Digital Security: Cybersecurity,
Privacy and Trust
DS-02-2014 Access Control

European Commission

Horizon 2020
European Union funding
for Research & Innovation

From Real-world Identities to Privacy-preserving and Attribute-based CREDentials for Device-centric Access Control

ReCRED

WP7 –Large Scale Pilots and End User Experience Assessment

Deliverable D7.5 “HCI concept testing on user groups” (revised)

Editor(s):	CNIT, TID, Upcom
Author(s):	Annamaria Recupero (CNIT), Alessandra Talamo (CNIT), Claudio Soriente (TID), Vangelis Bagiatis (Upcom)
Dissemination Level:	PU - Public
Nature:	R
Version:	0.4

ReCRED Project Profile

Contract Number	653417
Acronym	ReCRED
Title	From Real-world Identities to Privacy-preserving and Attribute-based CREDentials for Device-centric Access Control
Start Date	May 1st, 2015
Duration	36 Months

Partners

	University of Piraeus research center	Greece
	Telefonica Investigacion Y Desarrollo Sa	Spain
	Verizon Nederland B.V.	The Netherlands
	Certsign SA	Romania
	Wedia Limited	Greece
	EXUS Software Ltd	U.K.
	Upcom Bvba (sme)	Belgium
	De Productizers B.V.	The Netherlands
	Cyprus University of Technology	Cyprus
	Universidad Carlos III de Madrid	Spain
	Consorzio Nazionale Interuniversitario per le Telecomunicazioni	Italy
	Studio Professionale Associato a Baker & Mckenzie	Italy

Document History

Version	Date	Author	Remarks
0.10	04.02.2016	Annamaria Recupero, Alessandra Talamo (CNIT)	First draft
0.20	02.05.2016	Annamaria Recupero, Alessandra Talamo (CNIT), Claudio Soriente (TID)	Second draft – added contents in 2.4.3
0.30	08.06.2016	Annamaria Recupero, Alessandra Talamo (CNIT)	Third draft - review by Upcom
0.40	18.07.2016	Annamaria Recupero, Alessandra Talamo (CNIT), Vangelis Bagiatis (Upcom)	Fourth draft - added contents in 2.4.3
0.50	26.07.2016	Annamaria Recupero, Alessandra Talamo (CNIT)	Final version
0.60	21.07.2017	Annamaria Recupero, Alessandra Talamo (CNIT)	Final revised version

Executive Summary

This document is a revision of the Deliverable 7.1 “HCI concept testing on user groups”. It includes further data gained from the investigation of Human-Computer Interaction (HCI) issues connected with the implementation of the ReCRED solution, within the Task 7.5 – *End-User Experience Assessment*.

According to the user-centred approach, the goal of this investigation is to understand the point of view of the different groups of target end-users, who have specific needs and personal representations of privacy and security when they use web services during their daily life.

Acquiring knowledge about the User Experience (UX) and developing empathy with the users are the keys to reach the best solution that can solve the problems of the current Access Control (AC) systems (such as the password overload) and provide a successful experience.

Taking advantage from the use of different research methods borrowed from the field of psychology and social research as well as from the field of design, we can evaluate the usefulness of the ReCRED solution and improve its positive impact on the UX.

The research framework and the methods used to collect and analyse empirical data are discussed in the second chapter of this document, while in the third chapter the main results are presented with reference to the literature.

The results provide an overview of users’ representations and attitudes regarding the topics of privacy and security on the web. Furthermore, they highlight the main aspects of the UX related to the traditional password-based AC, compared with the UX that is provided by the use of biometric factors for identity verification, also considering the findings of other studies conducted in the field of HCI.

The main objective of the research is to evaluate how the ReCRED concept meets the needs and preferences of different groups of end-users, and also to generate design issues to be addressed during the development of the ReCRED solution.

Table of Contents

List of Tables and Figures

1. Introduction

Within the ReCRED project, we apply the user-centred approach that is nowadays acknowledged by most of the experts in the field of Human-Computer Interaction (HCI) as a valuable perspective.

This approach requires to place the users at the centre of the design, through a deep understanding of their point of view, needs, attitudes and preferences, and also involving them in the usability evaluation [1].

On the contrary, if the design is carried out according to an imaginary representation of the users that is inevitably influenced by designers’ personal experiences and point of view (by prejudice and beliefs), the result might not be valid for the actual users.

In order to reach a successful solution suitable for different kinds of users, the ReCRED project includes a qualitative research to investigate the User Experience (UX) connected with Access Control (AC) solutions for web services usage.

User Experience is a holistic concept and it can be defined as «all the aspects of how people use a product: the way it feels in their hands, how well they understand how it works, how they feel about it while they’re using it, how well it serves their purposes, and how well it fits into the entire context in which they are using it» [2 p.11].

The data we have collected through the research support and guide the design process of the ReCRED solution proving a general framework that describes the UX, as well as the contexts and the system of practices in which the ReCRED solution will be implemented, through the use of some design models (such as the *Personas*).

The research also provides suggestions and issues which are translated into use cases and scenarios[1].

Moreover, it highlights the positive impact of the ReCRED solution on the UX, based on the pain points of the current password-based paradigm.

In order to reach such purposes, the research has been carried out using different methods and tools within a HCI perspective that tends to consider the user as a “human actor” [3], guided by motivations and values, acting within a socio-cultural context.

Only if the design solution meets users’ needs, provides a positive experience and is recognized as a valid and valuable solution, will it for sure obtain a positive outcome [4].

2. Research methods

According to the general framework mentioned above, the qualitative methodology has been chosen because it is suitable to gain the kind of information we need. In fact, the goal of the research is to produce meaningful descriptions of the UX and identify design issues, rather than to verify pre-defined hypothesis.

The research has started at the beginning of the ReCRED project, and the first step was the identification of the topics to investigate and the elaboration of the research questions that guide the collection and analysis of data.

[1] See Deliverable 2.1 “Business cases” and Deliverable 2.2 “Business and technical requirements”.

Research questions	Scope and topics
– Which are the web services the users manage in their daily activities? – Which are the contexts of use of those web services?	Explore the scenarios for the implementation of the ReCRED solution, and contextualize the use of web services within daily practices.
– How do the users manage their online identities? – Which are the pain points the users meet when they manage their online accounts?	Explore common practices for managing online identities, and identify the main problems of the current password-based AC.
– How do the users interpret the concept of privacy? – What kind of information do the users consider as sensitive and confidential?	Understand the personal representations and attitudes towards privacy.
– Which are the criteria the users consider to evaluate the reliability of the online accounts and AC systems? – Which are the precautions the users apply to make their online account secure?	Analyze the perceived reliability of AC and identify common and specific practices to ensure security.
– Which are users' attitudes and concerns toward the use of biometric factors for identity verification?	Explore the value of biometric factors for identity verification according to users' representations and preferences

Table 1- Research questions

In order to answer to these questions, the research has been carried out using different procedures for collecting data, both from empirical investigation and from secondary sources of information. Using different techniques and integrating the data, we can highlight findings which explain not just the behaviour of the users, but also the motivations and the personal representations connected with their practices.

The research has been carried out following this path:

1) literature review
2) semi-structured interviews
3) cognitive interviews
4) questionnaire
5) data analysis.

2.1.Literature review

The literature review was the preliminary step of the research to explore the domain and the different topics addressed by the ReCRED project. Among the several studies reported in the literature, we have selected those which provide useful findings to understand issues and concerns regarding privacy and security from the users' point of view.

This background material (including research reports, conference papers and academic publications) allows us to define the conceptual framework that guides the collection and the interpretation of empirical data, according to already recognized and developed theories and constructs [5].

Furthermore, because the UX research within the ReCRED project is a circumscribed investigation, the literature serves as secondary source of information as well as supplementary validation of the accuracy of our findings.

The literature review was carried out from the beginning of the research until the data analysis, because – when a new phenomenon (or even relations among concepts) emerges as pertinent from the empirical investigation – we use the literature as reference to understand what other researchers have reported about it [5].

2.2.Interviews

The interview was used as main technique to collect empirical data, involving users from the first pilot site (*Campus Wi-Fi and web services access control*).

Interviewed participants are 7 professors and 23 students from two universities of Rome (“Sapienza” and “Tor Vergata” that are members of CNIT), who can be considered as end-users of the ReCRED solution. In addition to the interviews conducted with students and professors, we have also involved two members of the front-office staff who work to provide services to students and professors: an administrative officer and a library assistant. They were interviewed in order to investigate their job and understand how the ReCRED solution can be implemented in their services.

User role	Professor	7 up to 32
	Student	23 up to 32
	Front-office staff	2 up to 32
Gender	Female	13 up to 32
	Male	17 up to 32
Age	18-24 years’ old	13 up to 32
	25-34 years’ old	10 up to 32
	35-44 years’ old	5 up to 32
	45-54 years’ old	1 up to 32
	+ 55 years’ old	3 up to 32

Table 2 - Information about interviewed participants

We have conducted two kinds of interviews[2]: semi-structured and cognitive interviews.

In the case of semi-structured interviews, the questions asked were mainly open-ended so to foster the respondents to describe their experience and point of view, without forcing them to select from pre-defined answers [6].

The framework of the interview has been defined to explore pain points and common practices related to campus WiFi and university web services, as well as to other kind of web services included in the different ReCRED scenarios (such as Internet banking, social network etc). Although this framework has been defined to cover a list of pre-defined questions, it was flexible enough to be adapted to the narration of the interviewed, so to expand and enrich the answers [7].

In addition to the semi-structured interviews, we have conducted cognitive interviews in order to reach two objectives: to collect primary data about the UX, and also to assess a questionnaire that we have created as further source of information.

Indeed, the cognitive interview is a face-to-face interview through which we have evaluated how the respondents understand the different items included in the questionnaire, and which cognitive and emotional processes are activated in the selection of the answers [8].

[2] According to the informed consent accepted by participants, the interviews have been video/audio recorded and then transcribed using fictional names in order to maintain the concealed identity of the participants.

2.3.Questionnaire

We have decided to collect data using an online questionnaire, because it allows us to gain a great amount of information about users from all the ReCRED partners’ countries, with less time and effort compared with the time and effort required to conduct interviews.

The items included in the questionnaire has been created based on the data gained through the interviews, and also considering other questionnaires used in similar researches [9, 10, 11].

The questionnaire has been assessed with a sample of respondents (10 students) using the cognitive interview technique described above, and it has been evaluated by three experts[3] who have provided suggestions to improve it.

The objective of such process was the assessment of the questionnaire according to the following questions:

- ✓ Does each item investigate what it is supposed to investigate?
- ✓ Are all the terms and expressions understood?
- ✓ Do all respondents interpret the questions in the right way?
- ✓ Are all response choices appropriate and do they cover all the possible alternatives?

Thanks to the feedback from testers and experts, we have improved the first draft of the questionnaire and we have spread it using *Google Form*[4].

The questionnaire (*Annex 1*) includes different groups of items.

The first items aim at identifying the respondents as “heavy” or “light” users [12]: while heavy users often use web services and manage several online accounts, light users are those who use the web only occasionally or rarely. These preliminary items (together with the personal information such as age, occupation, educational qualification and field of study/work) are useful to contextualize the other answers and shape the respondent’s profile.

The other items (with a 5-points or 3-points Likert scale) explore users’ general representations and attitudes towards privacy and security on the web, and users’ attitudes and preferences towards the use of biometric factors for identity verification, according to the different ReCRED scenarios.

The total number of respondents is 146 (N=146).

Age	18-24 years old	43%
	25-34 years old	37%
	35-44 years old	16%
	45-54 years old	1%
	+55 years old	3%
Nationality	Italy	67,4%
	Greece	10,3%
	Cyprus	8,1%
	Spain	7,4%
	Other[5]	6,8%
Field of work/study	Computer science, Engineering	87%
	Other[6]	13%
Occupation	Student	55%

[3] Experts in the field of HCI, external from the ReCRED project.

[4] https://www.google.it/intl/it/forms/about/

[5] The other nationalities are: Romania, USA, UK, Turkey, Morocco, India, Russia, Israel and Venezuela.

[6] The other fields of work/study are: Medical science, Psychology, Foreign Languages, Agriculture, Law.

	Researcher	10,2%
	Professor	4,4%
	Engineer, Computer scientist	18,8%
	Office worker	5%
	Other[7]	1,6%
Educational qualification	High school	38%
	Bachelor	22%
	Master	23%
	PhD/advanced	17%

Table 3 - Information about questionnaire respondents

2.4.Data analysis tools

The empirical data were integrated and elaborated using three tools which are useful models to provide a comprehensive and evocative representations of target users' characteristics, goals and needs: *Empathy Map*, *Persona* and *Mental Model*.

Each of these models serves a specific function for the data analysis: the Empathy Map provides a structure to integrate different emotional, cognitive and behavioral dimensions which compose the whole UX; Personas allow us to identify different groups of users and describe their characteristics; while the Mental Model represents the behaviors and the common practices in managing online identities.

2.4.1 Empathy Map

Empathy Map [13] is the tool that allows the first integration and organization of the great amount of collected data. It consists in a map of the whole experience in the domain of AC and web service usage, including different dimensions:

- feelings and emotions;
- meanings, opinions and visions of the world;
- typical quotes and relevant use of the words;
- activities, common practices and behaviors;
- needs and wishes;
- pain points, struggles and barriers;
- what the users see in their context;
- rumors, suggestions and opinions heard from others.

From the empirical data collected, we have created one Empathy Map for each user role (*Annex 2*): one of the students, one of the professors and another map of the front office staff.

The following figure shows how the Empathy Map looks like.

[7] The other occupations are: musician, laborer, attorney, religious person, director and pensioned.

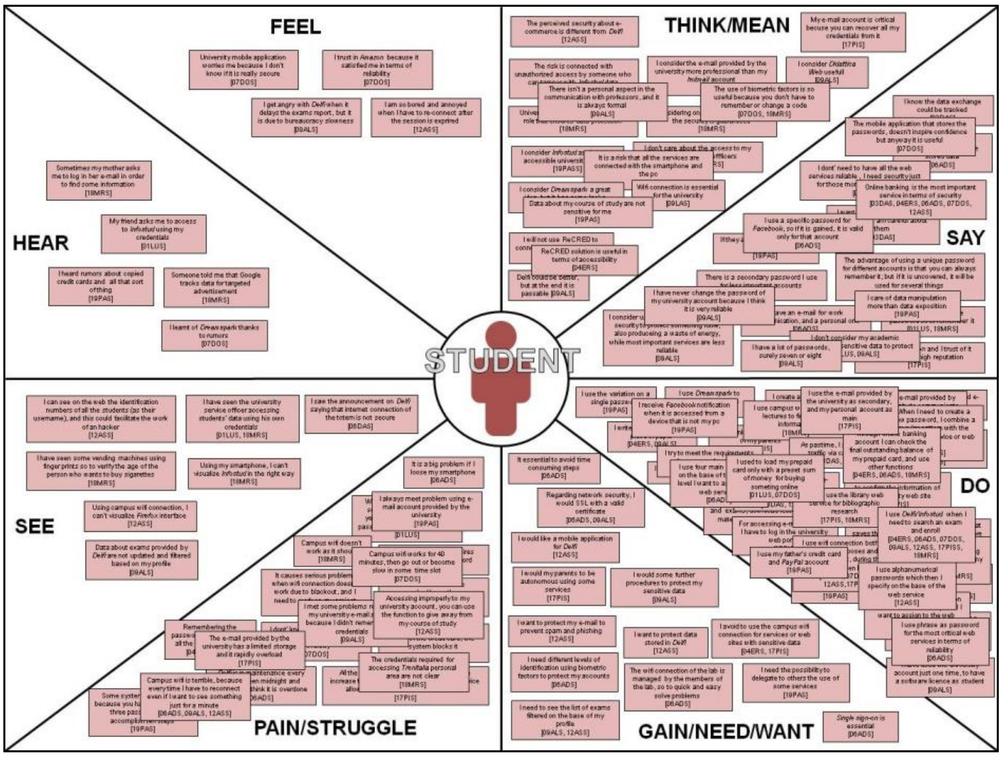


Figure 1 - Empathy Map of the student

2.4.2 Personas

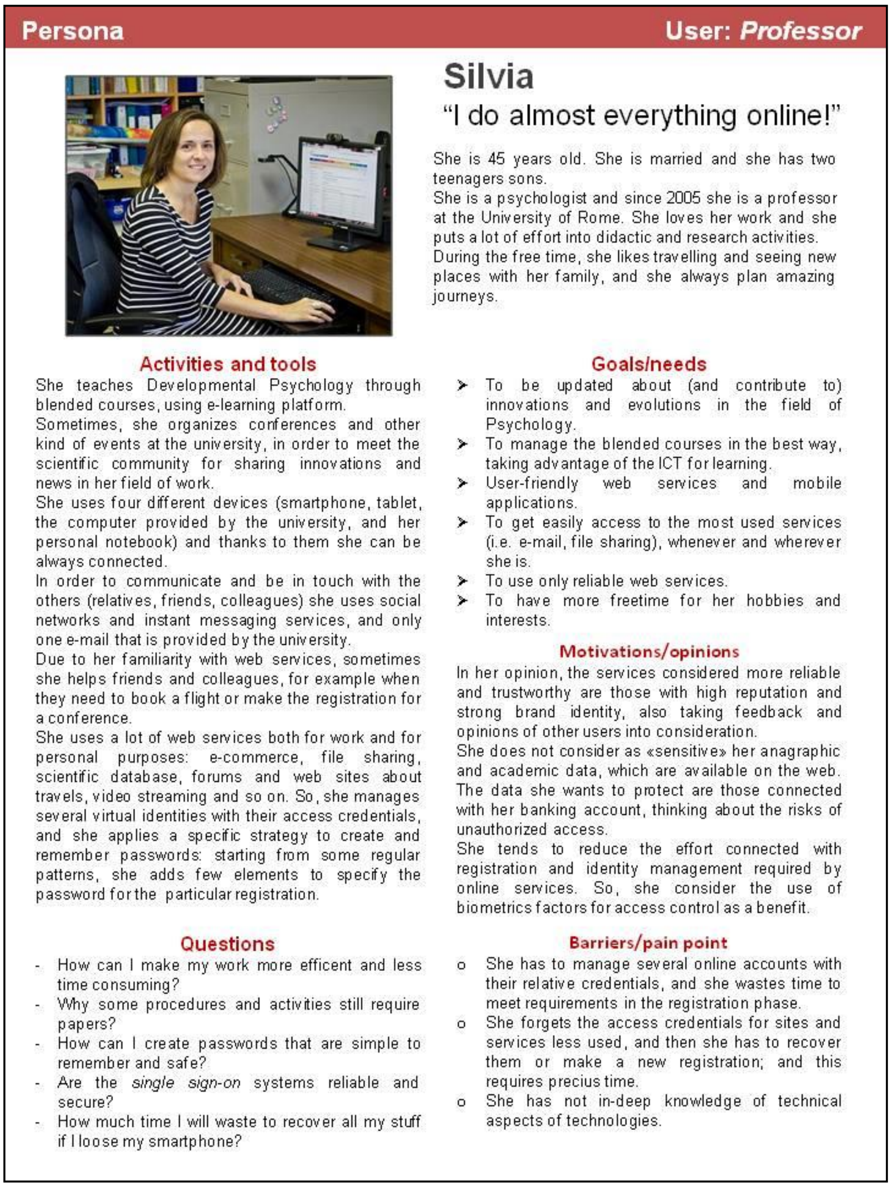
Personas [14] are typical users, fictional characters representing groups of real users who share common needs, motivations and activities.

Such archetypal users are defined as fully formed people, because verisimilitude most likely contributes to the strength of Personas [15]: they sound like people you could know, and over the course of the project can take on a reality that encourages empathy and facilitates thinking from the user’s perspective.

Among the several users involved in the research, we have identified 7 Personas (*Annex 3*): they differ for their roles as users of university web services (student, professor or front office staff), web services usage patterns and personal attitudes towards privacy and security on the web.

Each Persona is characterized by:

- proper name and picture;
- quote that is typical and distinctive of that kind of user;
- brief description of the profile;
- activities and tools used during daily life;
- motivations and personal representations;
- needs and goals;
- questions and doubts;
- barriers and pain points.



Persona **User: *Professor***

Silvia

“I do almost everything online!”

She is 45 years old. She is married and she has two teenagers sons.
She is a psychologist and since 2005 she is a professor at the University of Rome. She loves her work and she puts a lot of effort into didactic and research activities.
During the free time, she likes travelling and seeing new places with her family, and she always plan amazing journeys.

Activities and tools

She teaches Developmental Psychology through blended courses, using e-learning platform.
Sometimes, she organizes conferences and other kind of events at the university, in order to meet the scientific community for sharing innovations and news in her field of work.
She uses four different devices (smartphone, tablet, the computer provided by the university, and her personal notebook) and thanks to them she can be always connected.
In order to communicate and be in touch with the others (relatives, friends, colleagues) she uses social networks and instant messaging services, and only one e-mail that is provided by the university.
Due to her familiarity with web services, sometimes she helps friends and colleagues, for example when they need to book a flight or make the registration for a conference.
She uses a lot of web services both for work and for personal purposes: e-commerce, file sharing, scientific database, forums and web sites about travels, video streaming and so on. So, she manages several virtual identities with their access credentials, and she applies a specific strategy to create and remember passwords: starting from some regular patterns, she adds few elements to specify the password for the particular registration.

Questions

- How can I make my work more efficent and less time consuming?
- Why some procedures and activities still require papers?
- How can I create passwords that are simple to remember and safe?
- Are the *single sign-on* systems reliable and secure?
- How much time I will waste to recover all my stuff if I loose my smartphone?

Goals/needs

- ➤ To be updated about (and contribute to) innovations and evolutions in the field of Psychology.
- ➤ To manage the blended courses in the best way, taking advantage of the ICT for learning.
- ➤ User-friendly web services and mobile applications.
- ➤ To get easily access to the most used services (i.e. e-mail, file sharing), whenever and wherever she is.
- ➤ To use only reliable web services.
- ➤ To have more freetime for her hobbies and interests.

Motivations/opinions

In her opinion, the services considered more reliable and trustworthy are those with high reputation and strong brand identity, also taking feedback and opinions of other users into consideration.
She does not consider as «sensitive» her anagraphic and academic data, which are available on the web.
The data she wants to protect are those connected with her banking account, thinking about the risks of unauthorized access.
She tends to reduce the effort connected with registration and identity management required by online services. So, she consider the use of biometrics factors for access control as a benefit.

Barriers/pain point

- o She has to manage several online accounts with their relative credentials, and she wastes time to meet requirements in the registration phase.
- o She forgets the access credentials for sites and services less used, and then she has to recover them or make a new registration; and this requires precius time.
- o She has not in-deep knowledge of technical aspects of technologies.

Figure 2 - Persona of professor

2.4.2 Mental Model

Once we have identified the target users and shaped their profiles as Personas, we need to explore more deeply their activities within the domain of AC and web service usage.

The ReCRED solution is designed to enable users to perform activities, and this requires more than just an understanding of the roles the users play, but also a thorough understanding of the tasks that users accomplish while performing those roles [15].

Considering human activities, they are driven by certain needs where people wish to achieve certain purposes, and they are mediated by one or more instruments and tools [16]. This function of “mediation” is essential to understand the nature of artifacts as objects in use, and the way they support human activities [17].

For the purpose of analyzing users’ activity system (that includes goals, actions and artifacts) so to identify the best way the ReCRED solution can support them, we created the Mental Models.

A Mental Model is an affinity diagram of user activity system represented as a flow of tasks to accomplish goals; in the bottom part of the diagram, it also maps existing tools, services and contents which support the different users’ activities [18].

Based on the empirical data, we created two Mental Models (*Annex 4*): one for describing end-users (students and professors) behaviors regarding web service usage, and the other for representing the flow of the work of library assistant as member of the front office staff.

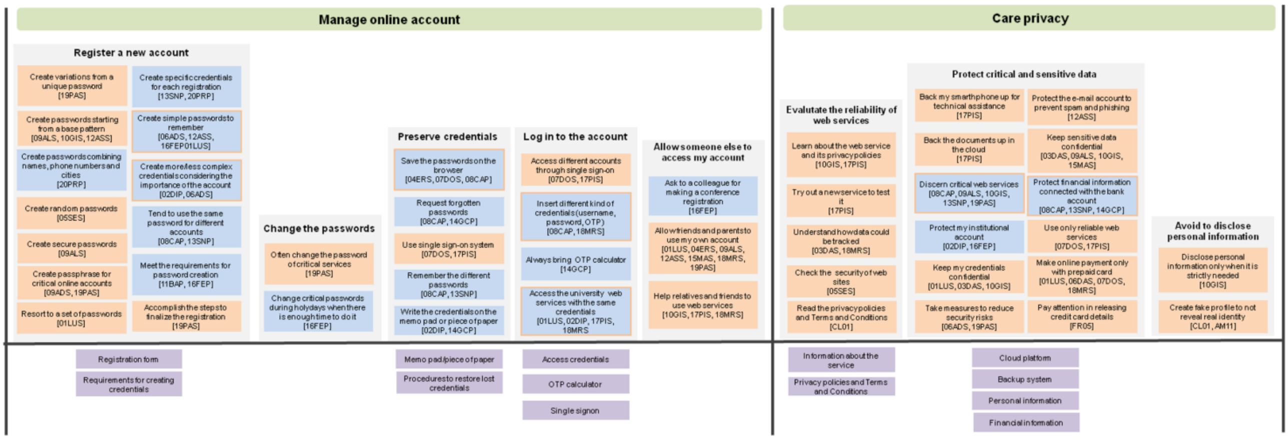

Manage online account
Register a new account
Create variations from a unique password [19PAS]
Create specific credentials for each registration [13SNP, 20PRP]
Create passwords starting from a base pattern [09ALS, 10GIS, 12ASS]
Create simple passwords to remember [06ADS, 12ASS, 16FEP01LUS]
Create passwords combining names, phone numbers and cities [20PRP]
Create more/less complex credentials considering the importance of the account [02DIP, 06ADS]
Create random passwords [05SES]
Tend to use the same password for different accounts [08CAP, 13SNP]
Create secure passwords [09ALS]
Meet the requirements for password creation [11BAP, 16FEP]
Create passphrase for critical online accounts [09ADS, 19PAS]
Resort to a set of passwords [01LUS]
Accomplish the steps to finalize the registration [19PAS]
Change the passwords
Often change the password of critical services [19PAS]
Change critical passwords during holydays when there is enough time to do it [16FEP]
Preserve credentials
Save the passwords on the browser [04ERS, 07DOS, 08CAP]
Request forgotten passwords [08CAP, 14GCP]
Use single sign-on system [07DOS, 17PIS]
Remember the different passwords [08CAP, 13SNP]
Write the credentials on the memo pad or piece of paper [02DIP, 14GCP]
Log in to the account
Access different accounts through single sign-on [07DOS, 17PIS]
Insert different kind of credentials (username, password, OTP) [08CAP, 18MRS]
Always bring OTP calculator [14GCP]
Access the university web services with the same credentials [01LUS, 02DIP, 17PIS, 18MRS
Allow someone else to access my account
Ask to a colleague for making a conference registration [16FEP]
Allow friends and parents to use my own account [01LUS, 04ERS, 09ALS, 12ASS, 15MAS, 18MRS, 19PAS]
Help relatives and friends to use web services [10GIS, 17PIS, 18MRS]
Registration form
Requirements for creating credentials
Memo pad/piece of paper
Procedures to restore lost credentials
Access credentials
OTP calculator
Single signon
Care privacy
Evalutate the reliability of web services
Learn about the web service and its privacy policies [10GIS, 17PIS]
Try out a new service to test it [17PIS]
Understand how data could be tracked [03DAS, 18MRS]
Check the security of web sites [05SES]
Read the privacy policies and Terms and Conditions [CL01]
Protect critical and sensitive data
Back my smarthphone up for technical assistance [17PIS]
Protect the e-mail account to prevent spam and phishing [12ASS]
Back the documents up in the cloud [17PIS]
Keep sensitive data confidential [03DAS, 09ALS, 10GIS, 15MAS]
Discern critical web services [08CAP, 09ALS, 10GIS, 13SNP, 19PAS]
Protect financial information connected with the bank account [08CAP, 13SNP, 14GCP]
Protect my institutional account [02DIP, 16FEP]
Use only reliable web services [07DOS, 17PIS]
Keep my credentials confidential [01LUS, 03DAS, 10GIS]
Make online payment only with prepaid card [01LUS, 06DAS, 07DOS, 18MRS]
Take measures to reduce security risks [06ADS, 19PAS]
Pay attention in releasing credit card details [FR05]
Avoid to disclose personal information
Disclose personal information only when it is strictly needed [10GIS]
Create fake profile to not reveal real identity [CL01, AM11]
Information about the service
Privacy policies and Terms and Conditions
Cloud platform
Backup system
Personal information
Financial information

Figure 3 - Mental Model of end-users

2.4.3 Assessment of biometric characteristics

Along with the UX research described in this Deliverable, ReCRED project includes a research to assess the effectiveness of the biometric systems that will be implemented in the ReCRED solution: gait-based authentication and face recognition.

Among the different biometric factors, gait-based authentication is the mechanism to authenticate a person based on his walking pattern that will be used within ReCRED solution.

The walking pattern of an individual is constructed by collecting three-dimensional accelerometer sensor data. Since accelerometers are available in almost every smartphone, this allows us to collect accelerometer data in real-world scenarios. With this data, we would be able to develop a robust model to authenticate users based on their gait characteristics.

In order to collect this data, we have invited some users to install an Android application, which periodically collects accelerometer data in a battery-efficient manner. The app uses a significant motion sensor, which is a low-power sensor and triggers an event whenever there is a change of place by the phone/user. This helps us to remove any noise caused by the device movement in addition to saving battery by not recording accelerometer data unnecessarily. In case there is no significant motion sensor in the phone, we check if the magnitude of accelerometer data is above a certain threshold in order to help us decide whether there is walk-like activity being performed. After successful collection of accelerometer data for a certain time period, the app goes to sleep to conserve battery power.

The process of data collection in the app starts as soon as the user opens the app for the first time. The user is presented with a form to specify his/her gender, age, height, weight and email address. All the fields in the form are optional to allow the user to be completely anonymous. A random UUID is assigned to the user upon installation which helps us to group the data from one user under a certain ID while keeping the user anonymous. Moreover, the app periodically syncs the data collected, every two hours, with a remote server on a secure and encrypted channel. User can also view the data collected in the past hour through file explorer in the application’s data directory.

Another biometric characteristic that will be used within ReCRED as a user authentication factor is face recognition.

Facial features are captured, extracted and then matched against a database of existing facial templates, in order to confirm (verify) the identity of an individual.

A mobile application has been implemented that can extract and store facial templates of the device’s owner and then seamlessly executes a verification operation in order to authenticate the user to the device. More specifically, during the verification operation, the application uses the device’s camera in order to detect a face. After a face is detected, the application extracts the facial features of the user and compares them against all the facial templates that are created during the enrollment. A matching score is then calculated (a number between 0 and 1 - the higher that number the most confident the application is of the user’s identity) and compared to a predefined threshold. If the matching score is above the required threshold, then the user’s identity is considered to be verified.

A small scale research has been conducted in order to evaluate this face recognition application. The purpose of this research is to test the face recognition engine using a sample of users with different characteristics and under different conditions, so that any false positives (results that indicates that an individual’s identity was verified by the face recognition engine, when it should not be verified) and/or false negatives (results that indicates that an individual’s identity was not verified by the face recognition engine, when it should be verified) are identified.

Initially, we trained the database with a sample of different face photos coming from 50 random individuals (males and females, having a diversity of emotions and features). After that, a set of 20 testers were identified, also with a diversity of gender and features. During the execution of the research, each tester was introduced to the face recognition application and then performed a series of verification attempts, under the guidance of a researcher who would ensure the proper execution of the verification attempts and log the results. The testers performed verification attempts before training the face recognition engine (in order to discover false positives) and after the engine’s training (in order to discover false negatives). In both cases, the verification attempts were performed both under good and poor lighting conditions and having different minimum matching score thresholds (.50 and .75 - the higher the threshold the lower the engine’s tolerance level).

The only false positives (20%) appear when the subjects used the app under poor lighting conditions and with the threshold set at 0.50. On the other hand, the engine seems to produce a significant number of false negatives when the testers used the app under bad lighting conditions (40% with the threshold set at 0.50 and 65% with the threshold set at 0.75). In conclusion, the face recognition engine seems to be most efficient while used under good lighting conditions, since poor lighting tends to hinder the successful verification of the subjects. Moreover, higher thresholds tend to produce less false positives but more false negatives, since the engine is stricter while trying to confirm the identity of the user. Lower thresholds, on the other hand, are more tolerant and, therefore, more successful on verifying the user’s identity, but may produce some false positives when used under poor lighting conditions.

The results of such researches about gait-based authentication and face recognition are fully described in the Deliverable 3.2 “Multifactor authentication for DCA”.

3. Discussion of results

Most of the results described in this Deliverable represent empirical evidence that supports and grounds the design concept of the ReCRED project.

Indeed, according to the problems the users report regarding their practices for managing online accounts, the attempt to design a reliable AC system using device-centric multifactor biometric authentication represents an innovative change in the traditional UX.

The discussion of results starts with some considerations about privacy concerns, so to explore how ReCRED can benefit the different kinds of users according to their specific needs and preferences.

Empirical data we have collected regarding this topic are integrated with the results from other surveys reported in the literature (involving wide samples of participants), so to enrich and enlarge the discussion about users’ personal representations and attitudes towards the protection of data.

Moreover, we can consider the different insights gained from the empirical data as suggestions to identify specific use cases, and design issues that need to be addressed in the perspective of the user-centred design.

3.1. Privacy concerns from users’ point of view

As the use of web services - and the disclosure of personal information to access them - increases, so do risks associated with security and privacy [19].

Privacy is a fundamental human right, enshrined in the *United Nations Universal Declaration of Human Rights* and the *European Convention on Human Rights*.

«Every day, billions of people around the world use the Internet to share ideas, conduct financial transactions, and keep in touch with family, friends, and colleagues. Users send and store personal medical data, business communications, and even intimate conversations over this global network. But for the Internet to grow and thrive, users must continue to trust that their personal information will be secure and their privacy protected» [20]

A survey conducted by the U.S. Census Bureau [20] shows that Americans are increasingly concerned about online security and privacy while data breaches, cybersecurity incidents, and controversies over the privacy of web services have become more prominent.

These concerns are prompting some users to limit their online activity (such as conducting financial transactions, buying goods or services, posting on social networks or expressing opinions), especially those who had been affected by an online security breach, identity theft, or similar malicious activity.

The results gained from the ReCRED questionnaire show that the security of online accounts is a fundamental issue for 91% of the respondents. Despite most of the respondents (62%) think that the privacy of Internet users is greatly violated and the web is not safeguarded enough (65%), security and privacy concerns don’t seem to represent barriers for the online activities: only 37% of the respondents limit the use of the web due to privacy and security concerns.

Considering users’ perception, it is not necessarily important how private or safe the users are from policy makers’ point of view, but whether they perceive themselves to be safe and private. Thus, identifying users’ perceptions of privacy is an important element for distinguishing what needs to be protected and how best to protect it [19].

According to the model elaborated by Adams [19], perception of privacy seems to be shaped by the interrelation of four key elements:

- the perceived identity of the information *receiver;*
- the perceived *usage* of the information;
- the subjective *sensitivity* of the disclosed information;
- the *context* in which the information is disclosed.

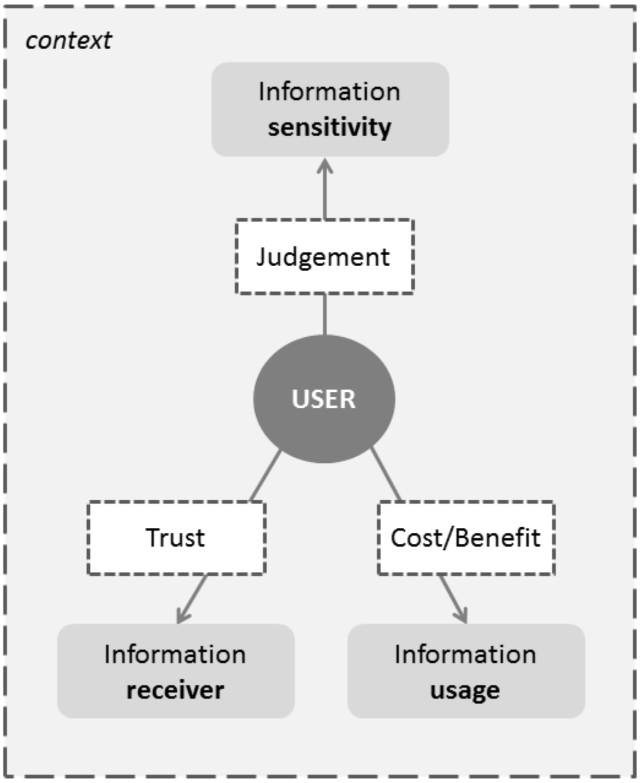


Figure 4 - User's perception privacy model

Based on this model, we can explore how the different components contribute to shape the users' personal representations and attitudes toward privacy.

3.1.1 Information usage: control and awareness

The *information usage* component relates to the users' perception of how and what their transmitted data are used for during data exchange and at a later date.

Perceived risks related to the use of personal information are several: information being used without users' knowledge, information being shared with third parties without users' agreement, identity theft and banking fraud.

> *I want to protect my e-mail account to prevent spam and phishing.*
> [quote from Empathy Map of the student]

Even if the users had not directly experienced security breach, they have heard about this issue through television, radio, newspapers, web, and also through word of mouth when data losses or identity thefts have affected acquaintances and relatives [21].

> *Someone told me that Google tracks data for targeted advertisement.*
> [quote from Empathy Map of the student]
> *I heard rumors about copied credit card and all that sort of things.*
> [quote from Empathy Map of the student]

The ReCRED questionnaire shows that users perceive fraud, forged identity and computer hacking as common phenomena on the web (80%), and half of them don’t feel safe when they release the credit card details on the web.

Security breaches are perceived as more common among the most intensive Internet-using households [19], those who can be considered as heavy users [12].

Even though a majority of users feel responsible themselves for the safe handling of their personal data, just few of them feel in complete control over the information they had disclosed, such as the ability to amend, delete or correct this information [21].

Beyond the perceived control over the personal information on the web, another issue related to privacy is the level of awareness.

ReCRED questionnaire shows that 72% of the respondents are aware about the use of personal information by web sites, and 64% of them know how web sites might use users’ personal information.

According to an European survey [21], over half of Internet users are informed about the data collection conditions and the further uses of their data when registering for a web service. Almost six in ten Internet users usually read privacy statements and the majority of those who read them adapt their behavior on the Internet: they had decided not to use a web service, or had been more cautious about the personal information they disclose through the web service.

But, among the users who read the privacy statements only a third say that they understand them, while a quarter that they read them but do not fully understand them. A quarter say they do not read them, almost one in ten ignore privacy statements, and one in twenty say they do not know where to find them.

> *I am one of the few people who always read the Terms and Conditions before accepting.*
> [quote from Empathy Map of the student]
> *When I register a new account, I don’t read the privacy policies because they are too long.*
> [quote from Empathy Map of the student]

The reasons why some users do not read the privacy statements are several: they think it is sufficient for them to see that websites have a privacy policy; they believe the law will protect them in any case, or conversely, that the websites will not honor the privacy statements anyway [21].

The decision to disclose personal information seems to depend on a cost/benefit analysis [19]: the users must be confident that they have more to gain than to lose [22].

As the cost/benefit analysis regarding information usage by web services plays a key role in the decision-making process, making policies regarding privacy and security easy to locate, read, and enforce is crucial. Although privacy policies are widespread, some are so difficult to find and incomprehensible to read that they only undermine trust [23].

3.1.2 Information sensitivity

Data Protection Directive[8] of the European Union defines “personal data” as any information relating to an identified or identifiable natural person: from the date of birth to the IP address.

[8] Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31)

Every user has a specific perception of which information are sensitive and confidential, and it depends on the context in which the data are exchanged [19].

The information the users consider as personal are, above all, financial information (i.e. salary, bank details, credit card details etc.), medical information, and national identity numbers or cards and passports [21].

The following quotes extracted from the Empathy Map of the students show the critical role of the financial information.

> *Bank account details must be kept safe.*
> [Giovanni - student, quote from interview]
> *I am only worried about my bank account details. I do not care about anything else.*
> [Erica - student, quote from interview]
> *Internet banking is the most important service in terms of security.*
> [quote from Empathy Map of the student]

Worldwide, Internet banking is a growing area among the web services, and financial services across the world are involved in a longstanding battle against fraud, due to the increase of frauds such as phishing where users are tricked into revealing their online banking security details [24].

For online banking users, security and more specifically trust is a highly rated issue.

Considering the relevance of security for this particular service, ReCRED project includes specific scenarios (*Microloan origination* and *Online banking*) which provide increased security for banking environments and they will benefit both the end-user and the financial institution.

3.1.3 Trust toward information receiver

Users’ perception of privacy is also shaped by the trust toward the *information receiver* (not necessarily the actual person, but also organizations) who collects and/or processes the information exchanged [19].

Trust with all its connotations has been studied in numerous disciplinary fields, and it provides important research and design opportunities especially in the context of web service. If the service providers enhance their perceived trustworthiness to potential customers, then the number of people who engage in the services should increase substantially [22].

Interviewed participants have reported that they trust in the university because this kind of information receiver is an institution.

> *I suppose that University staff members can access my account. Since I trust in my University and its staff, I do not care whether they access my account.*
> [Davide – student, quote from interview]
> *The institution guarantees the security of its services.*
> [quote from Empathy Map of the professor]
> *University office has an institutional role that ensures data protection.*
> [quote from Empathy Map of the student]
> *I think that the web services of the university are very reliable.*
> [quote from Empathy Map of the student]

Considering these quotes, they suggest a form of delegation of the responsibility for security to the institution that oversees the reliability of its services, and this implies a strong investment of trust [25].

When the information receiver is a company (i.e. a private organization), trust is connected with its brand identity and reputation: previous experiences, reports from other users and expectations act as antecedents and influence the UX of the service [23].

> *I trust in Amazon simply because it is Amazon.*
> [Donato – student, quote from interview]
> *I trust in Last Pass just because everyone uses it regularly.*
> [Sergio - student, quote from interview]
> *I am always worried about the reliability of the web sites for e-commerce. I use only secure web sites, such as Alitalia and Expedia for booking travels, or Amazon or other big organizations like that.*
> [Barbie - professor, quote from the interview]

Interviewed participants trust web services based on their high reputation as big organizations chosen by millions of users. From the users' point of view, the strong brand reputation guarantees the reliability and fosters the trust [26].

Beyond the identity of the information receiver (as institution, authority or company), there are other factors that affect the perceived reliability and credibility of a service. And these factors need to be considered in designing the ReCRED service that represents an information receiver in itself.

The survey conducted by Fogg and colleagues [26, 27] highlights the importance of web services' credibility that is a perceived quality and it results from evaluating multiple dimensions simultaneously [27].

«Although the literature varies on how many dimensions contribute to credibility evaluations, the vast majority of researchers identify two key components of credibility: trustworthiness and expertise. What this means is that in evaluating credibility, a person makes an assessment of both trustworthiness and expertise to arrive at an overall credibility assessment» [27 p. 80].

The results of that survey [26, 27] suggest the role of the design look as well as the organization and presentation of the information for enhancing the credibility of web services.

The design look (i.e. the elements of the visual design, how the user-interface looks like) represents a peripheral cue that affects the "surface credibility" which describes how much a perceiver believes someone or something based on simple inspection.

But, if the user has the ability and the motivation to further assess the credibility of the web service - we can say, due to the need for privacy and security - other criteria will be used for the assessment.

Thus, the information provided by the service should be well structured, accurate and clear, correct and understandable for users with different levels of skills and knowledge. Considering the contents, the information needs to be useful to understand the functionalities of the service as well as the identity of the service provider.

Moreover, some users tend to evaluate the credibility of a new service based on its performance on a test [26]: if the service doesn't prove to be useful (according to users' goals, intentions and expectations), reliable and credible, then the users will give up.

Indeed, the "experienced credibility" refers to how much a person believes someone or something based on first-hand experience [27], and this means that the first impression plays a fundamental role in determining the UX and the success of the service.

3.1.4 Personas' attitudes and concerns toward privacy

One of the main objectives of the UX research is to identify different groups of users who could be ReCRED potential target users.

Indeed, ReCRED solution is not designed for a unique and generic user. It is addressed to different Personas, to specific users' profiles who differ for their personal attitudes and concerns toward privacy and security on the web.

Such differences in personal representations and preferences become evident when we compare three Personas of the students[9].

Name	**Giovanni**
Profile	27 years old, PhD student of Telecommunications Engineering
Personal quote	*“I tend to keep my stuff private”*
Privacy attitudes	He can be considered as a “privacy fundamentalist” [28]: he is extremely concerned about any use of his personal information and he is generally unwilling to provide his information to web sites, even when privacy protection measures are in place.
Name	**Marco**
Profile	24 years old, graduate engineering student
Personal quote	*“More safety, less effort”*
Privacy attitudes	He characterized by a pragmatist approach: he is concerned about privacy, but his concerns are reduced by the presence of privacy policies on the web sites, and also when the web service is run by a trusted company or organization with a trustworthy brand. Furthermore, he is not concerned about, for example, location-tracking or user profiling as long as he finds the services useful and efficient.
Name	**Susanna**
Profile	25 years old, student of Psychology
Personal quote	*“If they add another safe code, I will go crazy”*
Privacy attitudes	She expresses a mild general concern about privacy. She is generally willing to disclose personal information under almost any condition because she doesn’t consider herself as potential target of fraud. Nonetheless, in some cases she seems to value her privacy, for example related to targeted advertisement and e-mail spam.

Table 4 - Brief description of students’ Personas

Based on the Personas’ characteristics described above, we can discuss how the ReCRED solution can meet the different users’ needs and preferences.

According to his profile, *Giovanni* is aware of his strong security and privacy needs and he also acts to be safe and protected. He could easily recognize the added value of ReCRED that can provide a reliable AC to manage his several online accounts and to feel in control over his personal attributes. Indeed, ReCRED allows the user to define which kinds (or set) of information will be disclosed to web services, within a privacy-preserving framework.

Considering *Marco*’ profile, ReCRED can offer to him not only a reliable and secure solution to access his online accounts, but also a solution to reduce the effort, for example, transferring the identity attributes among services. Furthermore, because he distinguishes between more and less critical services in terms of privacy based on the kind of data they store, ReCRED allows him to define different degrees of privacy among his attributes.

But, the ReCRED solution is not only addressed to expert and informed users as *Giovanni* and *Marco* are. It can be also addressed to the group of users represented by *Susanna*, who has not developed a clear and conscious need for privacy and security yet.

[9] The complete descriptions of Personas are available in the Annex 3 of this document.

So, the attempt to engage non-expert users fostering their need for privacy and security and making them able to understand and use the ReCRED solution in the right way, represents one of the challenges of the project.

3.2.AC systems: from traditional paradigm to innovative approach

The traditional password-based paradigm is still the dominant approach used for AC. Passwords are widely used by and familiar to many people, and are often rated highly in terms of user acceptability [11]. But even the most sophisticated system based on this traditional paradigm becomes useless if users mismanage their password [29].

In the context of the Information Society, where Cloud Computing, Internet-of-Things and Ubiquitous Computing spread, users have to manage a lot of online identities to access different kinds of web services and digital resources.

Most of the users who have answered to the ReCRED questionnaire are heavy users [12]: 55% of the respondents use the web more than 30 hours every week, and 16% about 20-29 hours on a weekly basis; 47% of them manage more than three different e-mail accounts, accessing the accounts frequently or very frequently (87%); 96% of the respondents manage Social Network accounts; more than a half of the respondents use frequently or very frequently different web services (i.e. e-commerce web sites, Internet banking, web service to watch/download movies and videos, to share and store files) during their daily life.

Because most of the web services require the creation of accounts in order to be accessed, the users have to manage several online identities with their specific access credentials. Remembering such a large number of passwords can cause a major problem for users.

In order to cope with the complexity of password management, users develop specific strategies which result in established practices: they select dictionary words or personal names as the basis for their passwords, and they often use the same password for accessing multiple platforms [30].

> *Nowadays everything has username and password, and it is so hard to manage! For example, every scientific journal requires its own specific access credentials, and over the years I tend to lose them. So, what is my strategy? When it is possible, I tend to use the same username and two alternative passwords.*
> [Barbie – professor, quote from interview]

Despite most of the users know the security practices related to both the password’s contents (i.e. alphanumerical characters) and its management (i.e. memorized and not written down, often changed passwords), they seem to tend toward convenience more than security [29].

> *I know that simple passwords are less safe than complex ones, but I use them anyway. Passwords must be easy to remember.*
> [Federico – professor, quote from interview]

Users seem to be motivated to engage in risky password practices for two main reasons: to reduce the effort using easy-to-remember access keys, and also because they do not see any immediate negative consequence to themselves. In other words, they believe that negative events, such as identity theft and fraud, are less likely to happen to them [31].

According to the results of the ReCRED questionnaire, about 54% of the users are not afraid of security breaches because they don’t consider themselves as persons at risk.

Using the label proposed by Weinstein [32], we can define this common phenomenon as “unrealistic optimism”. Although it has not been empirically assessed regarding virtual events using Internet, this optimistic bias represents a useful concept to clarify the reason why users - who have concerns about privacy on the web - persist in engaging in risky behaviors.

If someone feels that it is unlikely that anything negative will happen to him/her, then he/she may engage in more risky behaviors and/or not take reasonable precautions to protect him/herself from harm [12].

Considering the different risky practices in password management, the need for innovative AC systems becomes an overriding concern, supporting the objective of the ReCRED project.

Based on the users' behaviors described in the Mental Model, it is easy to highlight that the tasks performed by the users to accomplish the goals "Register a new account", "Preserve credentials" and "Login to the account" are several, they require effort and some of them also represent risky behaviors (such as the use of a unique password among different platforms).

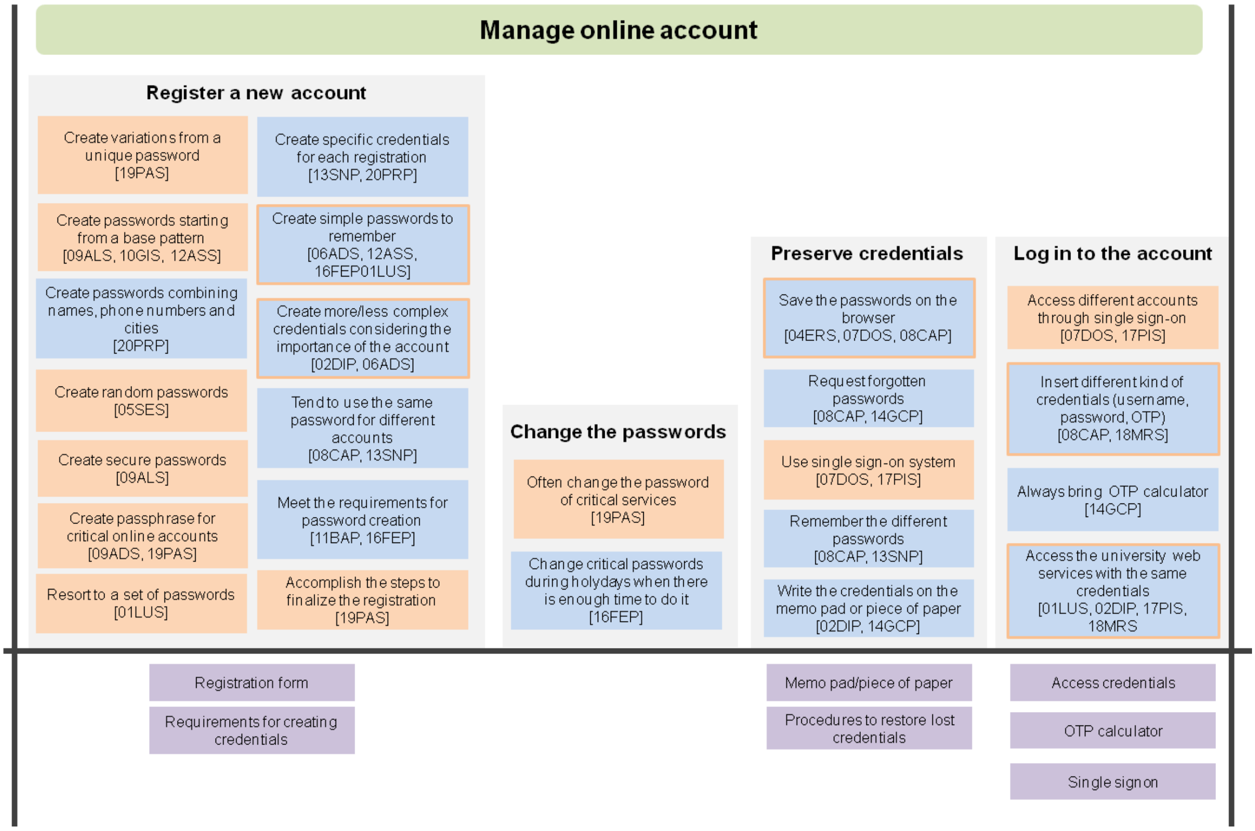

Manage online account
Register a new account
Create variations from a unique password [19PAS]
Create specific credentials for each registration [13SNP, 20PRP]
Create passwords starting from a base pattern [09ALS, 10GIS, 12ASS]
Create simple passwords to remember [06ADS, 12ASS, 16FEP01LUS]
Create passwords combining names, phone numbers and cities [20PRP]
Create more/less complex credentials considering the importance of the account [02DIP, 06ADS]
Create random passwords [05SES]
Tend to use the same password for different accounts [08CAP, 13SNP]
Create secure passwords [09ALS]
Meet the requirements for password creation [11BAP, 16FEP]
Create passphrase for critical online accounts [09ADS, 19PAS]
Resort to a set of passwords [01LUS]
Accomplish the steps to finalize the registration [19PAS]
Change the passwords
Often change the password of critical services [19PAS]
Change critical passwords during holydays when there is enough time to do it [16FEP]
Preserve credentials
Save the passwords on the browser [04ERS, 07DOS, 08CAP]
Request forgotten passwords [08CAP, 14GCP]
Use single sign-on system [07DOS, 17PIS]
Remember the different passwords [08CAP, 13SNP]
Write the credentials on the memo pad or piece of paper [02DIP, 14GCP]
Log in to the account
Access different accounts through single sign-on [07DOS, 17PIS]
Insert different kind of credentials (username, password, OTP) [08CAP, 18MRS]
Always bring OTP calculator [14GCP]
Access the university web services with the same credentials [01LUS, 02DIP, 17PIS, 18MRS]
Registration form
Requirements for creating credentials
Memo pad/piece of paper
Procedures to restore lost credentials
Access credentials
OTP calculator
Single sign on

Figure 5 - Mental space for managing online account

In conclusion, the UX will be positively affected by the implementation of the ReCRED solution: the UX will be simplified and it will make the users’ online accounts safer and more protected, even if they are not aware of this fundamental need for security and privacy.

Moreover, the implementation of the ReCRED identity management system can also benefit the users (and the service providers too) reducing a particular strategy that the users might apply to protect their identity: the creation of fake online profiles.

Indeed, some interviewed participants have reported that sometimes they create fake online profiles, not with the purpose of cheating someone else, but in order to avoid revealing their real identity and disclosing their personal information, as a sort of anonymity and concealed identity.

Considering the case of a web service that requires age verification to access its contents, thanks to ReCRED solution the users will not need to reveal their complete identity or other critical information (such as the credit card details) but only their age, and the information exchanged is cryptographically secured and preserves the anonymity of the users.

3.2.1 Users’ attitudes and concerns toward biometric factors

The use of biometrics, the automatic personal recognition based on physiological or behavioral characteristics is emerging as the innovative solution for reliable and secure authentication mechanism, both in public and private sectors [30].

To make a personal recognition, instead of something the user knows such as the password, biometric authentication relies on something the user is (in the case of physiological characteristics) or does (behavioral traits) [33].

Compared with the password-based paradigm, implementing biometric recognition to identity management and AC has several advantages for the end-users as well as for the service providers: it can guarantee that only the end-user who is the owner of the account can access and modify personal information, ensuring to the service provider that only authorized users can access the service and the resources it provides [34].

When designing a biometric system for AC, in addition to the requirements of accuracy, speed and reliability against fraudulent methods and attacks, users’ attitudes and concerns need to be considered.

«Biometric technologies are not without problems and come with their fair share of concerns. Some of these concerns are technical in nature, e.g. degradation of biometric features over time, variance in recorded and actual biometric characteristics, and threshold values for authentication. As the technology matures, however, the technical issues will be eventually overcome. On the other hand, many of the technology’s obstacles are based on attitudes and behaviors, related to user acceptance, trust, habits, etc., ultimately presenting a greater challenge for implementation» [35, p.115]

The issue of user acceptance is possibly the most difficult to assess, because it represents a highly subjective measure [30]. The perceived ease of use as well as the perceived usefulness and the perceived need for security are important determinants of user acceptance of biometric authentication [36].

According to the studies conducted to explore users’ acceptance of biometrics, it is linked to the familiarity with such technology. It seems that only few people really understand the technical details or have an extensive experience using biometrics for identity verification, and this lack of familiarity seems to affect users’ attitudes [35].

The perceived trust affects users’ appreciation of biometrics and the main users’ concern is related to the robustness against attacks and the misuse of personal information through the theft of the templates [37].

> *Once I obtain the digital file of the biometric factors of one person, I am that person, and the contrary is hard to prove.*
> [Fabrizio - professor, quote from interview]

Another concern connected with the use of biometric devices is related to hygiene (i.e. touching such devices for scanning fingerprint) and health risks for more advanced technologies such as iris or retina, despite none paper highlighted physical harm to users of these systems [37].

The invasion of privacy is another concern reported by users who think that the use of some systems represents an intrusion into daily life [35].

> *Sensitive data that could represent a problem are those connected with the phone calls I make, the web sites I visit, I mean all the information that track my daily activities.*
> [Fabrizio - professor, quote from interview]

Because misinformation seems to affect users’ general attitudes toward biometrics [10], the ReCRED solution should be transparent and clear, and comprehensive information should be provided in order to inform users regarding the potential of biometrics [38].

«More than anything, generating interest in the topic seems to be a suitable vehicle for improvement in the area of general familiarity, as well as better technical understanding of the subject. Through a better comprehension of the technology, better informed users will be able to achieve a sense of comfort while using it, as well as deeper appreciation for the benefits it provides. A sound understanding of the basic operation will also go a long way towards eliminating apprehensions about privacy issues that are today perceived as one of the inhibiting factors in adoption» [35, p.118].

3.2.2 Design issues

The UX research has been carried out in order to collect opinions from target users about ReCRED design concept: a device-centric AC solution that enables the users to authenticate using short pins, biometrics or combinations.

Interviewed participants appreciate this solution, because it can solve the main problem of the current password-based AC: the password overload.

> *Biometric authentication could be really useful because there is no more need to keep in mind different codes and passwords.*
> [Marta - student, quote from interview]
> *Multifactor authentication should be faster than “classical” log in, thus better.*
> [Adriano- student, quote from interview]
> *Biometric factor is personal, so it is secure. Beside I think that impregnable technology doesn't exist, over the years my accounts increase, so the idea of the unique access credential can help*.
> [Piero - student, quote from interview]

Beside this positive impact of the ReCRED solution on the UX, interviewed users have pointed out a fundamental issue that deals with the device-centric mechanism. As reported in the following quotes, the users wonder about the security mechanism that ReCRED could guarantee if the mobile phone is stolen, lost or damaged.

> *Based on my experience, the critical aspect of the smartphone is connected with the fact that it is “volatile”, I mean it can be easily lost, stolen or broken*.
> [Carlo - professor, quote from interview]
> *Smartphones and portable devices might be easily lost. What will happen next?*
> [Adriano- student, quote from interview]

This design issue has been considered and specific scenarios for the mobile device data protection have been described in Deliverable 2.1 “Business cases”.

Name	*Stolen Mobile Phone*
Author/Partner	TID
Stakeholders	Mr. Jones (mobile phone user)
High Level Description	Mr. Jones is a keen user of online services and tech-savvy software engineer who works for an established software company. Mr. Jones has a lot of work and is distracted during traveling in the public transport by thinking about a new algorithm he has to implement and deliver in less than five hours. He did not notice that Mr. Badbob has stolen his mobile phone out of the notebook case and found it out on the subway platform. Instead of freaking out, Mr. Jones quietly admits he should have paid greater attention to his belongings and start thinking about a new mobile phone. There is no need to search a nearest computer to log in to different online services and change passwords – ReCRED authentication on the mobile phone keeps him calm because he knows nobody would be able to access his accounts without triggering a global lock on all his online services accounts.
Issues & Benefits	- Mr. Jones knows that thanks to ReCRED none of his online accounts could be accessed. While Mr. Badbob tries to log in to Mr. Jones’ Amazon account, it is recognized from its unexpected user’s location, network traffic and typing pattern that the mobile phone is possessed by a different user and a global lock is applied on all online service accounts. Mr. Badbob does not succeed while Mr. Jones knows that he can visit his ReCRED account web page and see the services blocked by ReCRED. Some of those services he does not even remember and is glad there is a list of them and those services have been locked too. - Mr. Jones knows from his ReCRED profile when and where the global lock has been applied so he can give the Police better information about where he was robbed. It will be harder for Mr. Badbob to steal from people in that area again.

Table 5 - Stolen mobile phone scenario

Another design issue raises from the analysis of users’ practices in managing online identities: in some situations, users delegate to trusty people (relatives, friends or colleagues) the use of web services, authorizing the access with personal credentials. This happens as exceptional case but also as a habit [29].

> *I have asked a reliable colleague to sign me up for a conference, giving to him my credentials and the codes of my credit card, but only because he is trustworthy.*
> [Federico - professor, quote from interview]
> *Since I am not at home so often, I get used to ask my parents to buy on Amazon.*
> [Alessandro - student, quote from interview]
> *I often use web services on behalf of my parents, such as online purchase or internet banking, if they can’t do it by themselves or when they need to learn how to use such services. Potentially, I can access all the accounts of my parents because I know their passwords, but I do it only when they ask me to do it.*
> [Piero - student, quote from interview]

This form of delegation represents an open design issue that could be addressed in the further discussion about the implementation of ReCRED solution into real users’ practices.

4. Conclusion

The ReCRED project includes a qualitative investigation of the HCI issues involving potential target users from the first pilot (*Campus-wide WiFi and web services access control*), in order to inform the design process with useful insights gained from a deep understanding of the users’ point of view.

In the perspective of HCI, there has been an underlying assumption that because humans are so inherently flexible and adaptable, it is easier to let them adapt themselves to a new system or service [39].

On the contrary, within ReCRED project we adopt the user-centred approach that places the user at the center of the design process [40]: our attempt is to develop a solution that is adapted to the target users’ needs, preferences and concerns.

The objective of the research carried out is the investigation of the User Experience with a particular focus on the problems and obstacles the users face in managing their online accounts.

In the Information Age, the spread of web services causes a growth of the online identities that the users have to manage during their daily life. But, not all the users have the motivation, the skills or even the time to deal with privacy and security issues and to cope with the problems of the traditional paradigm of AC that is based on passwords.

According to the results of the UX research and to the findings of several studies conducted in the field of HCI, we can understand that users tend to apply risky practices (i.e. the use of a unique easy-to-remember password to access different accounts) due to the convenience of such strategies [29] and because they don’t see any immediate consequence to themselves [31].

In fact, despite most of the users know about fraud, computer hacking and other malicious events on the web, every user has a personal representation of privacy and a specific need for security.

There are the “privacy fundamentalists” [28] who are extremely concerned about any use of their data and generally unwilling to provide their data to web sites. They are informed and prudent users who care about privacy and who have the skills and the knowledge to evaluate the reliability of a service. But there are also people who are not so skilled and aware of possible risks and strategies to prevent them.

This fundamental understanding of the UX means that the ReCRED solution cannot be addressed to a unique user, but to different users’ profiles (both expert and non-expert) and it can offer to each of them specific benefits, providing an innovative and satisfying UX.

In conclusion, the UX research discussed in this Deliverable tends to validate the ReCRED design concept according to the needs and the attitudes of the potential users.

The next step will be the evaluation of the ReCRED solution as it will be implemented in the pilot sites, involving actual users of the pilots in test sessions to assess the usability of the ReCRED service and its interfaces[10].

[10] The large-scale demonstration of the pilots and the results of the assessment will be reported in the Deliverable 7.4 “All pilots in operation and end user assessment report”.

5. References

[1] Abras, C., Maloney-Krichmar, D., & Preece, J. (2004). User-centered design. *Bainbridge, W. Encyclopedia of Human-Computer Interaction. Thousand Oaks: Sage Publications*, *37*(4), 445-456.

[2] Alben, L. (1996). Defining the criteria for effective interaction design. *interactions*, *3*(3), 11-15.

[3] Bannon, L. (1991). From human factors to human actors: The role of psychology and human-computer interaction studies in system design. Design at work: Cooperative design of computer systems, 25-44.

[4] Norman D.A. (2004), Emotional design. Why we love (or hate) everyday things, Basic Book, New York.

[5] Strauss, A., & Corbin, J. (1990). *Basic of qualitative research*. SAGE Publications, CA.

[6] Silverman, D. (2015). *Interpreting qualitative data*. Sage.

[7] Zucchermaglio, C., Alby, F, Fatigante, M., & Saglietti, M. (2013). Fare ricerca situata in psicologia sociale. Il mulino.

[8] Fisher, R. P., & Geiselman, R. E. (1992). *Memory enhancing techniques for investigative interviewing: The cognitive interview*. Charles C Thomas Publisher.

[9] Udo, G. J. (2001). Privacy and security concerns as major barriers for e-commerce: a survey study. *Information Management & Computer Security*, *9*(4), 165-174.

[10] Moody, J. (2004). Public perceptions of biometric devices: The effect of misinformation on acceptance and use. *Journal of Issues in Informing Science and Information Technology*, *1*, 753-761.

[11] Jones, L. A., Antón, A. I., & Earp, J. B. (2007, October). Towards understanding user perceptions of authentication technologies. In *Proceedings of the 2007 ACM workshop on Privacy in electronic society* (pp. 91-98). ACM.

[12] Campbell, J., Greenauer, N., Macaluso, K., & End, C. (2007). Unrealistic optimism in internet events. *Computers in Human Behavior*, *23*(3), 1273-1284.

[13] Gray, D., Brown, S., & Macanufo, J. (2010). *Gamestorming: A playbook for innovators, rulebreakers, and changemakers*. " O'Reilly Media, Inc.".

[14] Cooper, A., Reimann, R., Cronin, D., & Noessel, C. (2014). *About Face: The essentials of interaction design*. John Wiley & Sons.

[15] Constantine, L. (2006). Users, roles, and personas. *The Persona Lifecycle*, 498-519.

[16] Engeström, Y. (2000). Activity theory as a framework for analyzing and redesigning work. *Ergonomics*, *43*(7), 960-974.

[17] Bannon, L. J., & Bødker, S. (1989). Beyond the interface: Encountering artifacts in use. *DAIMI Report Series*, 18(288).

[18] Young, I. (2008). *Mental models: aligning design strategy with human behavior*. Rosenfeld Media.

[19] Adams, A. (2000), Multimedia Information Changes the Whole Privacy Ballgame*, Proceedings of the tenth conference on Computers, freedom and privacy*, 25-32.

[20] Goldberg, R. “Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities”, NTIA Blogpost, May 2016 https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities

[21] Eurobarometer, S. (2011). Attitudes on data protection and electronic identity in the European Union. http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

[22] Wang, Y.D., Emurian, H.H. (2005), An overview of online trust, *Computers in Human Behavior*, 21, 105-125.

[23] Shneiderman, B. (2000), Designing Trust into Online Experiences, *Communication of the ACM*, 43 (*12*), 57-59.

[24] Nilsson, M., Adams, A., & Herd, S. (2005, April). Building security and trust in online banking. In *CHI'05 Extended Abstracts on Human Factors in Computing Systems* (pp. 1701-1704). ACM.

[25] Dourish, P., Grinter, R. E., De La Flor, J. D., & Joseph, M. (2004). Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8(6), 391-401.

[26] Fogg, B. J., Soohoo, C., Danielson, D. R., Marable, L., Stanford, J., & Tauber, E. R. (2003, June). How do users evaluate the credibility of Web sites?: a study with over 2,500 participants. In *Proceedings of the 2003 conference on Designing for user experiences* (pp. 1-15). ACM.

[27] Fogg, B. J., & Tseng, H. (1999, May). The elements of computer credibility. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems* (pp. 80-87). ACM.

[28] Ackerman, M. S., Cranor, L. F., & Reagle, J. (1999, November). Privacy in e-commerce: examining user scenarios and privacy preferences. In *Proceedings of the 1st ACM conference on Electronic commerce* (pp. 1-8). ACM.

[29] Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience. *Behaviour & Information Technology*, 29(3), 233-244.

[30] Furnell, S. M., Dowland, P. S., Illingworth, H. M., & Reynolds, P. L. (2000). Authentication and supervision: A survey of user attitudes. *Computers & Security*, *19*(6), 529-539.

[31] Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 3-7.

[32] Weinstein, N. D. (1980). Unrealistic optimism about future life events. *Journal of personality and social psychology*, *39*(5), 806.

[33] Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric recognition: Security and privacy concerns. *IEEE Security & Privacy*, (2), 33-42.

[34] Fu et al. (2001), Dos and Don'ts of Client Authentication on the Web. In *USENIX Security Symposium*, pp. 251-268.

[35] Pons, A. P., & Polak, P. (2008). Understanding user perspectives on biometric technology. *Communications of the ACM*, *51*(9), 115-118.

[36] Deane, F., Barrelle, K., Henderson, R., & Mahar, D. (1995). Perceived acceptability of biometric security systems. *Computers & Security*, *14*(3), 225-231.

[37] El-Abed, M., Giot, R., Hemery, B., & Rosenberger, C. (2010, October). A study of users' acceptance and satisfaction of biometric systems. In *Security Technology (ICCST), 2010 IEEE International Carnahan Conference on* (pp. 170-178). ieee.

[38] Elliott, S. J., Massie, S. A., & Sutton, M. J. (2007, June). The perception of biometric technology: A survey. In *Automatic Identification Advanced Technologies, 2007 IEEE Workshop on* (pp. 259-264). IEEE.

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

[40] Garrett, J.J. (2011). *The elements of user experience: User centered design for the web and beyond*, New Riders, San Francisco, CA.

Annex 1 - Questionnaire

Questionnaire about privacy and security on the web

Please, read carefully in order to give your informed consent

The aim of this questionnaire is to collect data about users' attitudes and opinions regarding privacy and security on the web.
We invite you to complete the questionnaire that requires about 10 minutes.
Your participation is totally voluntary; you can decide not to complete the questionnaire without any consequence.
Your anonymity will be safeguarded, and all the data collected through this questionnaire will be elaborated for research purposes, and used in scientific publications and conferences.

✓ I Agree

1.	Age	*[text]*
2.	Nationality	*[text]*
3.	Occupation	*[text]*
4.	Field of work/study	*[text]*
5.	Educational qualification	*[text]*
6.	Weekly Internet usage	○ 0-4 hours ○ 5-9 hours ○ 10-19 hours ○ 20-29 hours ○ More than 30 hours ○ Rather not say
7.	How many e-mail accounts do you have?	○ None ○ One ○ Two ○ Three ○ More than three
8.	What kind of e-mail account do you manage?	○ Personal ○ Work ○ University ○ Other *[text]*
9.	How often do you use your e-mail account?	Never (1) - (2) - (3) - (4) - (5) Very frequently
10.	Which Social Network do you use?	○ None ○ Facebook ○ LinkedIn ○ Google+ ○ YouTube ○ MySpace ○ Instagram ○ Twitter ○ Other *[text]*
11.	How often do you use social network?	Never (1) - (2) - (3) - (4) - (5) Very frequently
12.	How often do you use web services to storage and/or share files with other users?	Never (1) - (2) - (3) - (4) - (5) Very frequently
13.	How often do you use Internet banking?	Never (1) - (2) - (3) - (4) - (5) Very frequently
14.	How often do you use e-commerce services for online shopping?	Never (1) - (2) - (3) - (4) - (5) Very frequently
15.	How often do you use web services to book flight, hotel and/or travels?	Never (1) - (2) - (3) - (4) - (5) Very frequently
16.	How often do you participate in forum for	Never (1) - (2) - (3) - (4) - (5) Very frequently

	online discussion?	
17.	How often do you use web services to watch and/or download videos/movies?	Never (1) - (2) - (3) - (4) - (5) Very frequently
18.	Do you use password manager application? *It is a software application that stores and organizes encrypted passwords, so you use a single master password to access the entire password database.*	○ Yes ○ No

19. For each of the following statements, select the option that reflects your agreement/disagreement

Strongly disagree (1) - Disagree (2) - Undecided (3) - Agree (4) - Strongly Agree (5)

When I surf the web, I am aware about the use of my personal information by web sites	(1) - (2) - (3) - (4) - (5)
I know how web sites might use my personal information	(1) - (2) - (3) - (4) - (5)
I know the policies which regulate the processing of my personal information	(1) - (2) - (3) - (4) - (5)
The security of my online account is a fundamental issues	(1) - (2) - (3) - (4) - (5)
Security and privacy concerns are barriers for the use of web services	(1) - (2) - (3) - (4) - (5)
Fraud and impersonation are common on the web	(1) - (2) - (3) - (4) - (5)
Computer hacking is a common phenomenon	(1) - (2) - (3) - (4) - (5)
Privacy of web users is greatly violated	(1) - (2) - (3) - (4) - (5)
I am afraid of security breach because I consider myself as a person at risk	(1) - (2) - (3) - (4) - (5)
I am afraid of security breach because my online accounts are not sufficiently protected	(1) - (2) - (3) - (4) - (5)
Despite all the safety precautions in place today, the web is not safeguarded enough	(1) - (2) - (3) - (4) - (5)
The current laws and regulations are sufficient for protecting users' personal information	(1) - (2) - (3) - (4) - (5)
The current security features such as encryption and passwords are sufficient to provide security and safety on the web	(1) - (2) - (3) - (4) - (5)
I feel safe when I release my credit card details on the Internet	(1) - (2) - (3) - (4) - (5)
I trust in the safety precautions of Internet banking	(1) - (2) - (3) - (4) - (5)

20. How often do you comply with the following security precautions?

Never (1) - Rarely (2) - Occasionally (3) - Frequently (4) - Very frequently (5)

Use complex passwords including numbers, letters and/or special characters	(1) - (2) - (3) - (4) - (5)
Often change the passwords to access online accounts	(1) - (2) - (3) - (4) - (5)
Use a specific password for each online account	(1) - (2) - (3) - (4) - (5)
Avoid disclosing to others the personal credentials to access online accounts	(1) - (2) - (3) - (4) - (5)
Read carefully the privacy policies before accepting their conditions	(1) - (2) - (3) - (4) - (5)
Avoid disclosing personal information when it is not strictly needed	(1) - (2) - (3) - (4) - (5)

21. For each of the following statements, select the option that reflects your agreement/disagreement

Biometrics refers to physiological or behavioral metrics used as form of personal identification and access control (i.e. fingerprint scan, voice/face recognition etc.)

Strongly disagree (1) - Disagree (2) - Undecided (3) - Agree (4) - Strongly Agree (5)

The use of biometric factors by web services represents an invasion of privacy	(1) - (2) - (3) - (4) - (5)
Biometric factors are more secure than passwords	(1) - (2) - (3) - (4) - (5)
Biometric factors make web services logons faster and more reliable	(1) - (2) - (3) - (4) - (5)
When people are asked to provide their biometric identifiers, they should be fully informed about the intended use	(1) - (2) - (3) - (4) - (5)
I am concerned that someone else might use my biometric identifier to commit fraud	(1) - (2) - (3) - (4) - (5)

22. It will be useful the use of biometrics for identity verification...

Not likely (1) - Somewhat likely (2) - Very likely (3)

To unlock the smartphone	(1) - (2) - (3)
To login to social network	(1) - (2) - (3)
To access my e-mail account	(1) - (2) - (3)
To conduct financial transactions on the web	(1) - (2) - (3)
To purchase from an online retailer	(1) - (2) - (3)

To access web services that require age verification	(1) - (2) - (3)
To connect to university/company WiFi	(1) - (2) - (3)

Your response has been recorded. We really appreciate your collaboration

Annex 2 - Empathy Maps

Empathy Map	**user role: *student***
DO	**SAY**
I use campus WiFi during the lectures to find further information. [18MRS]	I can create a fake account that, if it is hacked, it will not cause damage. [CL01]
I use campus WiFi both for didactic purposes and entertainment, during the breaks between lectures. [04ERS, 07DOS, 12ASS,17PIS]	I don’t waste time reading privacy policies, because I don’t care about them and I always accept their conditions. [AM11]
I avoid using the campus WiFi for accessing services or web sites which store my sensitive data. [04ERS, 17PIS]	I always click on “accept” (the Terms and Conditions). [FR05]
I manage more than three e-mail accounts [CL01, GC06, FR05, GV07]	I am one of the few people who always read the Terms and Conditions before accepting their conditions. [CL01]
I log in to my e-mail account every day [CL01, LG02, FR05, GC06]	I know the data exchanged through the web could be tracked. [03DAS]
I use the e-mail provided by the university to communicate with professors and university staff. [01LUS, 18MRS]	I am aware of the possible use of my personal information, but I don’t pay attention to this issue, I don’t consider it. [FR05]
For accessing the e-mail account, I have to log in to the university web portal. [07PIS]	The level of security I demand is based on the confidentiality of the stored data. [06ADS]
I use the e-mail provided by the university as secondary, and my personal account as the main. [17PIS]	I consider useless to have high level of security to protect something futile, also producing a waste of energy, while most important services are less reliable. [09ALS]
I don’t need the university e-mail, I use my personal account. [03DAS, 12ASS]	Internet banking is the most important service in terms of security. [03DAS, 04ERS, 06ADS, 07DOS, 12ASS]
I often use the library web service for bibliographic research. [17PIS, 18MRS]	The advantage of using a unique password for different accounts is that you can always remember it; but if it is uncovered, it will be used to access several accounts. [18MRS]
I use the university web portal to gain information about professors and exams, download lecture materials and exercises. [04ERS, 17PIS]	The password manager application doesn’t inspire confidence, but anyway it is useful. [07DOS]
I use e-learning platform for attending online courses. [01LUS]	If they add another safe code, I will go crazy. [19PAS]
I use the university web portal when I need to search an exam and enroll. [04ERS, 06ADS, 07DOS, 09ALS, 12ASS, 17PISS, 18MRS]	I have never change the password of my university account because I think that the web services of the university are very reliable. [09ALS]
I use Social Network every day. [LG02, DN04]	I don’t know what encryption means. [GV07]
I am member of five different Social Networks	I don’t think that someone would steal my data

[CL01]	because I am a small fry [AM11]
I use the university web platform to download software. [17PIS]	**PAIN**
I use file sharing, as well as cloud and e-commerce services. [19PIS, 18MRS]	I often use campus WiFi, even if it hasn't a valid certificate. [09ALS]
Through the online banking service, I can check the final outstanding balance of my prepaid card and use other functions. [04ERS, 06ADS, 18MRS]	Campus WiFi is terrible, because every time I have to reconnect (authenticating with the credentials) even if I want to see something just for a minute. [06ADS, 09ALS, 12ASS]
I don't purchase products online. [LG02, VR08]	Remembering the passwords and managing all the accounts is hard. [04ERS, 17PIS]
I use web services to book travels or products. [LG02, DN04, GC06]	I can't remember the passwords, I lose them over and over again. [19PAS]
I access the university web services with the same credentials. [01LUS, 07DOS, 17PIS, 18MRS]	Recently, the university web platform requires alphanumerical password. [19PAS]
I choose among four main passwords covering different levels of complexity, based on the security level I want to assign to each web service. [06ADS]	I have met some problems recovering my university e-mail account because I didn't remember the credentials. [09ALS]
I try to meet the requirements for password creation. [03DAS]	When I try to access to web services I haven't used for years, I can't remember the password so I need to change it. [01LUS]
There is a secondary password I use for less important accounts. [19PAS]	After the third attempt to find the code of the credit card, the system blocks it. [19PAS]
I use phrase as password for the most critical web services in terms of reliability. [06ADS]	The credentials required for accessing my personal area on the train service web site are not clear. [18MRS]
I create similar passwords so to memorize them. [07DOS]	I don't use the Internet banking because I can't remember the password. [VR08]
When I need to create a new password, I combine a regular pattern with the name of the service or the web site. [09ALS]	Some systems are frustrating because you have to remember three passwords and accomplish ten steps for the registration. [19PAS]
I create variations starting from a single password pattern. [19PAS, FR05]	The more the web service is secure, the less usable it is. [CL01]
I try to use some patterns when I create a new password. [04ERS, 09ALS, 12ASS]	Having all the passwords stored in a single service increases the risk, because accessing that service allows to access all the other services. [17PIS]
I use alphanumerical passwords which are specific for each web service. [12ASS]	Saving the passwords on the browser is not secure, because someone using your pc can easily gain the credentials. [07DOS, 04ERS]
I don't change the password for accessing my online accounts [FR05]	My e-mail account is critical because you can recover all my credentials from it. [17PIS]

I use *single sign-on* service. [07DOS]	If I lose my smartphone, it will be a big problem. [06ADS]
I write the password on a piece of paper. [04ERS, 09ALS]	Accessing improperly to my university account, you can manipulate the information. [12ASS]
I make the registration to use web services only when it is strictly needed. [GC06]	I never feel safe when I release my credit card details on the web. [FR05]
I use a specific password for *Facebook*, so if it is hacked, it will be valid only for that account. [06ADS]	There are a lot of scam on the web. [GC06]
I use the web for planning and booking travels on behalf of my uncle. [17PIS, 18MRS]	Fraud is a common phenomenon on the web, but you don’t meet it every day. [CL01]
I use Internet banking on behalf of my parents. [17PIS]	I don’t know the policies which regulate the processing of personal information. [DN04, FR05]
I often share my credentials with my best friend. [19PAS]	I don’t read the privacy policy because it is too long. [VL03]
I gave my credentials to friends when they needed to use the campus WiFi. [04ERS, 09ALS, 12ASS]	**THINK**
I use my father’s credit card and *PayPal* account. [19PAS]	I don’t consider my academic information as sensitive data to protect. [01LUS, 09ALS, 19PAS]
As pastime, I sniff network traffic via campus WiFi network. [03DAS, 06ADS]	I think that fraud will not happen to me. [DN04]
I have used the university account just one time to have a software licence for student. [09ALS]	University office has an institutional role that ensures data protection. [18MRS]
In order to avoid disclosing my personal information, I have created a fake profile. [FR05]	Considering Internet banking service, it seems that the security is guaranteed. [18MRS]
SEE	**HEAR**
I see “Certified by Visa”. [GC06]	Someone told me that Google tracks data for targeted advertisement. [18MRS]
I see the padlock on the browser that indicates the secure mode. [LG01]	Sometimes my mother asks me to log in to her e-mail in order to find some information. [18MRS]
I saw some vending machines using finger prints to verify the age of the person who wants to buy cigarettes. [18MRS]	My friend has asked me to use my credentials to access the university web portal. [01LUS]
I saw the university officer accessing students’ data using his own credentials. [01LUS, 18MRS]	I heard rumors about copied credit cards and all that sort of things. [19PAS]
I saw the announcement saying that Internet connection of the totem at the university is not secure. [06DAS]	**GAIN**
FEEL	I receive *Facebook* notification when it is accessed from a device that is not my pc.

	[19PAS]
I am not worried about possible risks when I surf the web. [FR05]	I use the university mobile application that saves the campus WiFi password, so I don’t have to insert it every time I want to connect. [07DOS]
University mobile application worries me because I don’t know whether it is secure. [07DOS]	I try to use the same password so to remember it. [01LUS, 18MRS]
I am so bored and annoyed when I have to re-connect after the session is expired. [12ASS]	I use *single sign-on* and I trust of it because of its high reputation. [17PIS]
	Single sign-on is essential for me. [06ADS]
	The use of biometric factors is so useful because you don’t have to remember or change a code. [07DOS, 18MRS]
	I used to load my prepaid card only with a preset sum of money for buying something online. [01LUS, 07DOS]
	I want to keep private just few things, and I am careful about them. [03DAS]
	I don’t need to have all the web services reliable, I need security just for those which are more important for me. [09ALS]
	I want to protect the academic information stored in the university web portal. [12ASS]
	I would like some further procedures to protect my sensitive data. [09ALS]
	I need different levels of authentication using biometric factors so to better protect my accounts. [06ADS]
	I want to protect my e-mail to prevent spam and phishing. [12ASS]
	It is essential to avoid time consuming steps (required by web services to accomplish the registration). [06ADS]
	I need the possibility to delegate to others the use of some web services. [19PAS]

Empathy Map	**user role: *professor***
DO	**SAY**
I change the passwords in specific periods, during the holydays, when I have enough time to do it. [16FEP]	I know that simple passwords are less safe than complex ones, but I use them anyway. [16FEP]
As usual, I save the passwords on the browser, because it’s hard to remember them. [08CAP]	It will be a great advantage if they abolish all the passwords. [11BAP]
For creating a password, I combine names, cities, places and phone numbers. [20PRP]	The complexity of the passwords ranges based on the data to protect. [02DIP]
I use a specific password for every web service, not the same. [13SNP, 20PRP]	The web services must reduce the effort required to the users. [14GCP]
If necessary, I give my credentials to reliable colleagues for the conference registration. [16FEP]	I do almost everything entirely online, in fact I use so much web services. [11BAP]
I share the credentials to access e-learning platform with another professor who hold the same course. [08CAP]	The level of security of web services should be appropriate on the basis of the possible risks. [14GCP]
It happened that some colleagues logged in to the university web services using my credentials. [02DIP, 20PRP]	I am responsible for my institutional work. [11FEP]
Sometimes, I help relatives and friend to buy something online. [13SNP]	I have no idea of what the laws define as “sensitive data” [20PRP]
I prefer to use the WiFi connection of my lab that works better than campus WiFi. [08CAP, 16FEP]	**GAIN**
When I am in my room at the university I use the cable internet connection, while when I am around the building I use WiFi connection. [20PRP]	I use web services of serious organizations and brands. [11BAP]
I use the e-mail provided by the university not only for working, but also for personal communication. [13SNP]	I use the credit card for online shopping without anxiety because I trust of encrypted code. [20DIP]
I use the e-mail provided by the university every day and regularly, as main account. [02DIP, 08CAP, 11BAP, 20PRP]	The institution (university) guarantees the security of its services. [11BAP, 16FEP]
I use the e-learning platform of my department to distribute lecture materials and exercises to the students. [20PRP]	I need to be sure that the web services I use are reliable. [11BAP]
I regularly use the library web service, both in my office and at home. [02DIP, 20PRP]	I consider positively the use of biometric factors for authentication. [14GCP]
I use the university web portal every day. [14GCP]	The fingerprint is not enough to ensure security, I need different and integrated biometric factors. [14GCP, 20PRP]
I often use online banking and file sharing service. [02DIP, 08CAP, 14GCP, 20PRP]	Passwords must be easy to remember. [16FEP]
I use *PayPal* and prepaid card for online shopping. [20PRP]	I would like to have only one small keyring fob device for different services. [14GCP]

PAIN
If I need technical assistance for my cellphone, the problem will be that I will backup and then restore. [08CAP]
The university web portal is uncomfortable because, like the web site of the bank, it requires OTP for every action I want to do. [14GCP]
Managing the three credentials (username, password, OTP) of online banking is not easy. [20PRP]
Every scientific journal site requires its own credentials. [11BAP]
The problem arises because I have to remember passwords of different accounts. [13SNP]
It is hard to manage different passwords. [08CAP]
Passwords should be often changed. [14GCP]
Most of the web services require alphanumerical passwords. [16FEP, 20PRP]
All my passwords are saved on my pc, but when I log in with a different device I have to insert them. [08CAP]
E-commerce web site has saved my credentials, so everyone can log in using my pc. [02DIP]
I consider the university web portal not reliable, because the username is my fiscal code that is easy to obtain. [08CAP]
When the security intensifies, the access credentials required become complex. [08CAP]
The identity of the students who log in to the e-learning platform is just partially verified. [02DIP]
Once I obtain the digital file of the biometric factors of one person, I am that person and the contrary is hard to prove. [20PRP]
I don’t know if the electronic signature is secure. [02DIP]
I think that today not all the operating systems support the use of the biometric factors. [14GCP]

I would understand if the *single sign-on* is reliable. [14GCP]
Regarding *single sign-on*, I prefer to keep the critical passwords distinct from other less important credentials. [16FEP]
Using electronic signature on exam report is quick and reduce the waste of paper. [11BAP, 20PRP]
The web service must be user-friendly. [08CAP]
The smartphone is something volatile, it could be lost, stolen or damaged. [14GCP]
Concerning my work, I don’t have important information to protect, like patents, so a medium level of security is enough. [20PRP]

THINK
Security and risk are not the same concept. [14GCP]
I consider university web services critical in terms of security, due to my institutional responsibility. [02DIP, 08CAP, 20PRP]
In my opinion, the level of security that should be guaranteed by the university is high, but the level that is actually guaranteed is different. [16FEP]
I prefer to sign on papers rather than using the electronic signature, because (in the first case) I can deny my autograph. [08CAP, 20PRP]
Increasing the level of security is useless in the cases I don’t have sensitive data to protect. [14GCP]
The kind of data I want to protect are those connected with money transaction (online banking, e-commerce). [08CAP, 13SNP,14GCP]
I have a positive opinion about the use of biometric factors for access control. [14GCP]

Empathy Map	**user role: *front office staff***
DO	**SAY**
I access the system using my credentials which are my identification number as username and the password [21GVA]	I can remember the passwords, I don’t need to write them down. [21GVA]
When I need to change the password, I use one single pattern and I change just few characters [21GVA]	We are the first impact with students, the first meeting point with users. [21GVA]
We answer to e-mails as soon as possible, almost in real time. [21GVA]	Nowadays the interaction between user and administration is more efficient than before. [21GVA]
We check and supervise the academic careers of all the students. [21GVA]	Considering the thirty years I work in this office, I see an important evolution. [21GVA]
We support the students from enrolment to degree achievement. [21GVA]	In the last two years there was an exponential grow of technological tools. [21GVA]
We also manage the administrative aspects of students’ announcements of selection for the admission to courses of study. [21GVA]	There is a hierarchical scale within my organization. [21GVA]
We provide information to students who want to enroll, change the course and so on. [21GVA]	I have some functions and responsibilities which my subordinates don’t have. [21GVA]
I manage and supervise the proceedings archiving. [21GVA]	I can say that our work is rich of variations and variability. [21GVA]
I receive the e-mails from professors who ask me to make correction on the exam report, because they can’t do it by themselves and they need my authorization. [21GVA]	The job tasks depend on the work shift (morning, afternoon, evening). [15MASB]
I organize the service we provide based on student information booklet and the norms of the university legislation. [21GVA]	**GAIN**
We list the borrowed books in a catalog. [15MASB]	Technological tools implemented in the last years simplify our work, reduce the stress and also benefit the service we provide to students. [21GVA]
I need to update books' state (available or borrowed) on a media library. [15MASB]	Now our procedures are computerized and the timing is reduced. [21GVA]
We give out a sheet with the loan conditions described. [15MASB]	We benefit from effective and efficient digital system. [21GVA]
We use the computer to find out where the books are, on what shelf and in which sector. [15MASB]	Using e-mail and *Skype* we can reduced the amount of requests received by the desk. [21GVA]
When I don’t work (i.e. during vacations) I delegate my functions to trustworthy colleagues. [21GVA]	The students who turn to the desk for support are identified through their ID. [21GVA]
Due to the integration between the Faculties of	The exchange of information among universities

Psychology and Medicine, in the next years we are going to manage the service for both of them. [21GVA]	should be increased. [21GVA]
We certify only when we are sure that the procedures are done in the right way. [21GVA]	I would like to visualize the certificates released by other Italian universities, so to make the service more efficient. [21GVA]
We use the university web portal interface that is targeted for managing administrative procedures. [21GVA]	**PAIN**
When a problem arises using the university web portal, I ask for the technical support. [21GVA]	We still use pen and paper to work. [15MASB]
I collaborate with the other colleagues of the front office. [21GVA]	We still use a hardcopy catalog for magazines. [15MASB]
THINK	There is no computer program that could check whether a book has been returned or not. [15MASB]
The old procedure for reporting exams using the printed register was wasteful. [21GVA]	If someone forgets to return a book, it would be very hard to notice. [15MASB]
We are a public office with some administrative procedures which we can’t avoid and exclude. [21GVA]	We do not use any technological device to verify students' identities. [15MASB]
The collaboration with ICT operators is easy because they are willing to solve our problems. [21GVA]	We meet different problems using the university web platform and this causes malfunctions of the service we provide. [21GVA]
FEEL	The technological devices provided by the university do not work properly. [15MASB]
We were stressed searching for the printed exam reports within the hardcopy archive. [21GVA]	Sometimes, I cannot help students, because I am trying to figure out what is wrong with the computer. [15MASB]
HEAR	In the evolution to make our procedure computerized, there are some issues and I hope they will be solved. [21GVA]
I hear some people considering the printed certificate safer than its digital file. [21GVA]	People often don’t use some tools (i.e. Skype) through which they can avoid to turn to desk. [21GVA]
I heard the requests of users who lost their receipts of the book loan [15MASB]	The password needs to be changed every two months for privacy reason, and this is becoming difficult. [21GVA]
SEE	When I come back from holidays, I say: what is the last password? [21GVA]
I see a lot of colleagues as people of good will, who work hard to overcome the obstacles and find solutions. [21GVA]	When I delegate my functions to a colleague, she/he could need to use my credentials in order to manage particular issues, because the system doesn’t allow temporary permission. [21GVA]
I see the documents received in the electronic archive, such as the exam reports validated by professors using electronic signature.	

[21GVA]
I visualize the exam reports as digital files. [21GVA]
I check the ID and the library card shown by the users. [15MASB]

Annex 3 - Personas

Persona user role: *professor*

https://humanrights.ca/sites/default/files/styles/large/public/images/blog/blog113_human-rights-toolkitweb.jpg?itok=0IWUxXIS

Silvia

“I do almost entirely online!”

She is 45 years old. She is married and she has two teenagers sons.
She is a psychologist and since 2005 she is a professor at the University of Rome. She loves her work and she puts a lot of effort into didactic and research activities.
During the free time, she likes travelling and seeing new places with her family, and she always plan amazing journeys.

Activities and tools

She teaches Developmental Psychology through blended courses, using e-learning platform.
Sometimes, she organizes conferences and other kind of events at the university, in order to meet the scientific community for sharing innovations and news in her field of work.
She uses four different devices (smartphone, tablet, the computer provided by the university, and her personal notebook) and thanks to them she can be always connected.
In order to communicate and be in touch with the others (relatives, friends, colleagues) she uses Social Networks and instant messaging services, and only one e-mail that is provided by the university.
Due to her familiarity with web services, sometimes she helps friends and colleagues, for example when they need to book a flight or make the registration for a conference.
She uses a lot of web services both for work and for personal purposes: e-commerce, file sharing, scientific database, forums and web sites about travels, video streaming and so on.
So, she manages several virtual identities with their access credentials, and she applies a specific strategy to create passwords: starting from some regular patterns, she adds few elements to specify the password for the particular registration.
Furthermore, she tends to save the credentials on the browser when she uses her personal devices.

Questions

- How can I make my work more efficient and less time consuming?
- Why do some procedures and activities still require papers?
- How can I create passwords that are simple to remember and safe?

Goals and needs

- ➢ To be updated about (and contribute to) innovations and evolutions in the field of Psychology.
- ➢ To manage the blended courses in the best way, taking advantage of the ICT for learning.
- ➢ User-friendly web services and mobile applications.
- ➢ To get easily access to the most used services (i.e. e-mail, file sharing), whenever she wants and wherever she is.
- ➢ To use only reliable web services.
- ➢ To have more free time for her hobbies and interests.

Motivations and opinions

In her opinion, the services considered more reliable and trustworthy are those with high reputation and strong brand identity, also taking feedback and opinions of other users into consideration.
She does not consider as «sensitive» her personal information (i.e. age, e-mail address) and academic data, which are available on the web.
The data she wants to protect are those connected with her banking account, thinking about the risk of unauthorized access.
She tends to reduce the effort connected with registration and identity management required by online services. Thus, she consider the use of biometrics factors for access control as a benefit.

Barriers and pain points

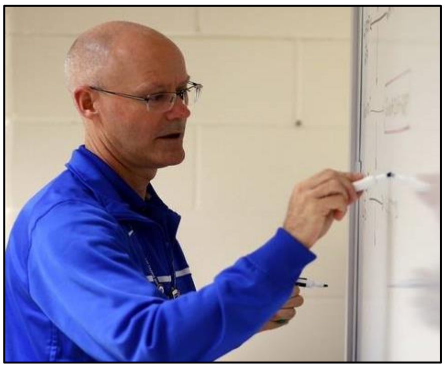
- ○ She has to manage several online accounts with their relative credentials, and she wastes time to meet requirements in the registration phase.
- ○ She forgets the access credentials for sites and services less used, and then she has to recover them or make a new registration; and this

- Are the *single sign-on* systems reliable and secure?
- How much time I will waste to recover all my stuff if I lose my smartphone?

requires precious time.

- She tends to save the credentials on the browser, but when she uses a different device to access the accounts she has to remember the passwords.
- Because her credentials are saved on the browser, her sons can easily access her online accounts.
- She has not in-deep knowledge of technical aspects of technologies.

Persona user role: *professor*



http://www.dailyherald.com/storyimage/DA/20141031/news/141039723/EP/1/1/EP-141039723.jpg&updated=201410310048&MaxW=800&maxH=800&updated=201410310048&noborder

Activities and tools

He collaborates with researchers and other professional figures to carry out his didactic work, and also to conduct innovative projects in the field of Telecommunications.

Due to the several courses to manage, he is often very busy and sometimes he asks for the support of trustworthy PhD students so to carry out lectures and exams.

As support for his activities, he uses different services as collaboration tools (i.e. file sharing).

Because of his several online accounts to manage, he writes the credentials on the memo pad that is always in his bag, so he doesn’t need to remember all the passwords and PINs.

Unlike the colleagues, he does not use the e-learning platform provided by the university, because he prefers to send the lecture materials to the students via e-mail.

He use two e-mail accounts: the institutional account used for work and research activities, and the personal one, keeping this two spheres distinct. Thanks to his smartphone, he can hold all the communications in check.

In order to reduce security risks, when he buys something online he use *PayPal* and a prepaid card.

Questions

- What is the reason why in the Engineering Faculty the WiFi connection doesn’t work in all the rooms?
- Is one single biometric factor enough to ensure the security of the access control?
- Why are the university web services in maintenance during the more busy academic periods?

Carlo

“There is a difference between the security that should be guaranteed and the state of play”

He is 65 years old. He is a long-time professor of Engineering at the University of Rome, and every academic year he holds different courses joined by several students. He cares of his work, in a professional and accurate manner, and with a strong sense of responsibility toward the institution.

He spends the free time playing chess (his main hobby) and staying with his family and friends.

Goals and needs

- ➢ Simple and efficient procedures required by university bureaucracy.
- ➢ To be sure the services he uses are reliable and secure.
- ➢ To protect the sensitive data from disclosure and unauthorized use.
- ➢ The university should guarantee the reliability of its services.
- ➢ To try to manage the amount of e-mails received every day as soon as possible.

Motivations and opinions

He has a specific representation of privacy and «sensitive» data: every single information about him should be protected because it could be used to cause damage and offense. He tends to avoid the exposure and visibility of the information connected with his daily life (i.e. habits, people he meets and places he frequents). He tries to pay attention when he surfs the web due to his institutional role as professor.

He doesn’t use *single sign-on* system and he prefers the analog memo pad, so to have the responsibility for his own accounts and avoid entrusting his credentials to a third part.

Barriers and pain points

- ○ The use of OTP is time consuming when he needs to carry out more than one function.
- ○ He can’t remember all the credentials, and he has trouble looking for a specific password among the pages of his memo pad.
- ○ He has doubt about electronic signature because he can’t deny the autograph.

Persona user role: *student*

http://images.collegexpress.com/article/majors-academics-advice-students-starting-college-study.jpg

Giovanni

"I tend to keep my stuff private"

He is 27 years old, he studies Telecommunications Engineering at the University of Rome and he is carrying out an important research for his PhD.

He is hardworking, but during weekends and holidays he likes to spend time listening and playing music with his band.

He is considering whether to create a startup company to develop some interesting ideas together with his friends and colleagues.

Activities and tools

He collaborates with other researchers and he spends a lot of time at the lab, where he has all the tools available provided by the university.

He prefers to use the WiFi of the lab that is more secure and efficient than campus WiFi.

Reliability and trustworthiness of the web services are fundamental issues for him.

He always read privacy policy before accepting its condition.

In order to ensure the security, he uses complex credentials for the online accounts. In particular, he uses four main passwords as starting point, and then he adds some elements to meet the requirements (length, characters, numbers etc.), considering the level of security he wants for the specific service.

Sometimes, he creates fake accounts when he needs to use a new web service without disclosing his real identity.

He uses the e-mail account provided by the university and the personal one, that is rarely used.

For online shopping, he uses a prepaid card so to feel more safe.

Questions

- Can web services be more secure?
- How do web sites use the data I disclose?

Goals and needs

- ➢ To avoid using web services that he does not consider secure.
- ➢ To take care not to lose his phone.
- ➢ To receive notifications for the online accounts protection.
- ➢ To avoid exposing data.
- ➢ To use services and tools which meet his needs for efficiency and high performance.

Motivations and opinions

He knows the risks connected with web use, so he tends to protect all his data and he discloses information only when it is strictly needed. He thinks that every kind of information could be used to cause sort of damage.

He doesn't use *single sign-on* or *password manager software* despite they could help him, because he prefers to have full control over his credentials.

When he finds a new web service or an innovative mobile application, he tries it out and if it doesn't meet his performance and reliability needs, he gives up.

Barriers and pain points

- ○ Managing all his online accounts is difficult for him.
- ○ Reconnect and re-insert the credentials to use the campus WiFi.

Persona user role: *student*

http://images.inmagine.com/400nwm/photoalto/faa049/faa049000039.jpg

Activities and tools

He uses different web services and mobile applications, and he prefers online procedures instead of those «offline».

During his free time, he likes to put his skills to the test, playing codewar and online role play games, and also sniffing at web traffic via campus WiFi connection, in the break between lectures.

Due to his familiarity with technologies and web services, sometimes he helps relatives and friends to use them and solve problems.

There is always the smartphone in his pocket, and he has a notebook that he can use sitting on the sofa as well as in the university library.

He uses Social Networks to keep in touch with friends and share contents. Furthermore, he follows blog and online forums to keep updated about new trends and innovations.

Using several web services, he has to manage the different access credentials. In order to make this task easy, he uses *single sign-on* system with a strong master passphrase.

He doesn’t need to use the e-mail provided by the university (except for having software licence for students), because his personal e-mail account is enough.

Questions

- Why are certain services not secure? (i.e. campus WiFi)
- Is there a mobile application of this service that I can use?
- What is the real identity (and the skills) of people discussing in online forums?

Marco

“More safety, less effort”

He is 24 years old graduate engineering student at the University of Rome, and he spends a lot of time studying.

He has excellent knowledge of ICT, and he is always updated about new trends and innovations.

He likes to stay with friends, even only for having a coffee during the spare time.

Goals and needs

- ➢ To have mobile apps of the services he uses.
- ➢ Efficient and trustworthy web services and digital devices.
- ➢ To follow blog and participate in forum for online discussions about interesting topics.
- ➢ To acquire knowledge and develop his skills.
- ➢ To make the study entertaining.

Motivations and opinions

In his opinion, not all the web services require the same level of security, and this depends on the kind of data they gather and store.

There are less important information (academic information) and more critical data (in the case of money transaction).

When he choose web services or digital tools to use, he prefers those of major brands and trustworthy reputation.

When someone asks for his help, he wonders why some people are still not autonomous in the use of digital tools and web services.

Barriers and pain points

- ○ Some access control systems and registration procedures require too many steps to be accomplished.
- ○ He knows the importance of multifactor authentication of the Internet banking account, but he considers it frustrating.

Persona user: *student*

http://www.thesoundsnews.com/wp-content/uploads/2013/05/college-girl-stock-300x199.jpg

Susanna

“If they add others safe code, I will go crazy”

She is 25 years old and she studies Psychology at the University of Rome, but her interests range from Art to English literature.

When she has some free time, she likes reading books and visiting museums and exhibitions around the city together with her friends.

She lives with her family and, at this time, she can’t have a job because she puts a lot of effort into the study.

Activities and tools

She spends most of her time in the campus to attend lectures and study in the library.

She often uses different web services (i.e. fidelity cards, online magazines, scientific database, cloud storage etc.); she is member of five Social Networks and she uses them every day.

She hasn’t a good memory for password, so she uses similar passwords and she usually saves the credentials on the browser.

She always tries to solve the problems she meets using university web services by herself; if she can’t do it, she asks to skilled colleagues or she turns to the support desk.

She manages two e-mail accounts: the first is provided by the university and she uses it only for formal communications with professors and university staff; while her *hotmail* account is used as the main.

In addition to the smartphone and the notebook, she has a tablet that is useful especially during lectures to surf the web searching for further information about interesting topics.

When she needs to buy something (books as well as shoes) or to make flight reservation, she uses her father’s credit card and she always do it using web sites of major brands.

She tends to accept the privacy policies and the Terms and Conditions of the web services without reading them, because she considers them too long and rarely clear.

Questions

- Is this web service reliable?
- How can I delegate to others the use of web services with biometrical access control?
- Why are the privacy policies so unclear and difficult to understand?

Goals and needs

- To get easy access to her online accounts.
- To create simple and similar password so to easily remember them.
- To avoid phishing and spam.
- To have mobile applications for most used web services (i.e. e-mail, *Facebook*, *Google Maps* etc.)

Motivations and opinions

Few years ago, she had the habit of using a unique password among different platforms; but over the years, she heard rumors about frauds and friends’ suggestions about useful strategies to prevent them.

She is not worried about possible risks when she surfs the web, because she doesn’t consider herself as a person at risk. She thinks that nobody can be interested in her personal information because she is just a small fry.

She relies on university web services because the institution guarantees their trustworthiness, and the kind of data they store (course of study, exams reports etc.) are not sensitive for her.

Barriers and pain points

- The requirements for password creation are perceived as constraints.
- The use of different credentials (username, passwords, PIN, OTP and safe codes) for accessing web services is frustrating.
- She is not aware of security precautions and risks connected with the web.

Persona user role: *front-office*

https://pixabay.com/static/uploads/photo/2014/11/24/16/22/secretary-544180_640.jpg

Maria

“We are the first meeting point between the students and the university”

She is 57 years old and she works as office manager in collaboration with her subordinates to provide service to the students of the Faculty of Psychology at the University of Rome.
Within the hierarchical scale, she has an important role with particular tasks and responsibilities.
But during vacations, she can delegates her functions to trustworthy colleagues and enjoy the free time.

Activities and tools

Together with the colleagues, she provides informational and administrative support to students who want to enroll, change the course etc.
She uses the web service UI targeted for the administrative role, and she manage the electronic archives in which all the reports and certificates are stored.
When some problems arise using these tools, she asks for the support of technical staff.
The access credentials of all the tools she uses to carry out her work (e-mail, web portal, electronic archives) are the same: the identification number as username and the password.
The privacy policies demand that she often changes the password, and in order to simplify this task she uses a single pattern and every time she changes just few characters to create a new code.
She uses the e-mail account provided by the university to communicate with the users and the staff.

Questions

- Why do people hesitate using tools through which they can avoid turning to desk?
- Why does the web portal not allow temporary permissions to other user roles?
- How can I quickly and easily verify some certificates and documents released by other institutions?

Goals and needs

- ➢ To support students from enrolment to degree achievement, supervising their careers.
- ➢ To change the password to comply with the privacy policies.
- ➢ To solve administrative issues.
- ➢ To reduce the effort and the time needed to accomplish tasks during her daily work.
- ➢ To increase the use of ICT.
- ➢ To provide high quality service.

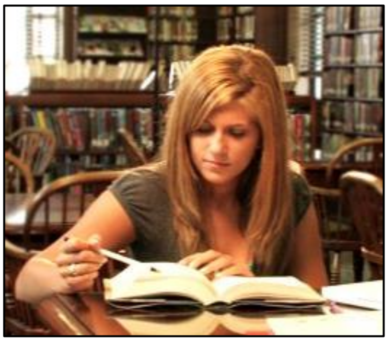
Motivations and opinions

She considers the innovations introduced in the bureaucracy as a benefit for both staff, students and professors.
Due to her expertise and responsibility, she pays attention on everything she does during her work. She knows that solving mistakes and slips with critical effects is not always easy.

Barriers and pain points

- ○ Manage the hardcopy archive and search for old printed exam report.
- ○ Still existing lacks and problems of computerized procedures.
- ○ Lack of integration and communication among the services of the different universities
- ○ Due to the recurring change of password, it is hard to remember what the last one is.

Persona user role: *front-office*



http://ak.picdn.net/shutterstock/videos/476104/preview/stock-footage-students-study-in-the-library.jpg

Giulia

“We still use pen and paper to work“

She is 24 years old and she works as assistant at the university library. She likes this work because during the idle time she can consult all the books and papers she wants.

She got this job in order to earn some money to pay for her studies.

Activities and tools

She spend most of the time in the library where she work and study.

The digital tools provided by the library are not enough to accomplish all the tasks included in her job activity, which are: helping the students to find the books required, writing down what books have been borrowed in a catalogue and checking the identities of the students who borrow books, checking the status of a loan, and marking down the books required that are not yet available in the library.

Most of the work is done with pen and paper, and that is the reason why she encounters many obstacles in carrying out her job tasks efficiently.

Questions

- Can the library provide the digital tools we need to carry out the work efficiently?
- Why do we still have to use a hardcopy catalog instead of a digital one, which would be easier?

Goals and needs

- ➢ To use a computer program to verify student identities.
- ➢ To have an online catalog of books and magazines.
- ➢ To accomplish job activities as soon as possible so to spend the rest of the time studying.

Motivations and opinions

She believes that the computerization of data can enhance the library service that should be quick and efficient.

She is frustrated when some tools do not work properly, especially when she uses the system to keeping track of books borrowed/returned that is very outdated.

Barriers and pain points

- ○ Using the hardcopy catalog is time consuming.
- ○ It is difficult to notice if books are not returned.

Annex 4 - Mental Models

Mental Model		user roles: student and professor
	Manage online account	
Register a new account	Change the password	Preserve the access credentials
Create variations starting from a unique password [19PAS] Create passwords starting from a base pattern [09ALS, 10GIS, 12ASS] Create passwords combining names, phone numbers and cities [20PRP] Meet the requirements for password creation [11BAP, 16FEP] Create secure passwords [09ALS] Create passphrase for critical online accounts [09ADS, 19PAS] Create random passwords [05SES] Create simple passwords to remember [06ADS, 12ASS, 16FEP01LUS] Resort to a set of passwords [01LUS] Create more/less complex credentials considering the importance of the account [02DIP, 06ADS] Tend to use the same password for different accounts [08CAP, 13SNP, 20PRP] Create specific credentials for each registration [13SNP, 20PRP] Accomplish the steps to finalize the registration [19PAS]	Often change the password of critical services [19PAS] Change the passwords during holydays when there is enough time to do it [16FEP]	Request forgotten passwords [08CAP, 14GCP] Remember the different passwords [08CAP, 13SNP] Write the credentials on the memo pad or piece of paper [02DIP, 04ERS, 09ALS, 14GCP] Use single sign-on system [07DOS, 17PIS] Save the passwords on the browser [04ERS, 07DOS, 08CAP]
Access credentials Registration procedure to create a new account Requirements for password creation Random password generator	Procedure to change the password	Single sign-on Memo pad, pen and paper Feature to save the password on the browser

Login to the account	Allow someone else to access the account
Access different accounts through single sign-on [07DOS, 17PIS] Insert different kinds of credentials (username, password, OTP) [08CAP, 18MRS] Always bring OTP calculator [14GCP] Access the university web services with the same credentials [01LUS, 02DIP, 17PIS, 18MRS	Ask to a colleague for making a conference registration [16FEP] Allow friends and parents to use my own account [01LUS, 04ERS, 09ALS, 12ASS, 15MAS, 18MRS, 19PAS] Help relatives and friends to use web services [10GIS, 17PIS, 18MRS]
Access credentials Single sign-on OTP calculator	Access credentials

Mind privacy and security		
Evaluate the reliability of web services	Protect critical and sensitive data	Avoid to disclose personal data
Learn about the web service and its privacy policies [10GIS, 17PIS] Try out a new service to test it [17PIS] Understand how data could be tracked [03DAS, 18MRS] Check the security of web sites [05SES] Read the privacy policies and Terms and Conditions [CL01]	Back my smarthphone up for technical assistance [17PIS] Back the documents up in the cloud [17PIS] Discern critical web services [08CAP, 09ALS, 10GIS, 13SNP, 19PAS] Protect my institutional account [02DIP, 16FEP] Protect financial information connected with the bank account [08CAP, 13SNP, 14GCP] Keep my credentials confidential [01LUS, 03DAS, 10GIS] Take measures to reduce security risks [06ADS, 19PAS] Use only reliable web services [07DOS, 17PIS] Make online payment only with prepaid card [01LUS, 06DAS, 07DOS, 18MRS] Keep sensitive data confidential [03DAS, 09ALS, 10GIS, 15MAS] Demand different levels of access control security	Disclose personal information only when it is strictly needed [10GIS] Create fake profile to not reveal real identity [CL01, AM11]
Privacy policies, Terms and Conditions		Personal information Fake profile

[07DOS] Check the security of web sites [05SES] Protect the e-mail account to prevent spam and phishing [12ASS] Pay attention in releasing credit card details [FR05]
Back up procedures Account and access credentials Financial information

Mental Model user roles: *library assistant*

Communicate with users	Enroll users	Give assistance to users
Communicate with users	Enroll users	Give assistance to users
Check inbox [15MAS] Answer to received messages [15MAS]	Ask for completing the form with personal information [15MAS] Copy users’ ID [15MAS] Insert new users’ information in the database [15MAS] Give to new users the library card [15MAS]	Assist users looking for books/papers [15MAS]
E-mail service	Registration form Users’ ID Database Library card	

Manage the loan process		
Verify users’ identities	Find requested books/papers	Provide the loan
Check the library card [15MAS]	Search in the database the location of books requested [15MAS] Consult the hardcopy catalog of scientific papers [15MAS] Search the books requested in the catalog [15MAS]	Take the requested book/paper from the deposit [15MAS] Register the loan in the list [15MAS] Give the loan receipt [15MAS]
Library card	Database Hard copy catalog	List of loan Loan receipt

Store the books/papers	Manage the lockers	Provide photocopies
Store the books/papers	Manage the lockers	Provide photocopies
Update the books’ status in the catalog [15MAS] Check all books have been returned [15MAS] Put the returned book into the deposit [15MAS]	Get the ID to give the key of the locker [15MAS] Give back the ID when the key is returned [15MAS]	Check the user has the right to free copies [15MAS] Complete the photocopy form [15MAS]
Catalog	Users’ ID	Form to request photocopy