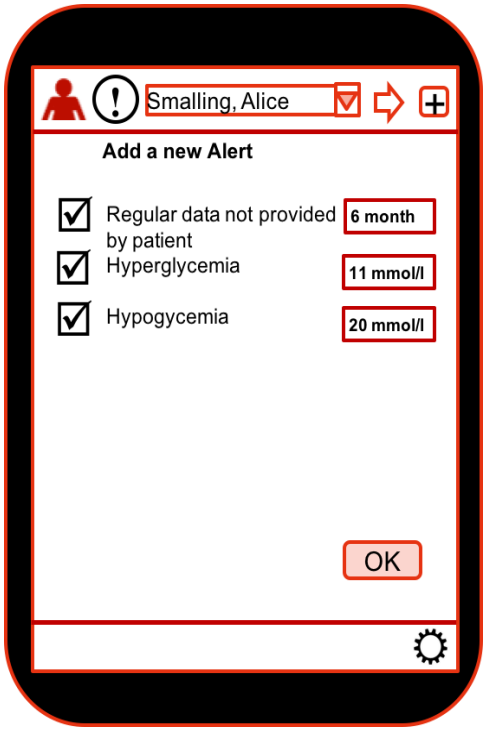


Figure 5-22: Add a new alert

5.2.7 Create a Therapy Summary

The therapy summary is used to register Alice's need for a sponsored wearable glucometer. Paul documents and verifies in this document the diagnosis, the care status, the therapy progress and selected compliance indicators about his medical treatment relationship and the health status of Alice. The proposed UI for verification is depicted in Figure 5-23. Paul starts by clicking on the create button in the "Therapy Summary" view. The app shows the "Create new Therapy Summary" screen. Here Paul has the options to provide a name for the therapy summary as well as the needed information for diagnosis, care status, therapy progress, and compliance indicators. After he has finished everything, he can click on the Sign button and save it to the CREDENTIAL Wallet by clicking on the "Save to CREDENTIAL" button. As yet undefined: If he clicks directly on a "Save" button, the document might automatically be signed or this action saves the unsigned document for further editing of the summary.

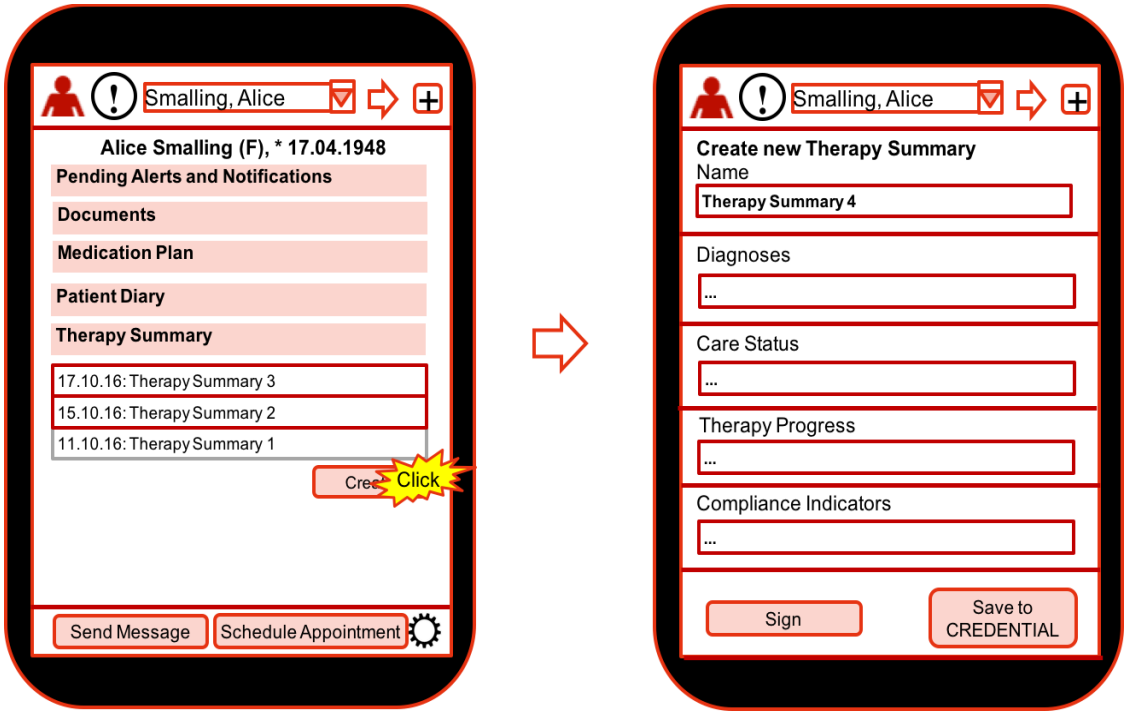


Figure 5-23: Create and Sign Therapy Summary in doctor app

5.3 Additional Comments on UI for the eHealth Pilot

This section has described the user interface for the eHealth pilot and specifies how the pilot specific Patient's app as well as the Doctor's app look like and interact with each other. The Patient's app is described as a standalone smartphone app which operates together with the generic CREDENTIAL app. The Doctor's app is designed as a tablet app and works independently from the generic CREDENTIAL app. The Patient's app extend the basic functionality of the generic CREDENTIAL app and defines a UI that considers the medical-specific interactions from patients and doctors while harmonizing with the way how the generic UI concepts should be used by the CREDENTIAL participants.

6 Research Challenges: Adoption of New Technologies

To what extent will people understand and appreciate the benefits offered by solutions like the CREDENTIAL Wallet? Previous research show that there is a general lack of understanding among users of different login solutions, and a lack of appreciation of identity providers, etc. This section depicts the main frameworks that researcher the last half a century have used to understand the adoption drivers for new technologies and also hints at possible reference frameworks for questionnaires to use in surveys or in usability tests within the project. It also reports related questions for specific problems concerning identity provision, such as multi-factor authentication and authorization frameworks, the user understanding of the presently so common social login options and also discuss risk communication. Some of the work behind the things reported here will be further developed in a theoretical direction while others has had a direct impact on the development of the UI Prototypes V1.

6.1 Adoption of Internet Technologies and Services

This section presents an overview of theories for studying the adoption of new technologies and services, and identifies how these methods have been considered for analyzing the adoption of Internet services.

The *classical diffusion theory* has increased our understanding of how innovations (e.g., a new protocol) spread within populations. Rogers' diffusion of innovations theory (1962) breaks the adoption process down into five stages. In the *knowledge* stage, the individual is exposed to the innovation, but lacks complete information about it. In the *persuasion* stage the individual becomes interested in the new idea and seeks additional information about it. The next stage is *decision*, where the individual mentally applies the innovation to his present and anticipated future situation, and then decides whether or not to try it. In the *implementation* stage the individual employs the innovation. Finally, in the *confirmation* stage the individual decides to continue the full use of the innovation.

Rogers also defines five categories of adopters. *Innovators* are the first individuals to adopt an innovation and they are willing to take risks. The second fastest group who adopt an innovation is called *early adopters*. *Early majority* represents those who adopt an innovation after a varying degree of time, which is significantly longer than the first two groups. *Late majority* represents the group that adopts an innovation after the average member of the society. Finally, *laggards* are the last who adopt an innovation.

Rogers furthermore presents five characteristics of an innovation. The *relative advantage* is the degree to which the new technology is better than a preceding one. *Compatibility* is the consistency with existing values, past experiences and needs. *Complexity* is the difficulty of understanding and use. A new technology is more likely to be adopted if it is compatible with existing practices of adopters, and is relatively easy to understand and use. *Trialability* is the degree to which it can be experimented with on a limited basis. Finally, *observability* is the visibility of its results.

The diffusion phenomenon has also been studied from a community point of view, focused on the economic value an innovation brings to potential adopters. This economic value to an adopter depends on the size of the existing network of adopters and the potential network of adopters. Katz and Shapiro (1986) analyze the adoption of a new technology for cases where network externalities are significant. Adoption becomes more likely when the number of current adopters in the network increases.

There are also some other concepts mentioned by Katz and Shapiro that influence adoption of a new technology, i.e. the *development of a related technology infrastructure*, *economies of scale*, *communication channels* which could also help the process of diffusion of innovation, the *presence of sponsorship* which decreases the risk of adoption, etc. Hence, despite the fact that a new technology is considered to be superior to the incumbent, an adopter may still not adopt the innovation. For example, adopters may be unwilling to bear the incompatibility cost and the risk of being locked into the innovation before it reaches critical mass.

Last but not least, *information asymmetry* could lead to different incentives and strategic behaviours in the technology adoption game. In particular, Zhu and Weyant (2003) present how asymmetric information affects firms' decisions to adopt a new technology, by using game theory. In particular, the authors compare two information structures under which two competing firms have asymmetric information about the future performance of the new technology. Zhu and Weyant conclude that equilibrium strategies under asymmetric information conditions are quite different from those under symmetric information conditions.

The theories presented above have mainly been used for studying the adoption of consumer products. However, the adoption of new Internet protocols and services, such as those developed within the CREDENTIAL project, is more complex than that of consumer products, and therefore requires more elaborated modeling. Several attempts have been made at studying the adoption of new Internet protocols and services.

In particular, the IAB has identified the most important factors that enhance or limit the success of a protocol based on several case studies (Thaler and Aboba, 2008). Although a protocol design will not necessarily be able to incorporate all the proposed success factors, experience indicates that following some of them will improve the probability of success. The most important factors for the initial success are *filling a real need* and being *incrementally deployable*.

Hovav *et al.* (2008) present a model of Internet standards adoption that identifies additional factors that influence adoption of a new technology, focused on the IPv6 protocol. Development of a *related technology infrastructure*, *economies of scale* and *amount of information* available could also help a new protocol to spread. Moreover, the presence of *sponsorship* will decrease the risk of adoption, and thus could positively influence the adoption rate and adoption extent of the new protocol.

In the study by Joseph et al. (2007), an economic model based on users' utility is used to study the adoption of new network protocols and services. The model incorporates various factors, such as *user* and *network benefits*, and *switching costs*, and discusses the impact of *converters* on the adoption of new Internet protocols and services. Key findings include that new Internet protocols and services need to withstand a period of decreasing total system utility till a critical mass of users is reached.

The aforementioned models could improve our understanding, as well as guide the design and implementation – and even the presentation – of mechanisms enhancing the adoption of the CREDENTIAL services. The following subsections go into more detailed structures and problems of what may influence (potential) users understanding and willingness to adopt.

6.2 CREDENTIAL Wallet Adoption

To generate a real impact with CREDENTIAL it is of paramount importance that users understand the benefits and are willing to adopt the new technology. This section thus takes a look at the Technology Acceptance Model and how its factors can be related to CREDENTIAL features.

However, we first want to give a concise overview of the most important benefits that users can expect from the tools and technologies developed within CREDENTIAL. These benefits correspond to the main ambition of the project and are also in line with the requirements set out in Deliverables D2.2, D2.3, D2.5, and D2.6. Additional factors for adoption not listed here include the concepts discussed in section 6.1.

Table 6-1: Benefits of the CREDENTIAL Wallets solution

Benefit	Description	Scenario
Selective disclosure	Users have full control over which data should be revealed to which service provider. These rights can be adjusted dynamically and are enforced on a technical (not a policy) level.	IdP
Authentic data sharing	Users can share authentic (i.e., signed) documents with other users or stakeholders, while still being able to redact predefined parts of those documents without invalidating the signature. This puts back users into control over which data they want to reveal to whom also in the data sharing scenario.	Data sharing
Maximal cloudification	A personal device holding secret cryptographic key material is only needed when initially granting rights to a new service provider or data receiver. All other actions can be done fully only without requiring physical access to a personal device.	IdP and data sharing
End-to-end confidentiality	The confidentiality of the user's data is guaranteed at any point in time. That is, the central CREDENTIAL Wallet is technically unable to learn the data stored in the Wallet, while the intended receiver in every interaction can do so.	IdP and data sharing
Metadata privacy	Any two actions taken by a user are unlinkable even by colluding service providers if not intended otherwise by the user. In its final maturity level, the user's actions could even be widely hidden from the Wallet. *	IdP
Platform independency	Even though only prototyped on Android systems, all developed libraries could also be ported to other operating systems and hardware settings. This way, a hardware vendor lock-in can be avoided.	IdP and data sharing
Personal data safe	The Wallet can be used as a highly secure personal data and identity safe because of its high security and privacy guarantees.	IdP and data sharing

Strong authentication	Due to strong 2FA methods (including, e.g., passwords, biometrics, secure devices, etc.), the risk of unauthorized access to the Wallet can be minimized.	IdP and data sharing
Interoperability	Interoperability with existing authentication schemes like OAuth, etc. simplifies the integration into existing IAM solutions.	IdP

* This metadata privacy might not actually be realized in CREDENTIAL, but it belongs to a discussion of adoption because as pointed out in section 6.1, to be incrementally deployable will increase the probability of success.

Technology adoption modeling has been in place for decades to help scientists and technologists understand the weaknesses and strengths of their product as viewed by the end users. Thus far, a number of approaches have been proposed to study the adoption of new technological products. Of these all, the Technology Acceptance Model (TAM) has gained more popularity within the information systems community.

TAM, as depicted in the figure below, was first proposed by F. D. Davis (1989) in his pioneering work in this domain. According to TAM, users' actual use of a given technology is influenced directly or indirectly by the user's behavioral intentions, attitude, perceived usefulness of the system, and its perceived ease of use (for schematic overview, see Figure 6-1). TAM was developed in further versions which elaborate what external factors affect intention and actual use through mediated effects on perceived usefulness and perceived ease of use.

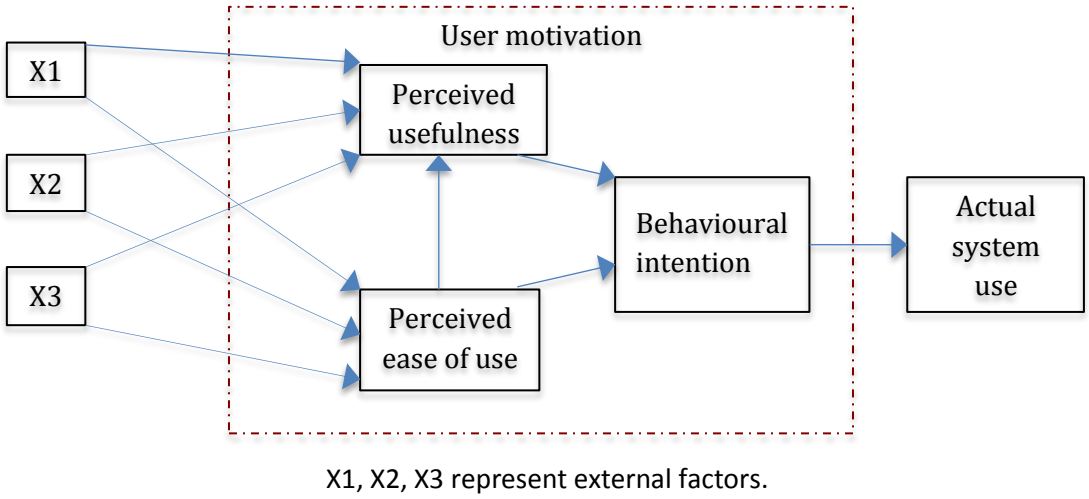


Figure 6-1: A simplified model showing main components of TAM

(originally proposed by Davis, 1989, extensions in Venkatesh and Davis, 2000, and Venkatesh and Bala, 2008).

TAM provides a basis with which one traces how external variables influence belief, attitude, and intention to use of a given technology. In a deliverable from the H2020 project PRISMACLOUD (Alaqra

et al, 2015, D2.1 section 6.2.2) examples from security and privacy critical contexts are collected where applications of these foundations or extensions thereof by new factors have been evaluated and tested (the examples come from eBanking, email authentication services, anonymous credentials, and information security technology). Given the privacy and trust factors inherent in the CREDENTIAL technology, one can imagine to develop an extended version which includes such constructs as trust, complexity, credential management, etc.

The CREDENTIAL Cloud Wallet has distinct features that may affect its adoption by end users in accordance with Rogers' concept of *relative advantage* but also *complexity* (section 6.1). We plan to map these features into the acceptance factors to explain how understood and "dis/liked" the technology in general might be. This does not directly relate to how companies and public authorities may adopt it, but it will help them to approximately predict people's intention to use.

Based on concepts from TAM, CREDENTIAL partner GUF has provisionally adapted some constructs and items for further consideration, as shown in Appendix H. By necessity, this will overlap with the SUS model (Brooke, 1996) used for the post-test questionnaires in the user test reported in section 4.2. In that test a set of questionnaires was given to the participants in combination with the tasks to be performed; by this design of the test, the number of questions had to be very limited. Therefore, the SUS set of only ten questions with a simple grading scale to each was used. In addition, SUS values for "acceptability" exist which made it easy to gauge user apprehension of the most essential parts of the UI Porotypes V1 already from this first test (cf. 4.2.2 and see Ruoti et al. 2015). For the same reasons, we have not yet used the more comprehensive set of questions suggested by the PET-USES (Wästlund et al., 2009; caveat to use it in "fast iterative design cycles" in section 4.2.5 of Graf et al., 2011).

Individual partners in the CREDENTIAL project have expressed specific ideas for adoption condition. Klughammer, active in the eHealth pilot, explains that clinics have to adopt first, then it easy to get patients to adopt, but the other way will not work. The argument comes from experience in telemedicine: people do not use telemedicine software when they are healthy or very sick. Rather, patients who are willing to use telemedicine are those who have a chronic disease. This is one reason why CREDENTIAL selected the Diabetes Use Case. For other reasons, see sec. 5.3 in D6.1 (Thiemer, 2016).

But even when there are patients with chronic diseases they need some kind of incentive to use telemedicine. These incentives have to be provided by somebody. That could be the practitioner, the clinic or the health insurance. Incentives can be of various kinds: less traveling = save time and money, better diagnosis, better treatment, or simply being reimbursed by the health insurance when taking part in such a project (cf. *sponsorship* in 6.1). For how this is reflected in the eHealth pilot use case, see 3.2.

6.3 Multi-Factor Authentication and Biometric 2FA

The most common way to authenticate to a device or a service provider is using a password. However, more and more devices and in particular more and more service providers offer two-factor authentication (or even multifactor authentication). Many two-factor authentication schemes assume that users enter a password on one device (most likely their desktop PC or laptop) and receive a code on a second device (e.g., mobile phone), a code which they are supposed to enter on the first device; i.e. their password is one factor and the fact that they have access to the mobile phone the second factor. Two factor-authentication

was introduced to increase the security as: (a) users have problems to deal with passwords and as a coping strategy tend to use insecure ones, but with 2FA in place, an attacker who is able to guess the password cannot take any actions without also having access to the second factor; and (b) in case of a corrupted first device, the damage a corresponding malware can cause is limited.

6.3.1 End-User's Perspectives Unknown

There are many possible factors and ways to combine factors for authentication. Depending on the factors and the combinations, the security and the usability may vary. The focus of this paragraph is on the human aspects. There are a number of papers studying human factors of two-factor authentication. We started searching for papers using the search terms ('usability' OR 'user study') AND 'two factor authentication'. We found so far around forty research papers. The most relevant ones are Krol et al. (2015), Bruun et al. (2014), De Cristofaro et al. (2013), Wier et al. (2010), Weir et al. (2009), Strouble et al. (2009), Kaviani et al. (2008), and Payne et al. (2016). In particular the last one provides insight into the factors that may prevent users from adopting a scheme based on so-called tangible tokens. It also introduces processes that might help people accepting a token-based authentication scheme.

While the findings of these papers should be considered it is also worth mentioning that there might be culture differences (see for instance our note on the results of the user test result where all participants came from a country where people are used to use a smart app to authenticate to various sensitive services). In addition, the acceptance of two-factor authentication is likely to depend on the purpose it should be used for (e.g., which data or actions are to be protected and how often the corresponding account is in use). Furthermore, what apparently has not been studied to judge from the results of this first search is what people believe a two-factor authentication is used for, why they should use it and when, that is, their mental models of authentication schemas based on two or more factors. These questions will be further elaborated on in the course of the project.

While searching for these papers, the consortium decided to evaluate people's apprehension of authentication approaches using fingerprinting as corresponding sensors are likely to be included in all future smartphones. Correspondingly, we considered literature studying human aspects of fingerprint-based authentication. It is important to understand peoples mental models on fingerprinting (or biometric authentication in general) to know what to consider when using it in an application such as CREDENTIAL. Relevant literature in this area includes:

- In Bhagavatula et al. (2015), the authors study the perceived security, acceptance and usability of iPhones and Android fingerprint authentication.
- In Dorflinger et al. (2010), the authors study the perceived security and usage intention of biometric authentication in the broader smartphone context.
- Similarly, Sieger and Möller (2012) study the perceived security and intention to use, biometric authentication in a smartphone context
- In Heckle et al. (2007), the authors study fingerprint authentication in general, i.e. the usability of different approaches

6.3.2 Service Provider Point of View

If we strictly consider the Service Provider's (SP) point of view, the authentication problem is limited to defining the authentication security level that is needed to perform access considering the service

accessed, because the Lombardian IdP, called IdPC (Identity Provider of the Citizen; D2.1, sec. 6.1), will provide the authentication service for the individual SP. The Italian regulation, in compliance with the EU EIDAS Regulation[1], defines three levels with respect to the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party.

The following table sets out the requirements per assurance level with respect to the authentication mechanism.

Table 6-2: Requirements per assurance level

Assurance level	Elements needed
Low	1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity. 2. Where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including analysis offline. 3. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with enhanced-basic attack potential can subvert the authentication mechanisms.
Substantial plus Level low	2. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication. 2. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms.
High plus Level substantial	The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms.

Source: Regulation (EU) 2015/1502, paragraph 2.3.1. Authentication mechanism.

Based on the EU Regulation and ISO-IEC 29115, AGID, Agenzia per l'Italia Digitale (the Agency for Digital Italy), has provided, in the framework of SPID regulation, that is, the regulation according to the "*Sistema Pubblico di Identità Digitale"* (the Public System for Digital Identity), some use cases to select the appropriate level of assurance to be applied to different types of regional services in Italy.

[1] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

The following table, which is a revised version of the one provided by AGID in the document "Levels of minimum service for homogeneous functionalities (09/06/2016)", gives an overview of the main types of regional services and examples of use of the minimum level of SPID credentials to be used. (The reader should note that the requirements concern only to the Italian context and do not apply at European level.)

Table 6-3: Assurance levels and types of regional services

Minimum assurance level	Main types of regional services
Anonymous access	A citizen makes a spontaneous payment
SPID level 1 (LoA2 of ISO-IEC 29115)	1. Customization Service 2. Civic consultations 3. Request of general information
SPID level 2 (LoA3 of ISO-IEC 29115)	1. Citizen access to the list of its debt positions 2. An intermediary person that accesses the list of debt positions by power of attorney 3. Presentation of a request on behalf of another person without sending sensitive data (it refers to online services, generally carried out by professionals, for communications that do not process sensitive data such as seismic communications, starting of a construction site, mandatory labour market communications) 4. Others…
SPID level 3 (LoA4 of ISO-IEC 29115)	1. Presentation of a request on behalf of another person with sensitive data transmission (for example application to ask for economic subsidy due to a disease) 2. Certificate of tax exemptions / facilitations of third parties tax-based or age-based 3. Request-declaration of exemptions / facilitations on behalf of third parties on a health basis 4. Others …

Source: *SPID* Communication n.4 "Levels of minimum service for homogeneous functionalities 09/06/2016".

If we consider the IdPC point of view, Lombardy Region has undertaken several actions to improve user experience.

- In 2006, the centralisation of authentication services in IdPC and the removal of this layer from SP, has led to a single user experience.
- The single user experience implies a constraint: Lombardy Region citizens were already using a smartcard device (*CRS "Regional Card of Services"*) so all Lombardy citizen have smartcard why introducing another kind of token was not an option. This solution was on SPID level 3.
- The smartcard was a barrier for a good user experience as the device was not widespread. Therefore, smartcard readers were disseminated through newsagent shops, public schools, local authorities, etc. Moreover, the software was also distributed both through a CD disc and online downloading, and a specific tutorial for software setup addressed to elderly people was released.
- The user interface exploits the native browser cryptographic mechanisms.

- The process undertaken by Lombardy Region was not completely successful due to users' troubles in setting up the smartcard reader and the software, considering the wide range of operating systems and software running on citizens' computers.
- As a result, Lombardy Region has considered not using local software or hardware devices for authentication process.
- To overcome the problem, a partnership was set up with what is currently AGID to define an authentication mechanism with the same security levels but more user friendly. This considered also that the digital scenario was significantly changed by the widespread use of smartphones and tablets, which do not tally well with a smartcard reader.
- The final solution identified, which foresees a one-time password system based on mobile phone SMS, is grounded on a paradigm "something you know and something you have":
    - What you known: card number and password
    - What you have: an SMS sent on a mobile device that was registered by the user when joining the service (face-to-face registration or registration by smartcard and pin).
- This new authentication mechanism, at SPID level 2, was mostly successful in terms of citizens accessibility, with more than 1 ML credentials issued from 2012-2016.
- Access numbers *per se* cannot be considered as a quality index of the user experience in this specific case because users had to access essential services. However, the users' increased access through one-time password, once available, means that, in case of choice, users prefer this authentication system (80% vs. 20%).

In conclusion, the IdP can gain a lot of acceptance as noted by the basic TAM model when perceived ease of use and perceived usefulness are clear to prospective users. The one-time password scheme is at SPID level 2 whilst a smart card scheme qualifies to SPID level 3. So far, the perceived usefulness of SPID level 3 does not seem to outweigh the perceived lack of ease of use, even if this conclusion is more of a conjecture, a guess, based on the usage pattern described in the last point above.

As far as concerns eGovernment service authentication, Italy is implementing SPID, a Public System of digital identity, aiming at federating identity and service providers. SPID is actually a national network, gathering identity and service providers, assuring that they conform to a set of given rules and standards. The ultimate goal of SPID is to give a "digital identity" to all Italian citizens. Currently, the following five IdP providers are accredited and active: TIM, Infocert, Poste, SIELTE and Aruba. Each IdP provider can make available its favourite user experience, but great attention is given to users real experience of different solutions. Among the above mentioned identity providers, only one offers a service with smart card, whilst the others currently do not but are planning to introduce also a solution based on smart card. They only make available systems based on user name + password or user name + password + one-time password (through app or SMS).

6.4 Authorization Frameworks

While the factors that drive the adoption of multifactor authentication are a balanced combination of user-focused (e.g. requires convenience) and service-provider-focused (e.g. the ROI of the security solution) parameters, the selection of the authorization scheme is more focused on the service provider side. Originally, the authorization protocol in most cases was transparent for the users and it was an imposition of the service provider. However, once users started to share/store their data online, the classical

enterprise-centric authorization schemes where authorization policies were solely controlled by super users responsible for system-wide authorization were no longer valid. CREDENTIAL is part of a development where users are to be empowered with full control over their data disclosures, deciding who can access, modify or delete it. Protocols such as OAuth[1] were born to provide users the ability to grant third parties access to these user-owned resources. While this model has proven effective and is widely spread, it makes users responsible for establishing their own policies across dozens of services forcing them to keep track of their data in a fragmented online world.

In order to solve this, alternative authorization models have been proposed since some time (e.g. ADAGE[2]) while none of them have truly gained traction. The main focus of these novel and innovative authorization protocols is to provide users with a user-centric authorization model. With this model, as opposite to enterprise-centric models, the user may connect different compatible resource providers, service providers or applications to a central authorization decision server, where the user has full control over the policies that will govern access to the resources / data they own. The user would now be able to establish policies that affect multiple service providers and to see, in one glance, who can access its data.

Kantara's UMA (User Managed Access) work group[3] has proposed the UMA core protocol as an extension of OAuth but providing an additional layer of user-centric perspective which is more aligned with privacy principles. UMA only specifies the protocols to be used to communicate all involved stakeholders (resource provider, request party and resource owner) but does not require any specific implementation of any of the related process (e.g. authorization could rely in standard XACML[4] implementations or it could require biometric authentication).

UMA is built upon a privacy model that is based on four main considerations: **Context, Control, Choice and Respect** which are fully aligned with the GDPR data protection principles and moreover, with its ethical roots.

However, the actual status of UMA's adoption is the classic vicious circle. Even if the technology is mature enough and many providers include them in their offering (e.g. GLUU[5] and OpenAM[6]) and users would benefit from the novel role of *authorization service providers* springing from UMA's approach, the following interrelated factors hinder a more wide-spread adoption:

- Users are not aware of the benefits of this technology and will not pressure service providers for them to provide it.
- Service providers have no particular interest on moving from OAuth to UMA scheme as it does not add significant value to their services.

[1] https://oauth.net/
[2] https://pdfs.semanticscholar.org/017f/f1fb55c09f783a30b8a21402adbf8303a207.pdf
[3] https://kantarainitiative.org/confluence/display/uma/Home
[4] http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html
[5] https://www.gluu.org/
[6] https://forgerock.org/openam/

- No stakeholder will be willing to provide UMA Authorization services until there is a number of service providers large enough that would make it worth or exploitable.

Hence, the adoption of UMA as a de-facto standard will be bound to several circumstances:

- The creation or envisage of business models that will make authorization servers sustainable.
- Find incentives for service providers' adoption (OAuth was adopted because its convenience for both, service providers and users). In UMA, incentives for service providers, besides supporting their users demands, are not clear.
- Convenience and User Experience: while the protocol allows novel business models and provides users with a higher degree of control, the convenience of the particular implementations will be key. Possibly, novel user interfaces will be required to hide the complexity and power of policies (e.g. XACML policies) to users without constraining the underlying features

6.5 Privacy Related Awareness Challenges for ID Providers

Existing solutions for authentications are very much used and presumably liked by many users. Facebook, Google and others provide people with an easy way to authenticate (the corresponding buttons to use this option are often called social login buttons); easy because they neither need to set and later on remember a (new) password nor do they need to manually provide personal information such as name, birthday or credit card information. However, these solutions suffer from three types of privacy problems: Two by design because the identity provider can also read all the information that the user stores as they are not encrypted in a way that only the user can access them but also the identity provider[1]. Second, the identity provider knows of all the service providers the user have accounts with, and moreover also knows when and how often the user signs in to these accounts. The third privacy problem is by implementation: by default it is difficult to notice and to modify which information is shared between the identity provider and the service provider – one should observe that sharing also includes that the service provider may have the right to ask later on again for this information.

The CREDENTIAL Wallet has an advantage from a privacy point of view as the data is encrypted and only the meta data is really “known” by the Wallet (that is, by the Wallet provider, whoever that may be).

The question then is to what extent will people understand and appreciate the benefits offered by solutions like the CREDENTIAL Wallet. Furthermore, if there is a general lack of understanding among users of different login solutions, and a lack of appreciation of identity providers, what can be done to promote understanding and appreciation of the privacy friendly solutions developed within this project?

Existing identity provider, single sign on solutions, and social login buttons have been part of various human-centred research. In order to learn from previous research for credential, we conducted a literature

[1] Note, the first problem exists because Facebook and Google are mainly social networks and only later they started offering the functionality to be used as identity provider. While the social network companies are interested in user data as their business model, the business model of a service only acting as identity provider might be a different one.

study to find out users' problems and perceptions towards single sign on systems and identity providers. We started by the much-cited paper by Dhamija and Dusseault, "The seven flaws of identity management: Usability and security challenges" (2008), and then searched for papers referring this and basing their research on usability studies of how users' problem when using identity providers. Further papers where found be researching papers citing these papers, etc. Not to miss any related work, we also searched for "usability study" + "single sing on", "usability study" + "identity provider", "user study" + "identity provider", and user study"+" single sign on" , "social login button" + "user study" and "social login button" + "usability study" in ACM, Springer and IEEE databases. Filtering manually by reading abstracts, we eventually downloaded 33 papers, including some already identified. Some other papers did not involve any user study but rather new algorithms.

Altogether 19 papers were then left for an in-depth analysis of what different researchers have found regarding users' problems related to single sign on systems. We have categorized the problems and perceptions in five groups as seen in the left column of Table 6-4. Although some problems are the results of the others, we categorized them separately for the sake of clarity. For example, some mental model problems and problems related to consent form are related to not observing the usability in designing of user interfaces. Table 6-4 summarises the problems and perceptions encountered in the literature survey (article in preparation will discuss the individual studies reviewed).

Table 6-4: Summary of problems and perceptions

Category	Perceptions / problems reported
Usability Issues	• Lack of reassurance design elements • Unclear sequences and no call-to-action • Not enough information for returning users
Users' Concerns	• Security • Privacy • Trust • Control and Transparency
Mental Models Problems	• Breaking users' mental models • Incorrect security mental models • Implicit login to IdP and lack of single sign-off mechanism • Account linking misconceptions
Consent Form Problems	• Opaque, uninformative, ineffective • Habituation makes users not noticing consent forms • Perception that forms are static; preconceptions about content
Lack of Knowledge	• About data flows between entities • About the level of access service providers receive • About audit tools on IdP side • Lack of benefits of using single-sign-on benefits

Based on these findings the project is developing a tutorial to explain the general concept of using social networks as identify providers including the advantages and disadvantages compared to manually signing in to a new service provider. The goal is to enable with the tutorial more informed decisions regarding

whether to use social networks as identity providers or not. The tutorial needs to be adopted because the CREDENTIAL Wallet has an advantage from a privacy point of view as the data is encrypted and only the metadata is really "known" by the Wallet (that is, by the Wallet provider, whoever that may be).

A looming question is what kind of trade-off prospective end-users will make. Facebook users pay with data, but what do CREDENTIAL Wallet users pay? To what extent will people understand and appreciate the benefits offered by solutions like the CREDENTIAL Wallet?

6.6 Risk Communication

People's privacy attitudes often differ from the decision people make in the privacy context, i.e. when asking people how important privacy for them, most people acknowledge that it is very important; however they still use social networks intensively and do not use any privacy protecting tools such as TOR. This inconsistency is called 'privacy paradox' (Dienlin and Trepte, 2015). Many work researches this issue, mostly in the context of online privacy, e.g., from Trepte and her group (2011). An overview is provided by Kokolakis (2017). One possible explanation for those observations (referred to as privacy paradox) is provided by the so called privacy calculus theory. The privacy calculus theory states that people seek a balance between potential risks and benefits, e.g. in e-commerce from Dinev et al. (2006), in online market places from Kim et al. (2016) or from Lankton et al. (2011) in social networks. Note, while this is a valid approach for decision making, the problem is that potential risks are often not known or very abstract, e.g. what does it mean that service providers or identity providers or even the CREDENTIAL Wallet is collecting and analyzing data to profile us? This is different to the security context where risk such as financial losses are more concrete and better understood (and as such also considered) by people during decision making – see e.g. Bødker et al. (2012).

Correspondingly there are the following challenges for CREDENTIAL: 1) Communicating the trust model (also called security model) of CREDENTIAL (in comparison to other ID providers) in a way that users see the need for approaches like CREDENTIAL (as they are aware of the risks without); 2) Increasing general awareness of privacy risks w.r.t to data disclosure to service providers to increase the likelihood that people consider not disclosing all the information the service provider is asking for; 3) Communicating potential risks for individual items to be shared with a service provider in order to support informed decision making.

We already started researching this area. Different awareness-raising messages were developed and tested in an online survey (results to be published). It turned out that it is important to explain that the collected personal data can also be misused either by the service provider or by criminals hacking into the service provider's data base. We expected that describing concrete threats and consequences will further increase the perception of risk and thus the likelihood to take privacy protecting actions. However, it turned out that such messages are very difficult to design as each individual concrete consequence is not very likely and also perceived as such by many participants in the online survey.

6.7 Lessons for UI Prototypes V1 and Beyond

Far from giving a clear direction for the dissemination of the CREDENTIAL technology, the literature reviews above have shown the many intricacies involved. The various concerns and research reported above has nevertheless informed the first round of prototypes for CREDENTIAL.

So far, the mental models that various researchers have been investigating concerning users' understanding and acceptance of fingerprint authentications, have only concerned authentication towards the device and not for consenting to data disclosure (6.3.1). Our user test sheds some lights on this question but more can be done on the apparent confusion of what goes with the data disclosure (section 4.2.4).

The literature study on awareness challenges had an impact in particular regarding informed decisions when the user is about to disclose personal information (especially the consent form problems listed in Table 6-4 and also the second and third points of the ignorance category we tried to counter in the design found in 4.1.3). Some of the results from the user test of the draft V1 UIs show that the drafted UIs would not be able to rid the CREDENTIAL Wallet from all the problems found in usability investigations of other solutions. The presented "final" version in section 4.1 of the UI Prototypes V1 will also be subject to evaluation as will parallel developments of slightly different solutions for the interaction design.

In addition, and as several of the subsection above mention, there are new aspects to what our project brings to public. These aspects will be investigated more deeply now when the UI Prototypes V1 have been delivered. A scientific approach to the question about how to introduce people to the benefits of the CREDENTIAL Wallet will have to be broader than merely evaluating the UI design proper; it has to include also other means of introductory efforts; the tutorial mentioned in the end of 6.5 is one example.

However, in order to accommodate the adoption dependencies for eHealth applications mentioned in 6.2, specific eHealth applications apps have been envisioned within the CREDENTIAL project which motivated the second set of UI prototypes (section 5). Thus, the instruments to measure user adoption willingness would need to be developed in more than one direction (cf. envisioned questions to employees/doctors and to voluntary users/patients in Appendix H).

Furthermore, the assemblage of theoretical approaches brought forth above will be used to develop the instruments for user analysis be it surveys or post-test questionnaires after usability tests. A brief discussion of this was given in section 6.2. Further departure points can be found in previous EU projects, especially the PrimeLife Deliverable D4.1.6, "Towards Usable Privacy-Enhancing Technologies: Lessons Learned from the PrimeLife Project" (Graf et al. 2011).

7 Conclusion and Outlook

This document describes the user interfaces version 1, i.e. “UI Prototypes V1”, and underlying task analyses. The UIs elaborated here consists of two sets: one designated “general UIs” that will appear in the general CREDENTIAL Wallet applicable in all three project pilots on eGovernment, eHealth and eBusiness; a second set of UIs consist of the eHealth-specific UIs that need to be drafted, and later refined, for the two “Wallets” planned for the eHealth pilot’s use cases – one for the Patient and for the Doctor (healthcare practitioner).

These sets of UI Prototypes V1 are necessary for the implementation that now starts in the CREDENTIAL project. They are also useful for elaborations of specific details of the interaction design and, as further evaluation results may indicate, for refinements of the specification of some of the functionality.

In the first user evaluation of the general UIs we found, in line with other studies, that people are not paying sufficiently attention to details of data releases and settings for disclosure policies. However, the participants in the conducted user test showed a desire to have control over their data and wanted to select the mandatory information manually. A design that makes people more actively regard and select the data to be disclosed may make them reflect more. There are many alternative interaction designs to consider here. Also, user evaluation should be wanted of file-based authorization requests and potential solutions to guide people to select the proper files from their Wallet like the file tag system discussed presently within the project.

The eHealth-specific UIs have not been subjected to any kind of formal user testing yet as they will be evaluated within the pilot development cycle. Nevertheless, the development process of these mockup UIs brought the project to, and through, crucial decision points. According to the projects plans, all three pilot prototypes including the eHealth with its two tailor-made apps for Patient and Doctor, respectively, are going to be developed with evaluation phases.

The ongoing research strands described in the section on research challenges will produce results on various levels. It can be noted that even an approach based on high-level frameworks such as Diffusion of Innovation or Technology Acceptance Model, may yield very concrete and detailed results if not on exact design details of UIs and introduction texts/videos but on the design of user studies including the questionnaires and interview guides that accompany such studies. Evaluation is needed of how the technology is introduced and explained in various contexts. Participants in our study and in other studies have been worried about the security and thereby also about their privacy because they could not really figure out how it worked. Moreover, there are worries concerning the single point of failure, that if the one and only IdP goes down the user is left without options.

The user-related KPIs (Key Performance Indicators) of the CREDENTIAL “Pilot Use Case Specification” (D6.1, Thiemer, ed., 2016) will be developed and tried in future evaluations of refined general UIs, and feedback to the developers of the pilots will be provided on methods and scales for usability evaluation.

Finally, the next deliverable devoted specifically to CREDENTIAL user interfaces, D3.2 “UI Prototypes V2 and HCI Patterns”, will beside the version 2 of the UIs also include a guide for user interface design for secure data-sharing technologies. This will break out details from UIs used in the use cases to highlight

particular solutions but also generalise because “a pattern is a structured description of an invariant solutions to a recurrent problem in context” (Dearden and Finlay, 2006, p. 58-59). Previous attempts within the sphere of Privacy-Enhancing Technology (Fischer-Hübner et al. 2010, Graf et al. 2011) show that there can be several ways of structuring such solutions and evaluation methods, and that also patterns of mistaken mental models are good to map in order to guide future designers and others who will influence the dissemination of this type of technology.

References

Alaqra, A., Fischer-Hübner, S., Pettersson, J.S. (2015). Legal, Social, and HCI Requirements. Report D2.1, PRISMACLOUD. www.prismacloud.eu

Arianezhad, Majid, L. Jean Camp, Timothy Kelley, and Douglas Stebila (2013). Comparative eye tracking of experts and novices in web single sign-on, Third ACM Conference on Data and Application Security and Privacy (CODASPY) 2013 (San Antonio, Texas), ACM Digital Library, 2013, pp. 105–116.

Art. 29 Data Protection Working Party (2004) Opinion 10/2004 on More Harmonised Information Provisions. (November 25th, 2004). 11987/04/EN WP 100. European Commission.

Bangor, A., Kortum, P., Miller, J. (2009). Determining what individual SUS scores mean: adding an adjective rating scale. *Journal of usability studies*, 4(3), 114-123.

Bauer, Lujo, Cristian Bravo-Lillo, Elli Fragkaki, and William Melicher (2013). A comparison of users' perceptions of and willingness to use Google, Facebook, and Google+ single-sign-on functionality, Proceedings of the 2013 ACM Workshop on Digital Identity Management (New York, NY, USA), DIM '13, ACM, 2013, pp. 25–36.

Benenson, Z., Girard, A., Krontiris, I. (2015). User acceptance factors for anonymous credentials: an empirical investigation. In Workshop on the Economics of Information Security (WEIS).

Besmer, Andrew, Heather Richter Lipford, Mohamed Shehab, and Gorrell Cheek (2009). Social applications: Exploring a more secure framework, Proceedings of the 5th Symposium on Usable Privacy and Security (New York, NY, USA), SOUPS '09, ACM, pp. 2:1–2:10.

Bhagavatula, Ch., Ur, B., Kywe, S.M., Cranor, L.F., Savvides, M. (2015) Biometric Authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption. USEC '15, 8 February 2015, San Diego. Internet Society.

Bødker, Susanne, Niels Mathiasen, and Marianne Graves Petersen. (2012). Modeling is not the answer! Designing for usable security. *Interactions* 19(5), 54-57.

Bonneau, J., Herley, C., Van Oorschot, P. C., Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy*(pp. 553-567). IEEE.

Braun, V., Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3 (2), 77-101.

Brooke, J. (1996). SUS: A "quick and dirty" usability scale. In: Jordan, P. W., Thomas, B., Weerdmeester, B. A., McClelland (eds.) *Usability Evaluation in Industry* pp. 189-- 194. Taylor & Francis, London, UK.

Brostoff, S., Jennett, C., Malheiros, M., Sasse, M. A. (2013). Federated identity to access e-government services: Are citizens ready for this? In *Proceedings of the 2013 ACM workshop on Digital identity management* DIM'13 (pp. 97-108). ACM.

Bruun, A., Jensen, K., Kristensen, D. (2014). Usability of Single-and Multi-factor Authentication Methods on Tabletops: A Comparative Study. In *Human-Centered Software Engineering*, 299-306. Springer.

Carter, L., Bélanger, F. (2005). The utilization of e- government services: citizen trust, innovation and acceptance factors. *Information systems journal*,*15*(1), 5-25.

Chandrasekaran, B. (1990). Design Problem Solving: A Task Analysis. *AI Magazine*, 11(4), 59-71.

Chen, H., Nicogossian, A., Olsson, S., Rafiq, A., Stachura, M. E., Watanabe, M.. Xiao, Y. (2009). Electronic health. *International journal of telemedicine and applications*, *2009*.

Chuttur M.Y. (2009). "Overview of the Technology Acceptance Model: Origins, Developments and Future Directions," Indiana University, USA. Sprouts: Working Papers on Information Systems, 9(37). http://sprouts.aisnet.org/9-37

Conzola, V.C., Wogalter, M.S. (2001). A Communication—Human Information Processing (C-HIP) approach to warning effectiveness in the workplace. *Journal of Risk Research* 4 (4), 309-322.

Credential. (2015). *Credential*. [Online] Available at: https://credential.eu/ [2016-08-04].

Crystal, A., Ellington, B. (2004). Task analysis and human-computer interaction: approaches, techniques, and levels of analysis. *AMCIS 2004 Proceedings*. New York, NY.

Davis, F. D. 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Qutarterly*. 13 (3), 319-339.

De Cristofaro, E., Du, H., Freudiger, J., Norcie, G. (2013) A comparative usability study of two-factor authentication. arXiv:1309.5344.

Dhamija, R., Dusseault, L. (2008). The seven flaws of identity management: Usability and security challenges, *IEEE Security and Privacy* 6 (2), 24–29.

Diaper, D. (2004). Understanding task analysis for human-computer interaction. In *The handbook of task analysis for human-computer interaction* (pp. 5-47). Mahwah, New Jersey: Lawrence Erlbaum Associates.

Diaper, D., Stanton, N. A. (2004). *The Handbook of Task Analysis for Human-Computer Interaction*. Mahwah, New Jersey: Lawrence Erlbaum Associates.

Dienlin, T., Trepte, S. (2015). Is the privacy paradox a relic of the past? an in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology* 45(3), 285-297.

Dinev, T., Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information System Research* 17(1), 61-80, http://dx:doi:org/10:1287/isre:1060:0080

Dorflinger, T., Voth, A., Kramer, J., Fromm, R. (2010) “My smartphone is a safe!” The user’s point of view regarding novel authentication methods and gradual security levels on smartphones. 2010 International Conference on Security and Cryptography (SECRYPT), pp. 1 – 10. IEEE.

Egelman, S. (2013). My profile is my password, verify me!: the privacy/convenience tradeoff of Facebook Connect, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (New York, NY, USA), CHI '13, ACM, pp. 2369–2378.

Fischer-Hübner, S., Köffel, Ch., Pettersson, J.S., Wolkerstorfer, P., Graf, C., Holtz, L.E., König, U., Hedbom, H. KEllermann, B. (2010). HCI Pattern Collection – Version 2. Deliverable D4.1.3, PrimeLife project, www.primelife.ee

Freeman, Beverly (2008). Yahoo! openid: one key, many doors. Available at http://developer.yahoo.com/openid/openid-research-jul08.pdf.

Graf, C., Hochleitner, Ch., Wolkerstorfer, P., Angulo, J., Fischer-Hübner, S., Wästlund, E. (2011) Towards Usable Privacy Enhancing Technologies: Lessons Learned from the PrimeLife Project. Deliverable D4.1.6, PrimeLife project. www.primelife.eu

Hackos, J. T., Redish, J. C. (1998). *User and Task Analysis for Interface Design*. New York, NY, USA: John Wiley & Sons, Inc.

Harbach, M., Hettig, M., Weber, S., Smith, M. (2014). Using personal examples to improve risk communication for security & privacy decisions. CHI'14. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Pp. 2647-2656.

Heckle, R.R., Patrick, A.S., Ozok, A. (2007) Perception and acceptance of fingerprint biometric technology. SOUPS '07, pp. 153-154.

Hörandner, F., Krenn, S., Migliavacca, A., Thiemer, F., Zwattendorfer. (to appear) CREDENTIAL: A Framework for Privacy-Preserving Cloud-Based Data Sharing. In *Availability, Reliability and Trust – SECPID@TRUST 2016*.

Hovav, A., R. Patnayakuni, D. Schuff, (2004) "A model of Internet Standards Adoption: the Case of IPv6", *Information Systems Journal*, 14(3), 265–294.

Hudson, W. (2003). Metaphor in user interface design: A View from the trenches. In *HCI workshop.* Available at: http://www.syntagm.co.uk/design/articles/muid01.pdf [2016-10-31].

International Standard Organization [ISO] (2010). ISO 9241-210 Human-Centred Design.

International Standard Organization [ISO] (2013). ISO-IEC 29115:2013 Information technology – Security techniques – Entity authentication assurance framework.

Javed, Y., Shehab, M. (2016). Investigating the Animation of Application Permission Dialogs: A Case Study of Facebook. In: Livraga G., Torra V., Aldini A., Martinelli F., Suri N. (eds) *Data Privacy Management and Security Assurance. DPM 2016. Lecture Notes in Computer Science, vol* 9963., pp. 146-162. Springer, Cham.

Johnston, J., Eloff, J. H., Labuschagne, L. (2003). Security and human computer interfaces. *Computers & Security*, *22*(8), 675-684.

Jøsang, A., Pope, S. (2005). User centric identity management. In *AusCERT Asia Pacific Information Technology Security Conference* (p. 77).

Joseph, D., N. Shetty, J. Chuang, I. Stoica, (2007) "Modeling the Adoption of New Network Architectures", International Conference on Emerging Networking Experiments and Technologies, CoNEXT '07 Proceedings of the 2007 ACM CoNEXT conference, Article No. 5, ACM New York, ISBN: 978-1-59593-770-4.

Karat, C. M., Brodie, C., Karat, J. (2006). Usable privacy and security for personal information management. *Communications of the ACM*, *49*(1), 56-57.

Karegar, F., Pulls, T., Fischer-Huebner, S. (2016). Visualizing Exports of Personal Data by excercising the right of data portability in the Data Track- Are people ready for this? To be appear in : Privacy and Identity Management – Facing up to next steps. Springer.

Katz, M., C. Shapiro, (1986). Technology Adoption in the Presence of Network Externalities, *Journal of Political Economics*, 94, 822–84.

Kaviani, N., Hawkey, K., Beznosov, K. (2008) A Two-factor Authentication Mechanism Using Mobile Phones. Technical report LERSSE-TR-2008-03. Laboratory for Education and Research in Secure Systems Engineering, University of British Columbia.

Kieras, D. E. (2004). GOMS model for task analysis. In *The handbook of task analysis for human computer interaction*, eds. Diaper and Stanton (pp. 83-116). Mahwah, New Jersey: Lawrence Erlbaum Associates.

Kim, G., Koo, H. (2016). The causal relationship between risk and trust in the online marketplace. *Computers and Human Behaviour* 55(PB), 1020-1029, http://dx:doi:org/10:1016/j:chb:2015:11:005

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour. *Computers & Security.* 64, C, 122-134. DOI: https://doi.org/10.1016/j.cose.2015.07.002

Krol, K., Philippou, E., De Cristofaro, E., Sasse, M.A. (2015) "They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking. arXiv:1501.04434.

Lankton, N.K., McKnight, D.H. (2011). What does it mean to trust Facebook?: Examining technology and interpersonal trust beliefs. *SIGMIS Database : the DATABASE for Advances in Information Systems* 42(2), 32-54, http://doi:acm:org/10:1145/1989098:1989101

Li, M., Gregor, S. (2011). Outcomes of effective explanations: Empowering citizens through online advice. *Decision support systems*, *52*(1), 119-132.

Linden, M., Inka V. (2005) An empirical study on the usability of logout in a single sign-on system, pp. 243–254, Springer Berlin Heidelberg, Berlin, Heidelberg.

Moey, L. K., N. Katuk, M. H. Omar (2016), Social login privacy alert: Does it improve privacy awareness of facebook users?, 2016 IEEE Symposium on Computer Applications Industrial Electronics (ISCAIE), pp. 95–100.

Morrison, A., McMillan, D., Chalmers, M. (2014). Improving consent in large scale mobile HCI through personalised representations of data. In *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational* (pp. 471-480). ACM.

Onwuegbuzie, A. J., Leech, N. L. (2007). Validity and Qualitative Research: An Oxymoron? Quality & Quantity, 233--249.

Patrick, A. S., Kenny,S. (2003) *From privacy legislation to interface design: Implementing information privacy in human-computer interactions.* International Workshop on Privacy Enhancing Technologies. Springer Berlin Heidelberg.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International journal of electronic commerce*, 7(3), 101-134.

Payne, J., Jenkinson, G., Stajano, F., Sasse, M.A., Spencer, M. (2016) Responsibility and Tangible Security: towards a Theory of User Acceptance of Security Tokens. USEC '16, 21 February 2016, San Diego. Internet Society.

Preece, J., Rogers, Y., Sharp, H. (2002). *Interaction Design*. New York, NY, USA: John Wiley & Sons.

Redish, J. C., Wixon, D. (2003). Task Analysis. In *Handbook of Human-Computer Interaction ,1st edition* (pp. Chapter 48, 923-940). Mahwah, New Jersey: Lawrence Erlbaum Associates.

Richardson, J., Ormerod, T. C., Shepherd, A. (1998). The role of task analysis in capturing requirements for interface design. *Interacting with computers*, *9*(4), 367-384.

Robinson, N., Bonneau, J. (2014) Cognitive disconnect: understanding Facebook Connect login permissions. COSN (Alessandra Sala, Ashish Goel, and Krishna P. Gummadi, eds.), ACM, pp. 247–258.

Rogers, E. (1962/2003). *Diffusion of Innovations*, 5th Edition. Simon and Schuster.

Ronen, S. (2013). Taking data exposure into account: How does it affect the choice of sign-in accounts? Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '13. New York, NY, USA.

Ronen, S., Riva, O., Johnson, M., and Thompson, D. (2013) Taking data exposure into account: How does it affect the choice of sign-in accounts?, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (New York, NY, USA), CHI '13, ACM, pp. 3423–3426.

Rubin, J., Chisnell, D. (2008). Handbook of usability testing: how to plan, design and conduct effective tests. John Wiley & Sons.

Ruoti, S., Seamons, K. (2016). Standard Metrics and Scenarios for Usable Authentication. Presentation at *2nd Workshop on "Who Are You?! Adventures in Authentication" (WAY 2016)* at the *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, June 22–24, 2016 Denver, Colorado. https://www.usenix.org/conference/soups2016/workshop-program/way2016/presentation/ruoti_metrics

Ruoti, S., Roberts, B. Seamons, K. (2015) Authentication melee: A usability analysis of seven web authentication systems, Proceedings of the 24th International Conference on World Wide Web (Republic and Canton of Geneva, Switzerland), WWW '15, International World Wide Web Conferences Steering Committee, pp. 916–926.

Sharma, A., Misra, P. K., Misra, P. (2014). A Security Measure for Electronic Business Applications. *International Journal of Computer Applications*, *102*(7).

Sieger, H., Möller, S. (2012) Gender differences in the perception of security of mobile phones. MobileHCI '12. Proceedings of the 14th international conference on Human-computer interaction with mobile devices and services companion, pp. 107-112. ACM.

Strouble, D.D., Schechtman, G.M, Alsop, A.S. (2009) Productivity and usability effects of using a two-factor security system. *Proceedings of SAIS*, pp. 196-201.

Sun, S.-T., Pospisil, E., Muslukhov, I., Dindar, N., Hawkey, K., Beznosov, K. (2011) What makes users refuse web single sign-on?: An empirical investigation of openid, Proceedings of the Seventh Symposium on Usable Privacy and Security (New York, NY, USA), SOUPS '11, ACM, pp. 4:1–4:20.

Sun, S.-T., Pospisil, E., Muslukhov, I., Dindar, N., Hawkey, K., Beznosov, K. (2013). Investigating users' perspectives of web single sign-on: Conceptual gaps and acceptance model, *ACM Transactions on Internet Technologies*, 13 (1), 2:1–2:35.

Suoranta, S., Manzoor, K., Tontti, A., Ruuskanen, J., Aura, T. (2014). Logout in single sign-on systems: Problems and solutions, *Journal of Information Security and Applications*, 19 (1), 61–77.

Thaler, D., Aboba, B. (2008) "What Makes for a Successful Protocol?", RFC 5218.

Thiemer, F. (ed., 2016) Pilot Use Case Specification. Deliverable D6.1, CREDENTIAL project. www.credential.eu

Thompson, R.L., Higgins, Ch.A., and Howell, J.A. (1991). Personal computing: toward a conceptual model of utilization. *MIS Quarterly* 15 (1), 125-143.

Trepte, S., Reinecke, L (eds.) (2011). *Privacy online: Perspectives on privacy and self-disclosure in the social web.* Springer.

Venkatesh, V., Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision sciences*, 39 (2), 273-315

Venkatesh, V., Davis, F. D. (2000). A theoretical extension of the technology acceptance model: four longitudinal field studies. *Management science*, 46 (2), 186-204.

Venkatesh, V., Morris, M.G., Davis, G.B., Davis, F.D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly* 27 (3), 425-478.

Wang, N., Grossklags, J., Xu, H. (2013). An online experiment of privacy authorization dialogues for social applications. Proceedings of the 2013 Conference on Computer Supported Cooperative Work, CSCW '13 (pp. 261–272). New York, NY, USA: ACM.

Wang, N., Xu, H., and Grossklags, J. (2011). Third-party apps on facebook: Privacy and the illusion of control, Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology (New York, NY, USA), CHIMIT '11, ACM, pp. 4:1–4:10.

Wang, N., Grossklags, J. and. Xu, H. (2013). An online experiment of privacy authorization dialogues for social applications, Proceedings of the 2013 Conference on Computer Supported Cooperative Work (New York, NY, USA), CSCW '13, ACM, pp. 261–272.

Wang, N., Wisniewski, P., Xu, H., and Grossklags, J. (2014). Designing the default privacy settings for facebook applications, Proceedings of the Companion Publication of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing (New York, NY, USA), CSCW Companion '14, ACM, pp. 249–252.

Wästlund, E., Wolkerstorfer, P., Köffel, C. (2009, September). PET-USES: privacy-enhancing technology–users' self-estimation scale. In *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life* (pp. 266-274). Springer Berlin Heidelberg.

Weir, C.S., Douglas, G., Carruthers, M., Mervyn. J. (2009). User perceptions of security, convenience and usability for ebanking authentication tokens. *Computers & Security* 28 (1), 47-62.

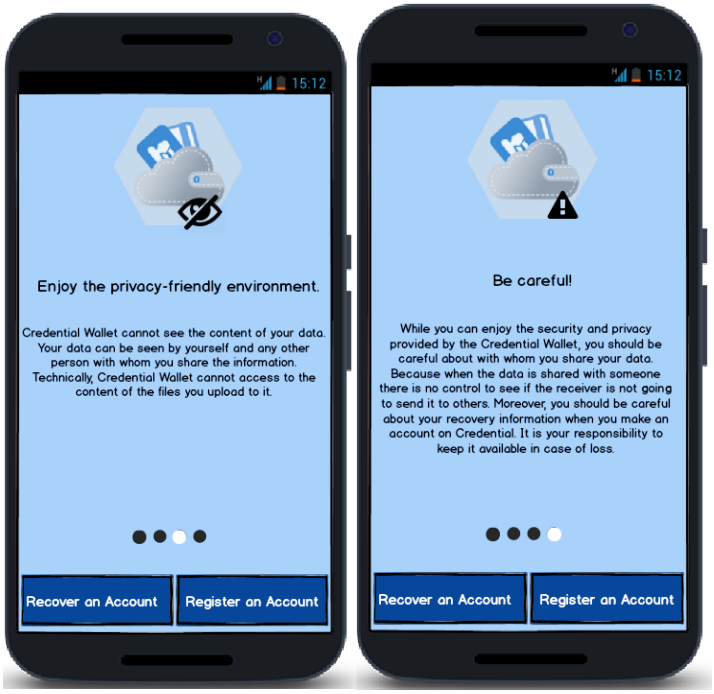
Weir, C.S., Douglas, G., Richardson, T., Mervyn, J. (2010) Usable Security: User Preferences for Authentication Methods in eBanking and the Effects of Experience. *Interacting with Computers* 22 (3), 153-164.

Xu, H., Wang, N., Grossklags, J. (2012) Privacy by redesign: Alleviating privacy concerns for third-party apps. International Conference on Information Systems (ICIS 2012).

Zhu, K., Weyant, J. (2003) Strategic Decisions of New Technology Adoption under Asymmetric Information: A Game-Theoretic Model, *Journal of Decision Sciences Institute*, vol. 34(4), 643–675.

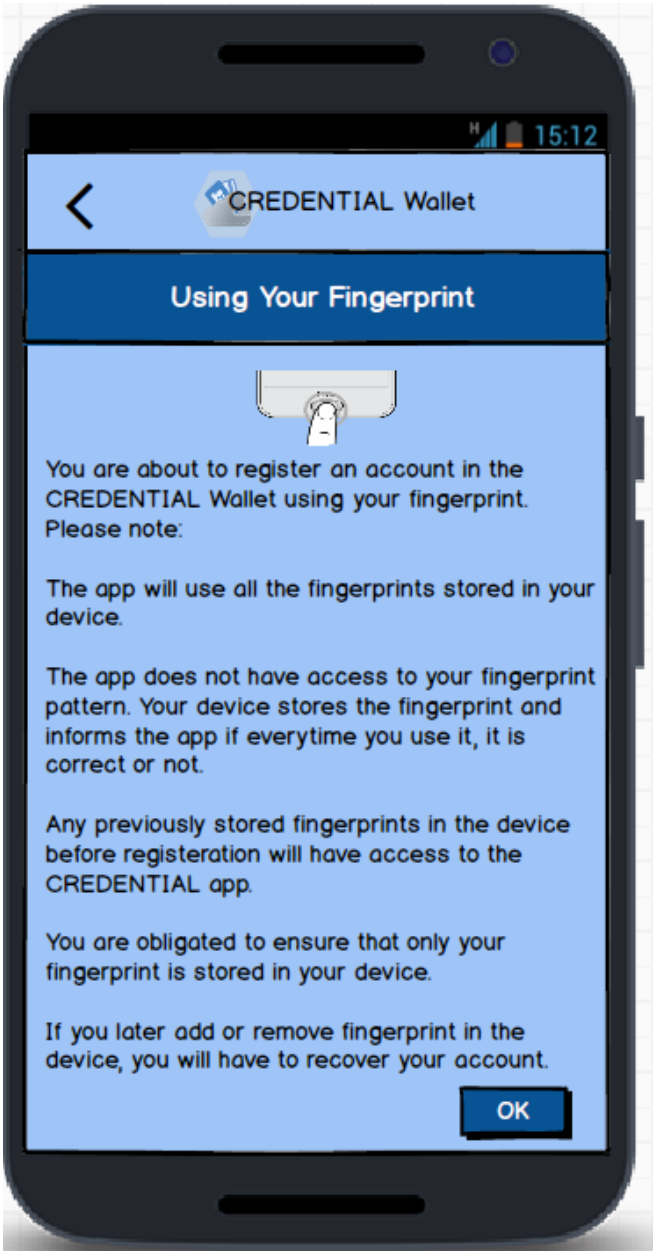
Appendix A. Introduction Screens

For the first time, when Elsa installs the app (or after removing the app and installing again on a device) an introduction is provided to give a general view of CREDENTIAL features. Elsa can swipe the screen to see each of the features one by one or they can easily skip it by using the buttons for recovering and registering an account.



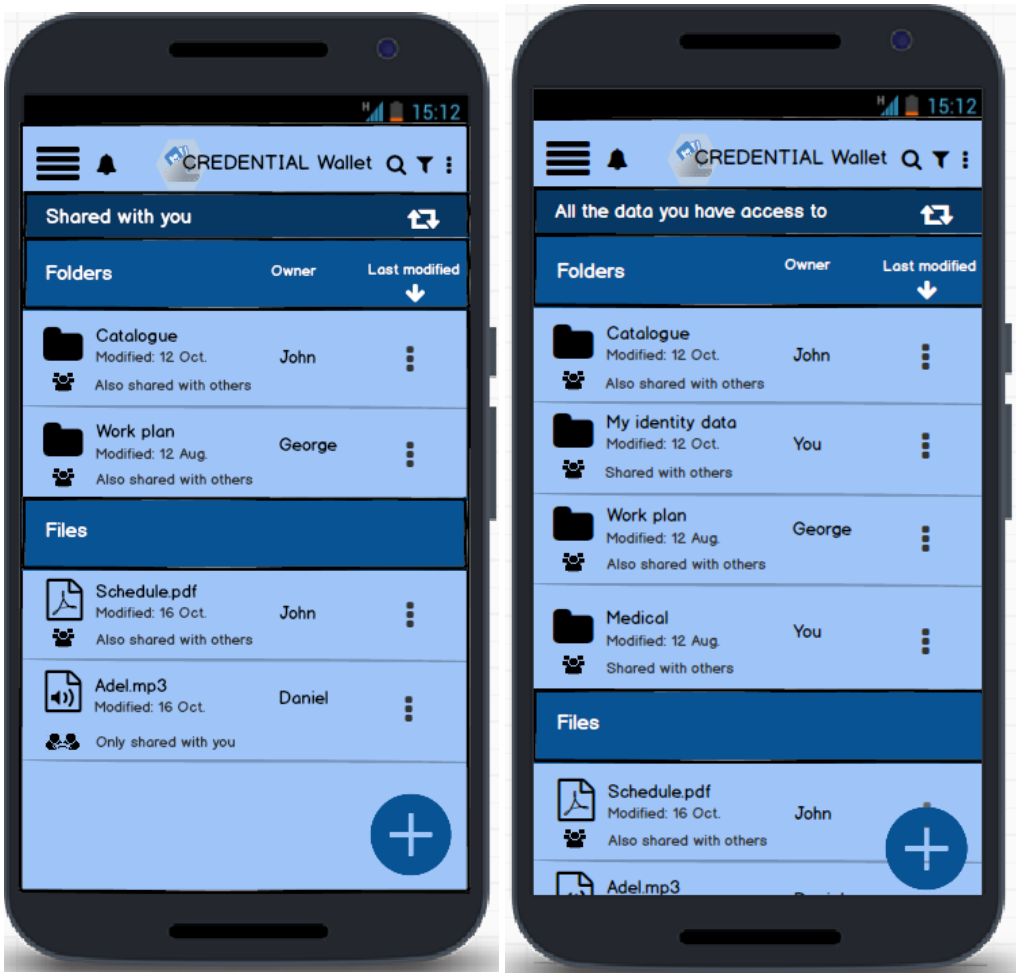
Appendix B. More Information about Using the Fingerprint

When Elsa is requested to scan their fingerprint registering their accounts, she has an option to read more about fingerprint usage in the app which is achieved by easily clicking on a related link.



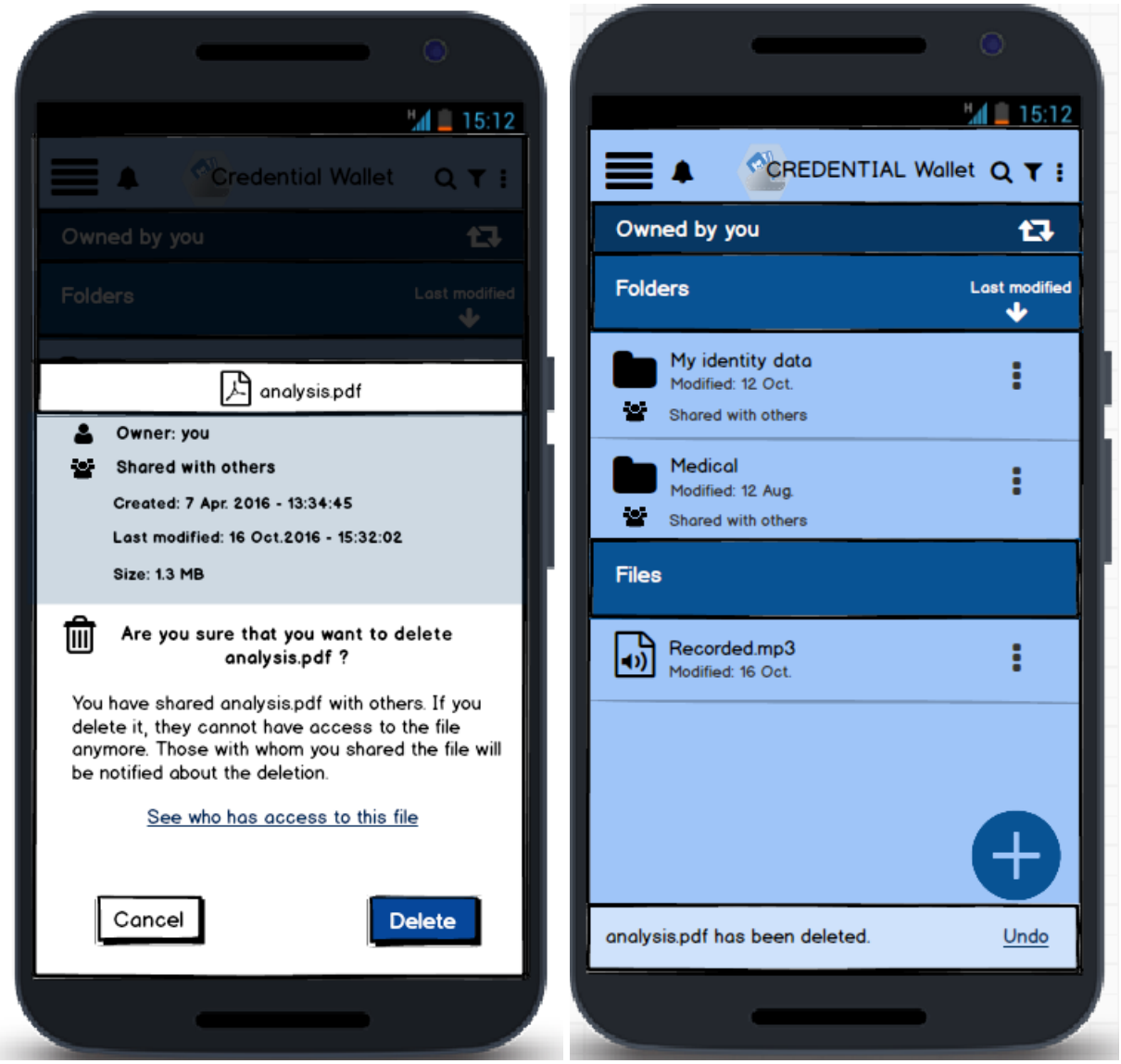
Appendix C. Other Views of the Main Page of the CREDENTIAL App

When viewing the main page of the CREDENTIAL app, Elsa has three different options to select which define the kind of files/folders she can see on the main page. The default is all the files that Elsa herself has uploaded. Elsa can select to see all the files that are shared with her or all the files being shared with her and uploaded by her.

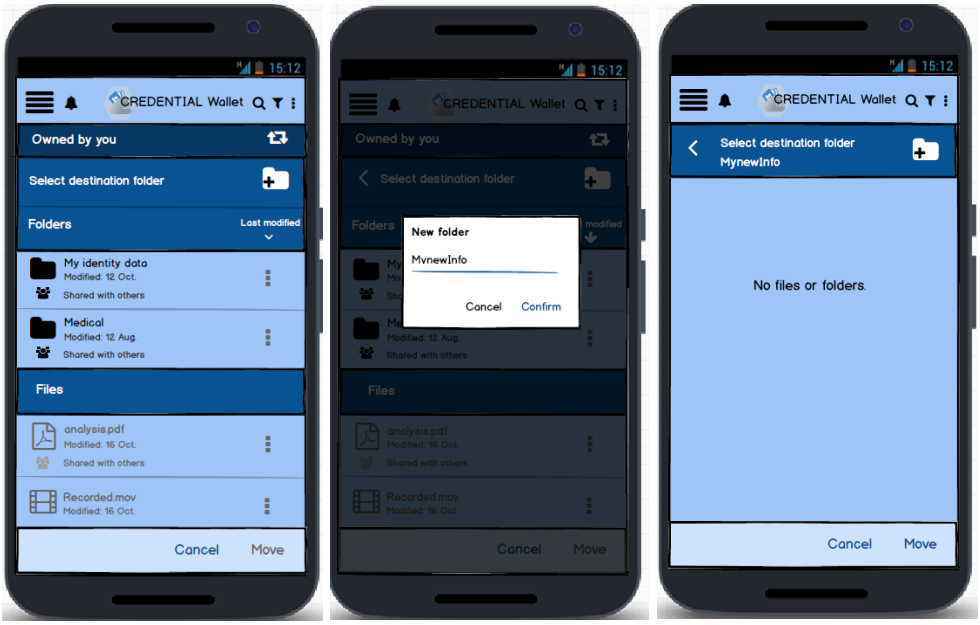


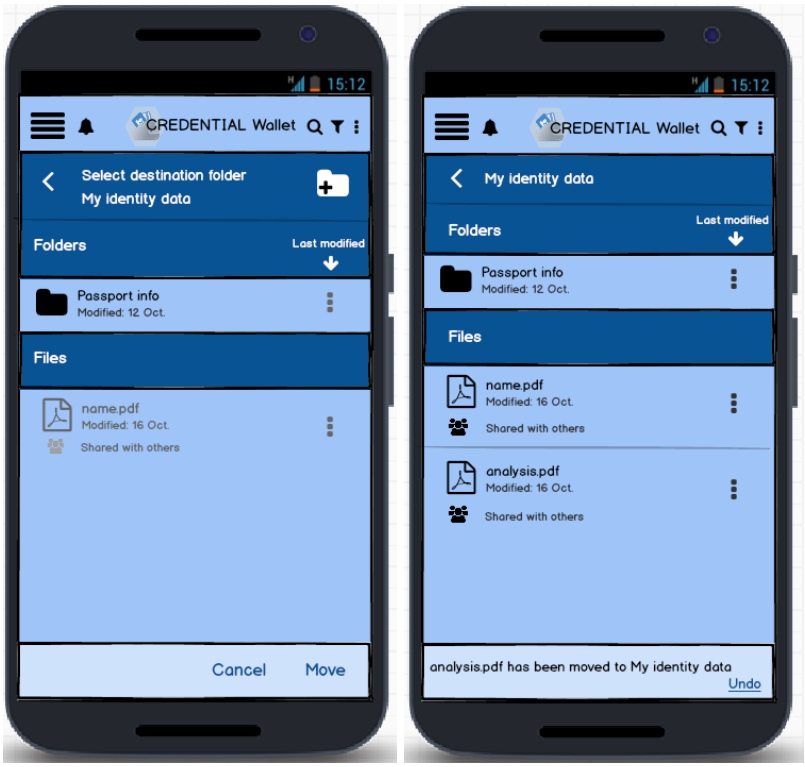
Appendix D. Delete, Move, Rename and Download Files and Folders

Delete Elsa can delete the files/folders that she has uploaded herself. If the file is shared with others, she is reminded of that fact and she is able to immediately see with whom the file is shared. After Elsa clicks on the “Delete” button, a small kind of notification is shown on the bottom of the page assuring that the file has been deleted.

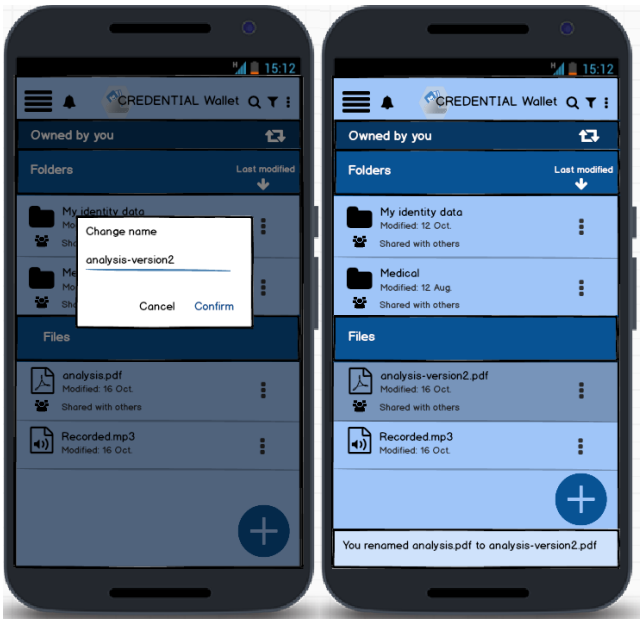


Move Elsa can change the path of the files she has uploaded by navigating through different folders or set a path if she wants to create some new folders.

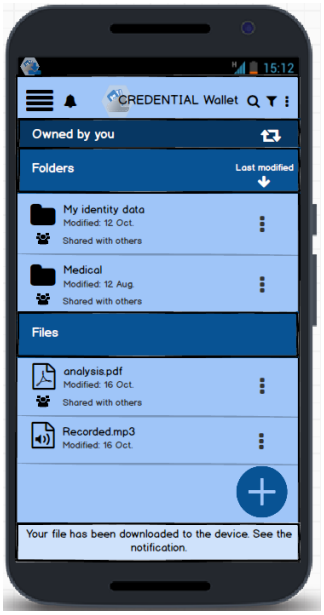




Rename Elsa also has the ability to change the name of the files/folders she owns. After she changes the name, a notification is shown to her at the bottom of the page and the renamed file/folder is briefly highlighted.



Download. When Elsa downloads a file on her device, she sees a notification informing the completeness of the download process.

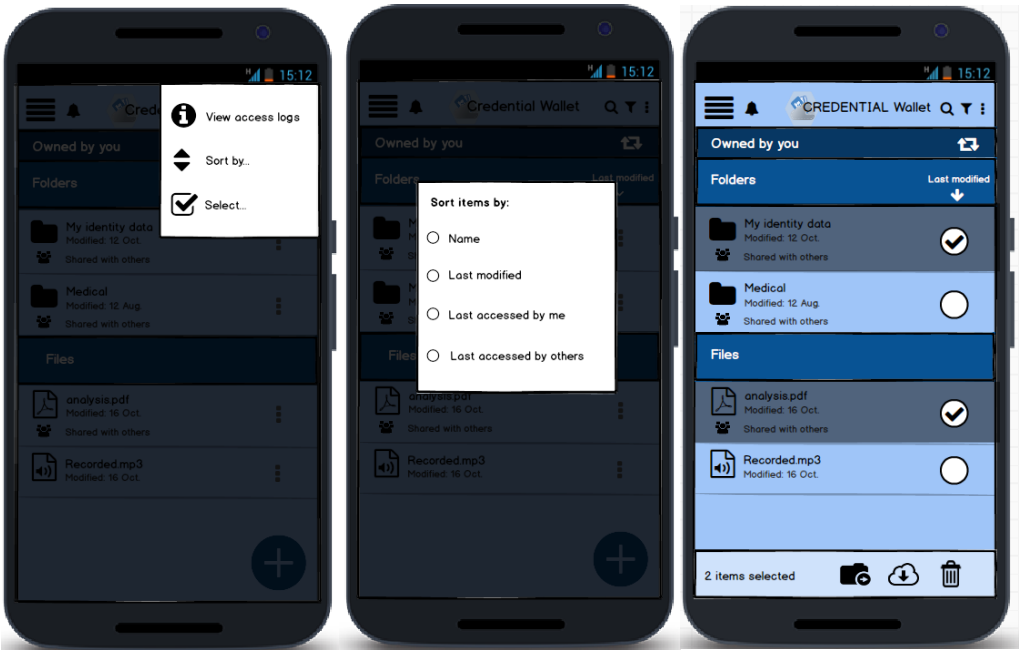


Appendix E. Filter, Search, Select and Sort Data

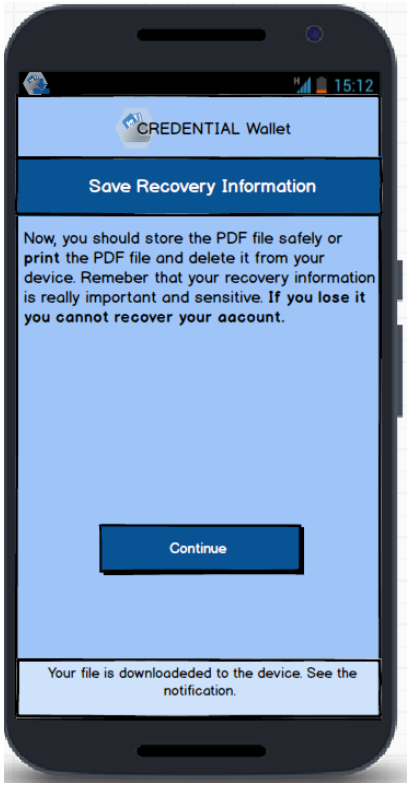
Filter Using the filter icon on the header bar, Elsa can filter the kind of files/folders she wants to see. The files can be filtered based on their types, their owners, if they are shared with others and their modification times.

Search Elsa can also search for files and folders typing specific keywords in a simple Search box.

Sort and select Moreover, using the vertical ellipsis on the header bar, Elsa can change the default property which the files/folders are sorted based on that. By default, the files/folders are sorted based on modification time but can be sorted based on some other properties.



Appendix F. Additional General UI



The current last state of "Save Recovery Information" has a text conveying "Now, you should store the PDF file safely or print the PDF file and delete it...." and when the user clicks on "Continue" button it means she/he is finished with recovery process and the PDF file is printed or stored somewhere safely. However, for the last state of "Save Recovery Information" screen the CREDENTIAL partners discussed several (dummy) alternatives in a Technical Workshop February 2017:

- Sending to a print service like the credit card companies use when they send us new pin codes: it is a trusted variant and the user only needs a permanent address;
- One could also upload the QR code to some Archistar storage that splits the file into fragments;
- Send it to your email account (disliked by me as these are often not so safe);
- And finally, upload to your trusted cloud storage, but with a notification of caution (as in the previous case).

Moreover, it was mentioned that in the last state of "Save Recovery Information" screen, the one with the above options, it should be stated that the exporting can only be done once.

Appendix G. Questionnaires in the User Study

Questionnaire for the Authorization Task (Task 1)

1. Please rank the following statements concerning the task you have done using the CREDENTIAL app. Use a number from 1 to 5 (**1: Strongly disagree, 2: Disagree, 3: Neutral, 4: Agree, 5: Strongly Agree**):

Statement	1	2	3	4	5
I think that I would like to use this system frequently.					
I found the system unnecessarily complex.					
I thought the system was easy to use.					
I think that I would need the support of a technical person to be able to use this system.					
I found the various functions in this system were well integrated.					
I thought there was too much inconsistency in this system.					
I would imagine that most people would learn to use this system very quickly.					
I found the system very difficult to use.					
I felt very confident using the system.					
I needed to learn a lot of things before I could get going with this system.					

2. What kind of information do you think can help you to make better decision when you are selecting the personal information you want to share with Photohex from your CREDENTIAL Wallet? (Do you want to receive any extra information for each requested piece of your personal data from PhotoHex?)

3. Which of the following options do you prefer? To manually select all the mandatory information by ticking the boxes to continue to next step (i.e., an interface as in current task); or to have all the mandatory information being selected by default where you do not have to tick any boxes?

4. When doing the task, what was unclear for you in the CREDENTIAL app? Did you have any difficulties? Where?

5. Tell us about the disadvantages and advantages of the interfaces you saw in the CREDENTIAL app.

6. What information did you share with the service provider (here, PhotoHex) in this task? (Select YES if you shared the information, select NO if you did not share the information and select NOT SURE if you do not know)

Information	YES	NO	NOT SURE
Your post address			
Your full name			
Your email address			
Your educational background			
Your fingerprint pattern			
Your home town			
The city in which you live			
Your birthday			
A photo of yours			
Your phone number			
Your interests			
Your credit card number			
Your age			
Your mobile device model			

Questionnaire for the Authentication Task (Task 2)

1. Please rank the following statements concerning the task you have done using the Credential app. Use a number from 1 to 5 (**1: Strongly disagree, 2: Disagree, 3: Neutral, 4: Agree, 5: Strongly Agree**):

Statement	1	2	3	4	5
I think that I would like to use this system frequently.					
I found the system unnecessarily complex.					
I thought the system was easy to use.					
I think that I would need the support of a technical person to be able to use this system.					
I found the various functions in this system were well integrated.					
I thought there was too much inconsistency in this system.					
I would imagine that most people would learn to use this system very quickly.					
I found the system very difficult to use.					
I felt very confident using the system.					
I needed to learn a lot of things before I could get going with this system.					

2. When you were doing this task, you were not asked for your consent to share the information with the service provider (PhotoHex). Why do you think it was like this?

3. [Whether you have rejected the request or not] what do you think will happen If you reject the request for this task (press the reject button rather than scanning your fingerprint)? Does the service provider still have access to your information?

4. When doing this task, what was unclear for you in the CREDENTIAL app? Did you have any difficulties? Where?

5. Tell us about the disadvantages and advantages of the interfaces you saw in the CREDENTIAL app when doing this task.

General Questionnaire (given to participants after they had answered questions about Task 2)

1. How old are you? _____

2. What is your highest educational degree? (If you study, please select the one you are pursuing)

   - Primary school - Grundskola
   - Secondary school - Gymnasiet
   - Bachelor degree, field: _____
   - Master degree, field: _____
   - Doctorate degree, field: _____
   - Other: _____

3. What is your gender?

   - Female
   - Male
   - Other

4. Have you ever seen the **Facebook or other websites' login buttons**? E.g.:

   - Yes
   - No

   If yes, have you ever used them?

   - Yes, on which websites? _____
   - No, why? _____

5. Do you use Mobile BankID?

   - Yes
   - No

   If yes, how often do you use it?

   - Almost everyday
   - 2-5 times a week
   - Once a week
   - Once a month
   - Other _____

6. What are your concerns regarding using the Credential app in future?

7. You scanned your fingerprint to give your consent to share your information from the CREDENTIAL app with a service provider (here, PhotoHex). What do you think about using your fingerprint to agree to share your personal data? What do you think are the pros & cons? Do you have any concerns regarding using your fingerprint to give consent?

8. Where do you think that your fingerprint is stored and processed:

a. On your mobile device
b. On the Credential Wallet
c. On the service provider side (PhotoHex)

Please tell us why you think so: _____

9. Please, explain why you think the following statements are correct or not. What does it mean if you accept to "share" your data in your CREDENTIAL Wallet with Photohex. (Select YES if you think each sentence is correct and NO if you think is not correct. State WHY you think so.)

- Photohex can request from my CREDENTIAL Wallet any updates of the selected information that I shared with it without notifying me.

  YES, because: _____
  NO, because: _____

- Photohex can request from my CREDENTIAL Wallet updates of the selected information that I shared with it only with a new consent from me.

  YES, because: _____
  NO, because: _____

- Photohex can also write information to my CREDENTIAL Wallet.

  YES, because: _____
  NO, because: _____

- I can revoke the "sharing" permissions that I have given to Photohex at any time.

  YES, because: _____
  NO, because: _____

Appendix H. TAM-like Factors and Possible Items of Inquery

This table is an exemplification of the work mentioned in section 6.2.

Factors (TAM and new ones)	**Items**	**Source**
Perceived Ease of Use (PE)	1. My interaction with the CREDENTIAL Wallet is clear and understandable. 2. Interacting with the CREDENTIAL Wallet doesn't require a lot of my mental effort. 3. I find the CREDENTIAL Wallet to be easy to use. 4. I find it easy to get the CREDENTIAL Wallet to do what I want it to do.	Davis (1989)
Perceived Usefulness for Primary Task (PU1)	"Employees" (e.g. doctors, public officers) 1. Using the CREDENTIAL Wallet improves my performance in my job. 2. Using the CREDENTIAL Wallet in my job increases my productivity. 3. Using the CREDENTIAL Wallet enhances my effectiveness in my job. 4. I find the CREDENTIAL Wallet to be useful in my job. "Voluntary users" (patients, citizens, consumers) 1. Using the CREDENTIAL Wallet helps me in my private life. 2. Using the CREDENTIAL Wallet makes it faster to do private errands. 3. Using the CREDENTIAL Wallet helps me to do many things I want to do. 4. I find the CREDENTIAL Wallet to be useful in my private life.	Davis (1989). Venkatesh and Davis (2000). Chuttur (2009). Benenson et al. (2015)
Perceived Usefulness for Privacy Protection (Secondary Task) (PU2)	1. Using CREDENTIAL Wallet improves my privacy protection. 2. Using CREDENTIAL Wallet enhances the effectiveness of my privacy protection. 3. I find the CREDENTIAL Wallet to be useful in protecting my privacy.	Benenson et al. (2015) Questions are deliberately made similar in order to correctly measure the construct. Most items in same construct are similar for same purpose.

Behavioral Intention to Use (BU)	1. Assuming I have access to the CREDENTIAL Wallet, I intend to use it. 2. Given that I have access to the CREDENTIAL Wallet, I predict that I would use it. 3. I plan to use the CREDENTIAL Wallet in the next <n> months.	Venkatesh and Bala (2008).
Credential management (CM)	1. I find it easy to add issued credentials into the CREDENTIAL Wallet. 2. I find it easy to add / import certificates into the CREDENTIAL Wallet. 3. I find it easy to manage my certificates and credentials.	Wästlund, et al. (2009).
Trust in provider (TP)	1. I trust that the CREDENTIAL Wallet does not reveal information about my identity because it contains technology developed by leading [technologists]. 2. I trust that the CREDENTIAL Wallet does not reveal information about my identity because the environment of the system is controlled by AIT (?). 3. I trust that the CREDENTIAL Wallet does not reveal information to the Wallet IdP because the CREDENTIAL technology was built within the framework of an EU project. 4. I trust that the CREDENTIAL Wallet does not reveal information about my identity because strong cryptographic algorithms are used.	This to be related to section 6.6 on risk communication in a discussion about the options for disseminating the Wallet as well as how users buy cloud storage for their Wallet.
Complexity (CO)	1. Using the CREDENTIAL Wallet takes too much time from my normal duties. 2. Working with the CREDENTIAL Wallet is so complicated; it is difficult to understand what is going on. 3. Using the CREDENTIAL Wallet involves too much time doing mechanical operations (e.g., data input). 4. It takes too long to learn how to use the CREDENTIAL Wallet to make it worth the effort.	Venkatesh et al. (2003)