CHALMERS

Interaction design of secure authentication and transaction signing in online banking

Master's Thesis in Interaction Design and Technologies

Marco Dondana

Department of Applied Information Technology
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden, 2013
Report No. 2013:134
ISSN: 1651-4769

Abstract

The presented report documents a research conducted together with the digital security company Gemalto as my Master's thesis in Interaction Design and Technologies.
The focus of the research is the optimal usability of a secure e-banking system with focus on secure authentication and transaction signing use cases. The analyzed scenario features a web interface run on different devices such as laptops and tablets together with an external device designed to face "challenge/response" security solutions called "token".
After considering previous researches in this field and analyzing the boundaries and the specific parameters of the scenario, an analysis of the system currently provided by the company will lead to the first concept ideas.
From these concept ideas, a first working prototype will be developed and a usability study will be conducted on it to define the improvements that will conduct to the development of a second version.
By comparing the results of the different usability study iterations, a list of design guidelines will be defined as a final result of the research.

Table of contents

1. Introduction

1.1 Background

During the Master's program I had the opportunity to discover the field of Interaction Design in its multitude of sides. This relatively new field is more and more considered relevant within the process towards the development of both tangible and digital products and services. At the same time, in the same way as it happens for every new field or science, it is easily misunderstood by many and often reduced and linked to the most common of its applications. From my personal experience, I can say that Interaction Design's most common associations can be sorted into two big fields: Arduino related electronic devices and interfaces and usability/gameplay of on-screen environments.
During my studies, thanks also to my Product design background, I've always focused my attention on the "Arduino side" which meant the opportunity to keep working on physical products while exploring the wide range of interaction possibilities offered by the use of sensors and actuators together with an Arduino board and some coding.
When the opportunity to work, together with a big company, on a system that was composed by a physical device (token) and a web site interface came out, I was really excited about the idea of exploring and getting experienced on usability and graphical interfaces while keeping the focus

also on the interaction with the tangible aspects of the physical product.

The thesis proposal was offered by an international company called Gemalto. Gemalto N.V. is a public company incorporated in the Netherlands that works on providing digital security solutions to support on-line banking, mobile payment applications, national identity programs, smart energy systems and other services of some of the world's biggest organizations. The company develops secure operating systems and software that run on trusted devices designed and managed to preserve the confidential data they contain and the services they enable throughout their life cycle. The Gothenburg branch, in particular, is specialized in the field of strong authentication for eBanking and eCommerce, providing solutions for digital signature and secure access to home and mobile banking services, retail and corporate bank networks, eCommerce sites and cloud computing services.

1.1 Objective and research question

The research can be located within the field of internet security with focus on a high security e-banking system provided by the company Gemalto. The study is approached from an interaction design point of view with main attention on graphical user interface.
The objective of the Master's thesis is to research design guidelines and construct a design proposal (prototype) for optimal usability and security in online banking covering several channels such as PC, Tablet and Smartphone.
The target use cases for this thesis were set by the company and are:

1. User log-in to an internet bank by using a provided security tool.
2. User signature for new payment recipient or transaction by using a provided security tool.

The research question originates from a first analysis of the thesis objective stated in the thesis proposal and was shaped and refined as the case was more deeply analyzed. It is structured as one main question followed by specific sub-question to delineate its focus and was initially stated as following:

How can Gemalto e-banking service be designed in order to optimize the interaction flow and user experience during safe login and signing actions through external devices on different platforms such as laptops, tablets and smartphones?

- Is it needed to make the users understand the dynamics of on-line frauds and the importance of safety precautions in order to let them feel safe and comfortable? How can it be done without overloading the system of not-core information?

- While banks constantly research and implement high-security systems to avoid on-line frauds, users might perceive them as barriers to overcome. Can usability meet security to design a high-flow system where safety precautions, beside actually protect the user, will let him feel safe and comfortable?

- How can the interaction of the system eventually help the user to more closely relate the virtual to the tangible transactions affecting not only the flow but the actual perception of money value?

During the process, as it will be shown in the following text, the focus points of the research question have slightly changed. In fact, since my personal and corporate goal was to deal with the tangible needs and parameters imposed by the company, the focus of the research has been adapted to the direct company goal according to the progression of the work.
Keeping the main question valid, the final sub-questions are:

- While banks constantly research and implement high-security systems to avoid on-line frauds, users might perceive them as barriers to overcome. Can usability meet security to design a high-flow system where safety precautions, beside actually protect the user, will let him feel safe and comfortable?

- Is it efficient, in terms of usability, to guide the users through the login and signing process by articulating the interaction flow on a longer but easier process?

Does the use of dynamic visual assistance help or confuse the users?

- Are different users from different age ranges familiar with secure on-line banking devices? How they perceive the use of this kind of solution? Which level of help do they actually need?

The final output of the research is a list of design guidelines based on the observations conducted trough the usability testing on the generated prototype focusing on the research questions as the main points of investigation. The design guidelines are intended as a design tool for Gemalto's interaction designers. In fact, they are aimed to contribute to improve the future products and services provided by the company, not only in terms of quality but also in terms of efficiency during the design process.

2. Theory

2.1 Interaction Design

Interaction design is about the design of interactive products to create user experiences that enhance and extend the way people perform everyday activities supporting their lives (Preece, Rogers and Sharp, 2002). The discipline of interaction design has been amply discussed and specifically defined in different ways. Löwgren and Stolterman (2004) define it as strictly related to digital artifacts and refer it to the process that is arranged within existing resource constraints to create, shape and decide all use-oriented qualities of a digital artifact for a client. Differently, and following the progress and evolution of the discipline, Cooper, Reimann and Cronin (2012) expand the relation of interaction design to digital products, services systems and environments, defining it as a design discipline with focus on the design of behaviors.

2.2 Graphical interface design

User-interface design is part of a wider field called Human-computer interaction which focus on the study, planning and design of how people and computers work together. User interface, specifically, is the part of a computer to which the user can directly relate (see, hear, touch, talk

to or direct in general) and is constituted by an input and an output. The input is the way how the user communicates his directions to the computer: keyboards and touch screens are just the most common examples of computer input. With output, at the contrary, we define the way the computer communicates the operations that have been performed back to the user: in this case the most common examples are screens, sounds and lights (Galitz, 2007)

In my case, the work aims to study and design an effective graphical user interface (GUI) within a system composed by keyboards and touch screens as inputs and screens and small LCD displays as outputs.
Graphical interface designer shares some knowledge and skills with graphic designers focused on new medias but with a deeper understanding and appreciation of the role of behavior (Cooper, Reimann and Cronin, 2012)

2.3 Usability testing

The term usability refers to the chance for the user to accomplish his task and the way he or she feels while doing it. What makes a product usable is the possibility for a user to do what he or she wants to do, in the way he or she expects to be able to do it, without hindrance, hesitation or questions (Rubin, Chisnell, 2008).
With the term usability testing, we define a research tool consisting in a process that directly involve final users as representative of the user group to evaluate the level conformity between the product and the specific usability criteria. For this reason, every other product evaluation techniques which not require representative users as part of the process cannot be labeled as usability testing (Rubin, Chisnell, 2008).

Within my research work, usability testing has a central role, not only to evaluate the effectiveness of the designed prototype, but as a main tool to answer the actual research questions and list some final guidelines on which to base the future work on.

2.4 Previous work

"Usability advocates favour making it easy to use a system ... security people favour making it hard to access a system" (Nielsen, 2000). This quote well illustrates the long-held belief that usability and security are opposite and cannot be considered together. While many designers are convinced that improving security necessarily degrades usability, on the other hand, many users tend to perceive the difficulty of use as a part of security (DeWitt, Kuljis, 2006).
The possibility to design systems optimized for both security and usability has been widely discussed as a design goal and many attempts have been done to solve something that might sound clashing by definition.
Kaa-Ping Yee from University of California has been conducting two similar studies: "User interaction design for secure system" (2002) followed by "Aligning security and usability" (2004). In these two articles he discusses the topic of security and usability of general web systems.
In the first article (2002) the author starts from the observation that many designers assume that security degrades usability and vice versa and that the only way to approach the problem is to plan a compromise between them. He, at the contrary, believes that a system that's more secure is also more predictable, more reliable and more usable. The idea is based on a list of design principles that have to match the condition that it should be fairly obvious that violation of any principle leads to a security vulnerability.
Directly quoting Yee (2002), the design principles are:

"- *Path of Least Resistance*. To the greatest extent possible, the natural way to do any task should also be the secure way."

This point may sound quite distant from the actual state of reality. In fact, in many cases, security restrictions strictly require to add some new inconvenience for the user. In these cases, it has to be provided a payoff to offset the cost of the new inconvenience, by making productive use of the extra effort the user is asked to make (Yee, 2002).

"- *Appropriate Boundaries*. The interface should expose, and the system should enforce, distinctions between objects and between actions along boundaries that matter to the user.
- *Explicit Authority*. A user's authorities must only be provided to other actors as a result of an explicit action that is understood by the user to imply granting.
- *Visibility*. The interface should allow the user to easily review any active authority relationships that would affect security-relevant decisions.
- *Revocability*. The interface should allow the user to easily revoke authorities that the user has granted wherever revocation is possible.
- *Expected Ability*. The interface must not generate the impression that it is possible to do something that cannot actually be done.
- *Trusted Path*. The interface must provide an unspoofable and faithful communication channel between the user and any entity trusted to manipulate authorities on the user's behalf.
- *Identifiability*. The interface should enforce that distinct objects and distinct actions have unspoofably identifiable and distinguishable representations.
- *Expressiveness*. The interface should provide enough expressive power to describe a safe security policy without undue difficulty; and to allow users to express security policies in terms that fit their goals.
- *Clarity.* The effect of any security-relevant action must be clearly apparent to the user before the action is taken."

In the second study "Aligning security and usability" (2004), Kaa-Ping Yee, taking into account the principles exposed in the previous research, and mainly extending the "path of least resistance" principle, discusses when and how security and usability can be aligned through three main steps:

- Security and usability cannot be considered as additional features to be applied at the end of the design process. They have to be incorporated simultaneously through the whole process in order to avoid conflicts.
- Both aspects are part of the common goal of fulfilling the user's expectations and belong to an agreement between the system's security state and the user's mental model.
- Security aspects such as authorization should be inferred from acts of designation that are already part of the primary task in order to incorporate security decisions into the user's workflow.

The research focuses on generic everyday security issues such as worms, cookie management and phishing attacks but doesn't cover cases related to authentication.
Two projects are introduced as examples of systems developed to align security and usability: CapDesk and Polaris.
CapDesk is a capability-based desktop shell that implements security by designation, eliminating vulnerability to viruses while letting users run untrusted software in a familiar GUI environment (Wagner, Tribble, 2002). It constitutes an example of designing taking into account both security and usability through the whole process and it's based on minimal default authorities to protect the system from viruses. In fact, an application doesn't have access to a given file or directory until the user allows it. The user can convey additional file access to applications by manipulating file icons and selecting files in file dialog boxes (Yee, 2004).

Case study: Polaris

Polaris is an alpha release software for Windows XP, developed by researchers at HP, designed to align security and usability. For this reason, this product can be closely related to my research work from the point of view of the common goal of exploring the possibility of aligning security and usability even if applied to a different product. The following case study, conducted by Dewitt and Kuljis (2006) in Brunel University (UK), is a usability study about the actual effectiveness of the product towards the goal and was important as a base to develop the evaluation study conducted within my research.
Polaris uses the Principle of Least Authority (POLA) introduced in the previous section to deny viruses the authority to edit files (DeWitt, Kuljis, 2006).In fact, Polaris, by radically restricting the authority of software and making only the files it needs to run accessible, prevents any

virus or malicious code from, reading, altering, or destroying files on the system.
Using Polaris, applications can be 'polarized', creating a 'tamed' version of that application which is immune to viruses.
Even though the primary goal of Polaris is to make Windows safer from viruses and malicious code, at the same time it was specifically designed to be highly usable. The basic idea is that, by aligning security with usability, the user is less likely to try to avoid or bypass the security system due to frustration, as the easy way should be the secure way.
The developers of Polaris had transparency as a specific usability goal so the user shouldn't be aware of the protection provided by the system (DeWitt, Kuljis, 2006).
DeWitt and Kuljis (2006) conducted a usability study about Polaris to actually observe and measure the usability of the system.
The test was conducted on ten users that were asked to attend two sessions. In the first session, following an expected real situation scenario, the users were asked to first perform some tasks to simulate the software configuration followed by ordinary computer usage tasks in which the security features were presented as a side effects of them. During the test, participants were alone with their pc and observed through a one-way mirror in a separate room. To collect more precise data, keystrokes and screen activity were captured and stored for later analysis.
After the first session, the users were asked to complete a questionnaire to gather subjective opinions and the results were measured using a scale called System Usability Scale (SUS) developed by Digital Equipment Co. Ltd to quickly evaluate the usability of a product. A short semi-structured interview followed the questionnaire in order to collect more in depth information.
After one week from the first session, the users were called again to perform a second session consisting in a shorter version of the old tasks but without any possibility to refer to any documentation. The point of this second part was to evaluate the learnability of the software.
The results were analyzed through usability metrics divided into three categories: effectiveness (the ability of users to complete tasks and goals), efficiency (the level of resources consumed in performing tasks) and satisfaction (a user's subjective reactions to using the system).
As a result, the study has found that usability problems are still present in the system even if it was designed to reduce them. The system's operations aren't enough transparent as they were meant to be and the users had issues related to security decisions. The possibility of removing such decisions from the user's tasks would increase the usability but could be problematic in the case where only the user could effectively decide when and how to share information. Other observations about the habits of the users were conducted and their willingness of compromising security in the name of speed and performance was confirmed. In fact, not only the users declared to prefer speed and ease of use to security, but they also showed the tendency to see security messages as a hindrance to avoid rather than an help. The goal of making Windows security more usable seems unsuccessful since security and usability must be developed in unison from the concept phase to the development as an integral part of the system.

3. Methodology

In the following paragraph the whole research method will be exposed. The methodology process is composed by methods learned during the Master's program shaped and adapted to the goal set by the company.

3.1 Task analysis

As said in the introduction, Gemalto, beside many other services, provides security solutions for on-line services handling people's money. Different products and services are specifically designed to face different needs and required levels of security. The solutions provided are: One Time Password (OTP), Double Authentication, Challenge/Response, Sign-What-You-See, XML Sign-What-You-See, Secure-Domain Separation and Dynamic Signatures. For my case study I considered only the Challenge/Response solution. Challenge/response is a method of protection based on a One Time Password (OTP) generated as a result of a process to be performed on a specific external device called Token. The token, designed and provided by Gemalto, doesn't have any type of connection with any other device or network and it's, so, un-hackable. In order to authenticate himself/herself into the system, the user has to use a eight digits code – called Challenge - generated by the system and displayed on

the website interface. The code, that has a short time validity and can be used only once, has to be typed into the token followed by the user's PIN code. At this point the token generates a Response code that has to be typed into the web site interface together with the user's ID code to login. Through the Response code, the system can verify in real time that the token that has been used is corresponding to the user ID and the PIN code.
When, once logged in, the user tries to perform a financial transaction, another Response code has to be generated in order to validate the signature and confirm the operation. The level of security precautions at this step is proportional to the operation's level of risk which is reported to the token through the Challenge code. According to a specific digit's value in the Challenge, in fact, the token can ask the user to perform less or more steps to confirm the operation. In case of a low level of risk transaction, for example a very small amount of money transferred to a well known national receiver, the user is simply asked to insert the challenge and the PIN code in order to get a response code. In the extreme opposite scenario, for instance a huge amount of money transferred to a first time private receiver in some other country, the user, beside Challenge and PIN code, will be asked to confirm the international payment, re-type the IBAN number of the receiver, re-select and confirm the chosen currency and re-type the amount of money he or she's willing to transfer. It is important to notice that the user has to select whether to perform a login or a transaction signature operation by pressing the respective button on the token right after having switched it on.
This method guarantees a very high level of protection against the following attacks (as stated in Gemalto documentation article Fraud Mitigation Methods for E-banking and E-commerce (2013)):

"- *ID Theft:* Stealing personal and/or financial information, such as name, Social Security Number, or account numbers, with the intent to commit fraud.
- *Password discovering:* Attacker makes use of brute force, dictionary, birthday or even as simple as guessing attacks to determine authentication credentials (username and password).

- *Shoulder-surfing:* Attacker covertly observes the keystrokes being entered or screen information being viewed during the authentication process in order to use it later.

- *Keylogging/Screenlogging:* Malicious software/spyware attacks that obtains authentication credentials (username and password) for future use.

- *Copy/Harvesting:* Attacker physically copies or uses a customer's authentication device to generate OTPs without hers/his knowledge. Using the OTPs later in time (but before the user enters next valid OTP).

- *Phishing:* Attacker deceives the customers by using fake look-a-like bank websites, emails or automated phone calls ("Vishing") to convince the customer to reveal or enter their internet banking credentials and authentication codes. When the phishing is close to real-time it does not matter of the OTP is based on event or time or both.

- *Pharming:* Attacker tampers the Domain Name entries on ISP DNS servers or the victim's wireless router and redirects the Bank's legitimate Domain Name (URL) to a fake/malicious site to hijack authentication credentials.

- *Social Engineering:* The oldest and simplest attack, but still one of the hardest to prevent. The attacker tricks, using convincing social skills, the user to reveal his authentication credentials (User). An even worse engineering attack is to trick the bank system owner to get access to the authentication system (System) itself.

- *Cross-Channel Attacks:* Attacker uses another channel/site to phish and hijack authentication credentials. For example asking for internet banking authentication credentials in an online shopping site. This attack can also be done in the same site, ex phishing login authentication codes which also can be used for signing a transaction.

- *Man-in-the-middle (MitM):* Attacker intercepts in real time, using a Trojan and/or a fake website, the user transaction messages. The attacker can collect authentication credentials and inject false

data between the user and the bank site.

- *Man-in-the-browser (MitB):* Similar to MitM, but the Trojan infects the Internet Browser and has the ability to modify pages, modify transaction content or insert additional transactions, all completely invisible to both the user and host application. The attack will be successful on both PKI and/or Two or Three Factor security mechanisms.

- *Relay Attack:* Attack by tampering POS terminals - capturing and harvesting customer card data and response for later use in the internet bank or online shopping. The card data is used for signing the transactions. This method targets explicitly EMV/CAP cards."

Challenge/Response, while being a high level of security method, requires an authentication device with a keyboard/pin pad and a size of the screen enough big to easily complete and review the tasks. For this reason, and for the quite advanced level of the actions the user is asked to perform, it can be perceived as potentially tricky and uncomfortable by the some users. The task consists in a re-design of the web-site interface for secure login and transaction signing using Challenge/Response device focused on meeting security criteria with optimal usability. The system, while being easy to learn and to use for first-timers as well as for those who are not comfortable with technology, should be quick and reactive for expert users that want to perform the task as quick as possible avoiding the possibility to make errors due to distraction. In addition, it should be perceived as secure and efficient at the same time for both categories of users.

3.2 Current system analysis

The system was analyzed by observing the current demo web site provided by Gemalto to try the different solutions. A transaction signing was performed using a challenge/response device called Ezio Grip. The focus of the analysis was the attention flow and the interaction possibilities.

3.2.1 Attention flow diagrams

Since the system is composed by two different devices (laptop and token), the user has to constantly shift his attention from one to another in order to complete the task.
Focusing on the user's eye-focus I outlined four categories:

- *Actions on screen:* every action that takes place entirely on the main device's screen. To perform these actions, the user has to focus exclusively on the web site part of the system.

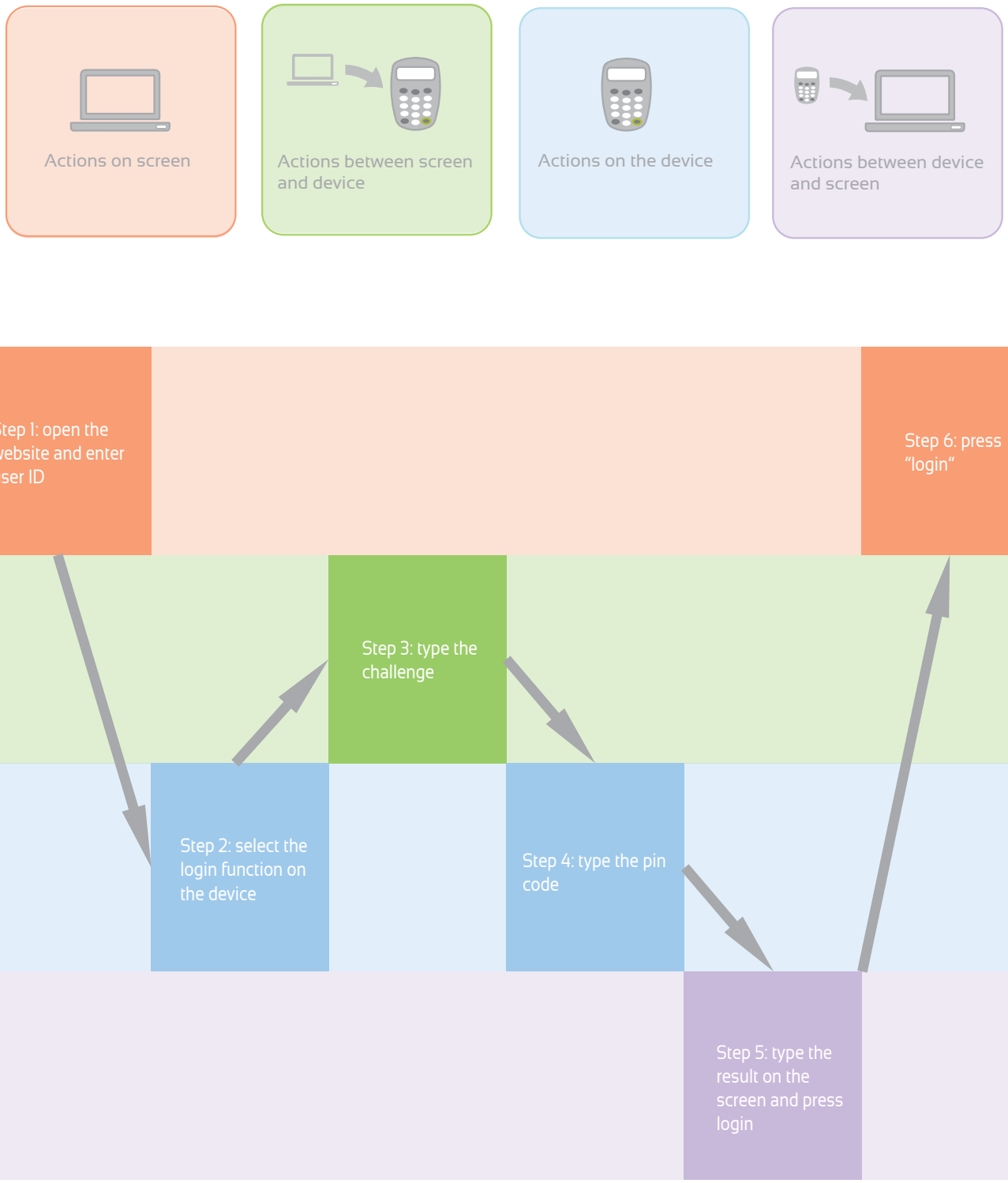
- *Actions between screen and device:* everytime the user is asked to report something from the screen into the token. During these actions, the user's attention bounces between the screen and the token.

- *Actions on the device:* actions taking place entirely on the token. The user interacts only with the token.

- *Actions between device and screen:* when the user is asked to report back something from the token into the device. As for the opposite case, the user has to interact with two different devices at the same time, constantly shifting his focus.

As we can see in the diagram (Pic. 1), the login process starts on the screen by opening the web site and typing the user ID. After everything is set on screen, the focus shifts to the token that has to be switched on and the function selected. At this point there's a bounce of the focus since the user has to read the challenge on screen, type it on the token and then following the "insert PIN code" step on the token's screen. Finally there is another eye-focus bounce when the challenge has to be reported from the token to the main screen where the last step takes place.
The second diagram (Pic. 2), shows the same method of analysis applied to the signature process. Since different payment conditions require different safety precautions in terms of amount of payment's details to be re-typed into the token, an international payment (which requires the maximum amount of extra steps) is represented. In fact, due to the need to report payment details

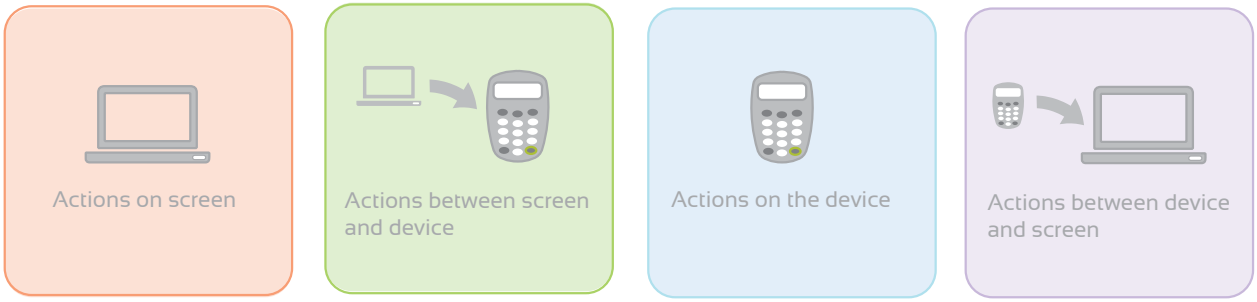
from the screen into the token, in the middle of the signing process the eye-focus flow follows the same path as for the login but the central iteration of actions between the token and the screen is longer. The user attention bounces back and forth from the screen to the token for most of the operation process. In the case of a payment considered as secure, for instance a small national payment to a very well known organization, the steps configuration in terms of attention flow would match the one presented for the login process.

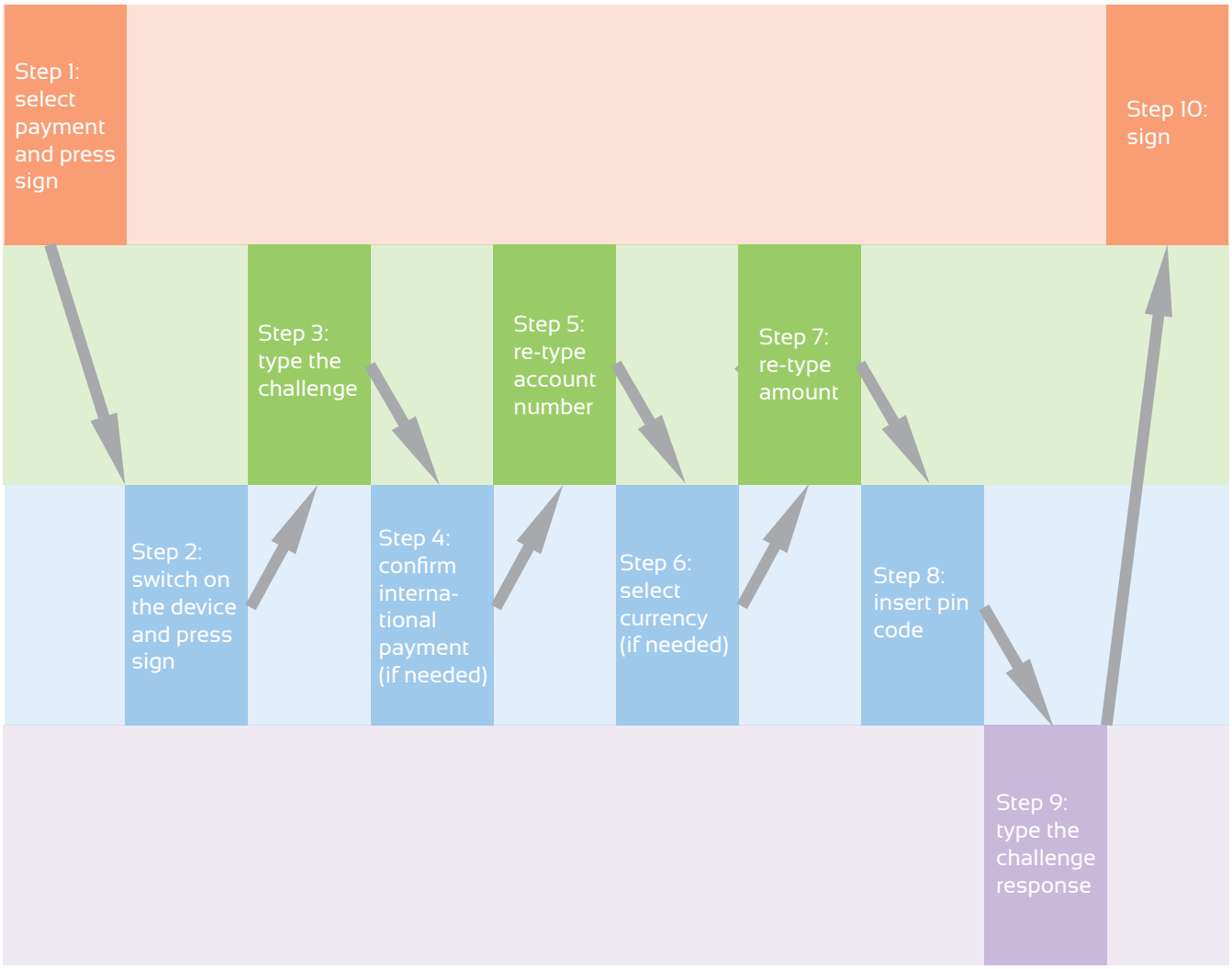


Pic.1 - Attention flow diagram of the login process. The actions are related to each category by color and position on different lines as stated on the top panel.

Attention flow

Eye-focus during signing with Challenge/Response device



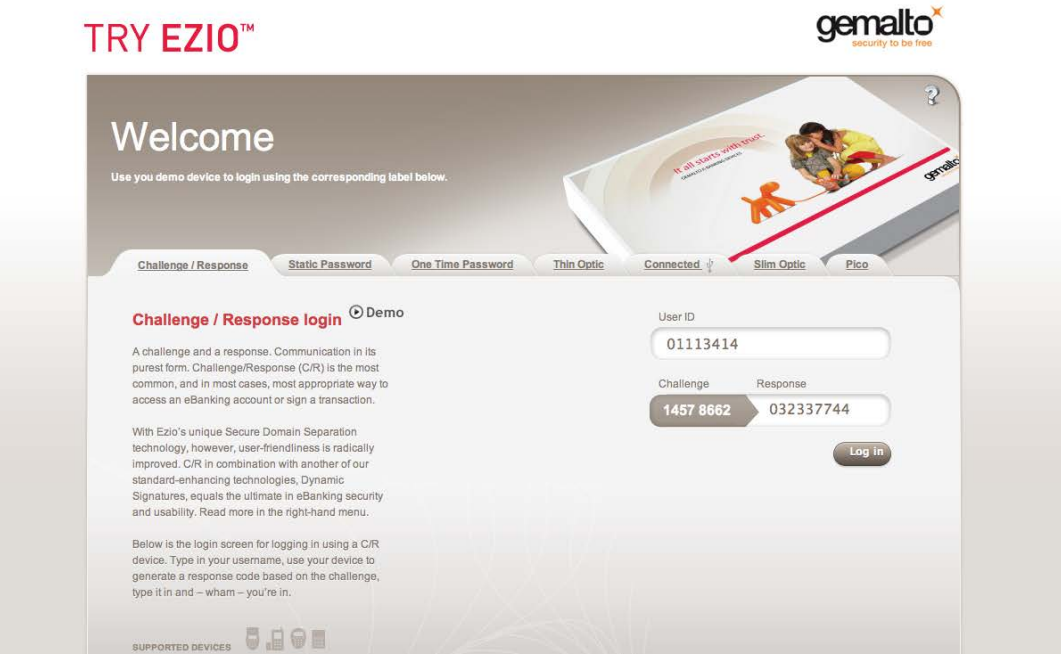


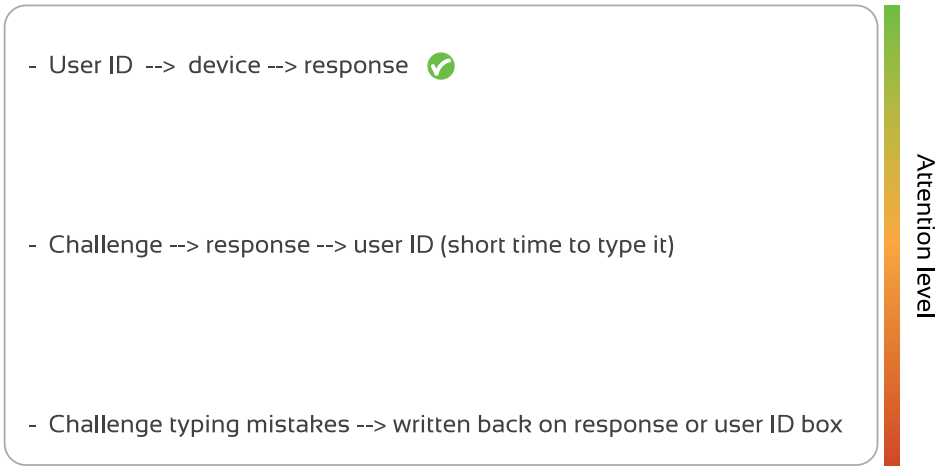
Pic.2 - Attention flow diagram analysis file: compared to the login diagram, 4 extra steps are located in the middle of the process.

3.2.2 Interaction possibilities

While studying the system I observed that, since the entire interaction required to go through the process is concentrated within a small portion of screen interface, the system is open to different levels of interaction. This aspect, if from one point of view doesn't force the user within a defined way of interaction, could lead to frequent mistakes. In fact, especially after a few tries, when I started to perform the action in a quite mechanical way, I confused the text fields quite often.

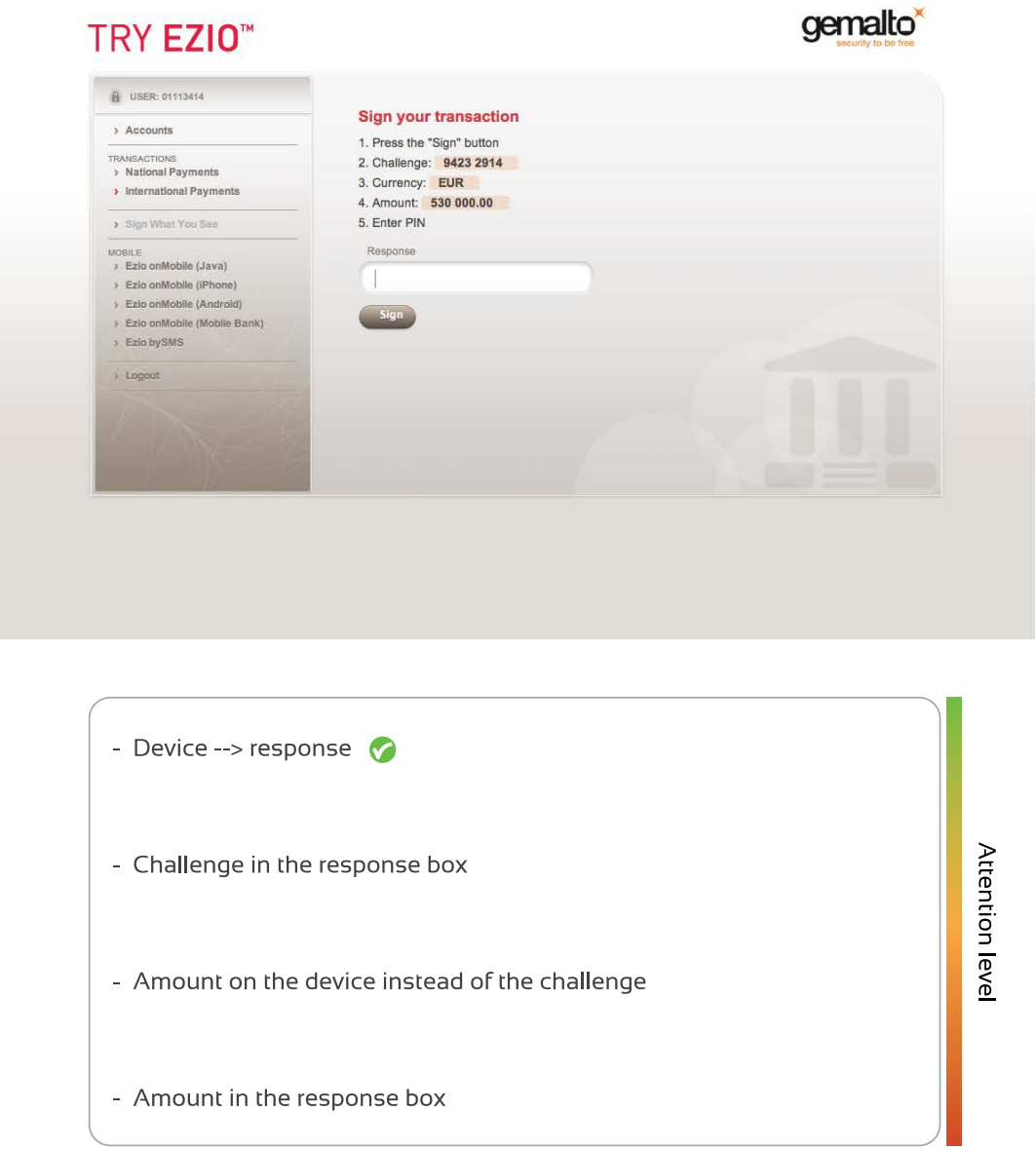
By having visual elements with the same dimension, shape and position it is impossible to distinguish the level of hierarchy and the relation between the elements of the interface (Cooper, Reimann and Cronin, 2012).
At this step of the analysis I considered the interaction possibilities as the actual possible interaction with the interface related to the level of attention paid by the user performing the task. I assumed that the level of attention on a task decreases the more the user gets used to it.
In the first diagram (Pic. 3), the current login interface is presented together with the chances





Pic.3 - Current TryEzio system's login screen (top) and interaction possibilities diagram (bottom). In the diagram, the possible actions that the user can perform are listed from top to bottom and related to the user's attention level represented as a colored bar from green (focus) to red (distraction).

of interaction with it: in the best scenario, the user should insert his or her user ID first and then perform the login task using the device in order to report the response code back and log in. Other options are to type the challenge first and then find and type the user ID before the limited time of validity of the challenge expires or, in the worst case scenario, to mix up the task. Possible mistakes are to report the challenge on screen into the user ID or response field or the response into the user ID field.
The second diagram (Pic. 4) shows the application of the same analysis method to the signing scenario. In this case there is one text field so the user, beside typing the response code correctly, can report any of the data shown in the resume box into the text filed or instead of the challenge on the token.
As stated in the beginning, in both cases the visual elements of the interface don't provide any hierarchy giving to the user no clear clue of the interaction flow (Cooper, Reimann and Cronin, 2012).



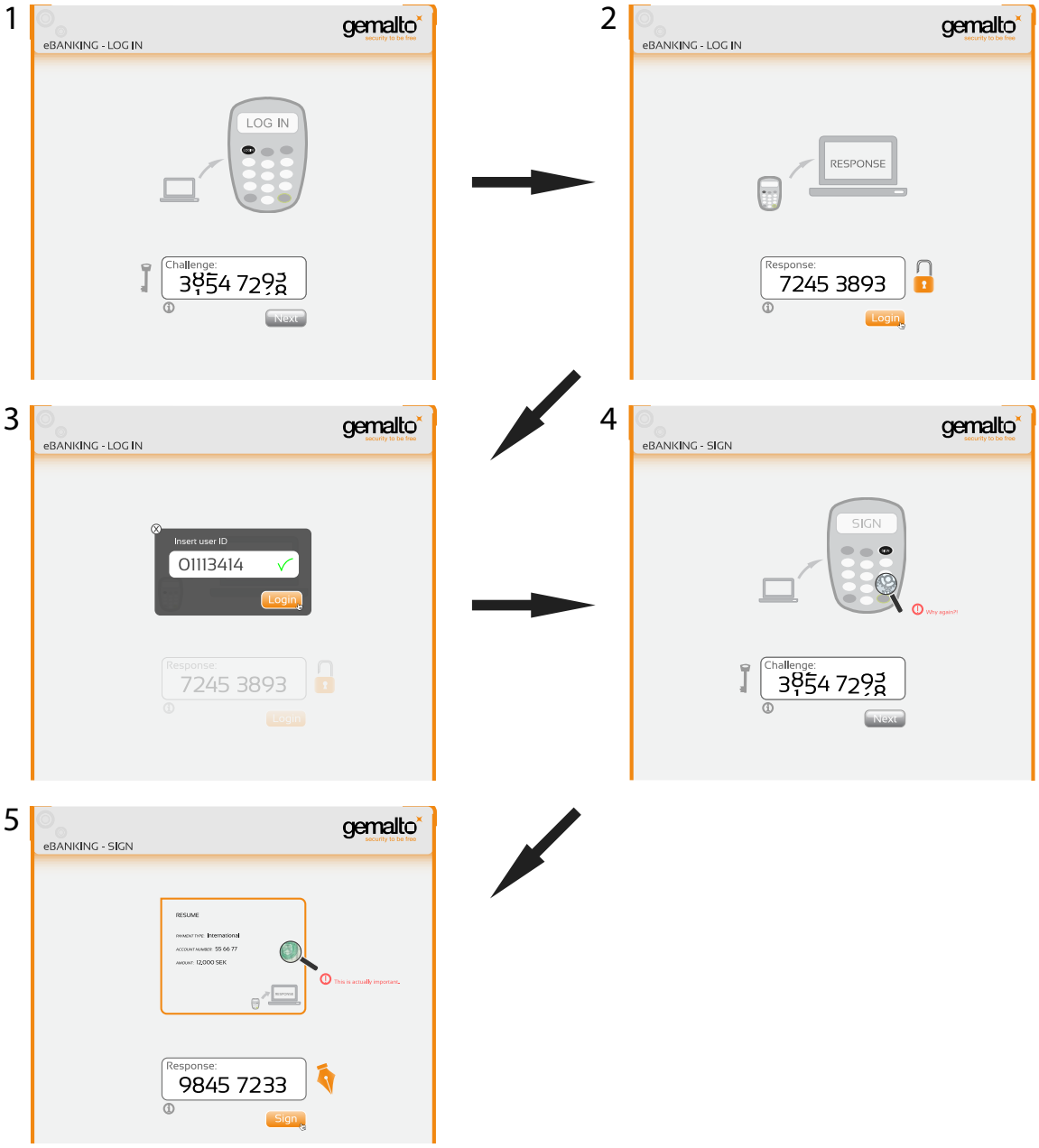
Pic.4 - As for the login screen, the same pattern of analysis is applied here to the transaction signing interface. The example is based on an average level of security payment with the assumption that, adding more listed data, confusion and chances of mistakes augment proportionally to the level of distraction.

3.3 Prototype design

At this step, after having analyzed the current system, I started the process that led me to the first prototype.
Once the first screen mock-ups were designed, interaction flow and interaction possibilities analysis were conducted in order to compare the new system's prototype with the current one. Since technical restrictions soon proved the impossibility of application of the interaction flow proposed in this model, I decided to not report such analysis but to focus on the aspects that led to the first prototype development.

3.3.1 Concept Ideas

The first concept ideas were based on trying to optimize the two factors I mainly analyzed:



Pic.5 - Overview of the first screen mock-ups based on the concept ideas. In order from 1 to 5: login challenge screen (1), login response screen (2), user ID light box (3), signature challenge screen (4) and signature response screen (5).

- "Group" the actions during the process in order to make the user shift his/her focus between the token and the screen the less as possible.

- Reduce the possibility of making mistakes by watering down the actions in clear steps by the use of single action screens.

- Optimize the graphical elements to enhance clear hierarchy and interaction flow.

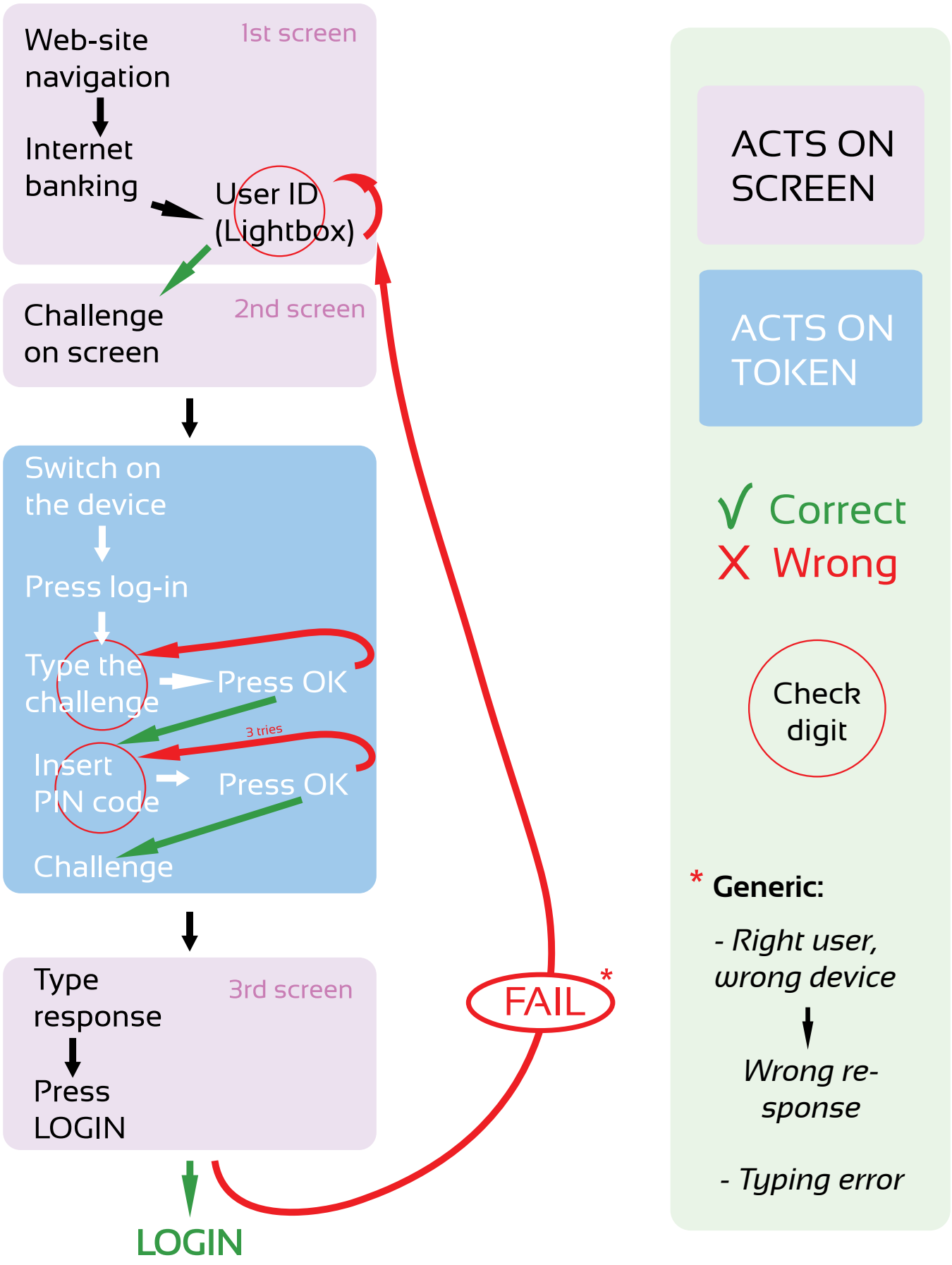
Some screens mock-ups were sketched to discuss and evaluate the general structure and interaction flow concept with the company members. The new flow (Pic. 5) starts with a whole screen focused on the challenge. The user here is supposed to perform all the token-related actions at once before clicking on "Next" button when the response code is shown. The following screen is entirely dedicated to the action of reporting the response code from the token to the screen in order to login. When the user clicks on "Login" button, a pop-up box comes up asking for user ID as a sort of final wall to complete the process. The signing part follows the same path as the login while showing the payment resume in the second page.
For what concerns the visual elements, each screen is composed by three elements placed in a top-to-bottom order: on the center there is a graphical explanation of what the step is about followed, right under, by the core-action box where the actual main action is performed and the "continue" button on the very bottom-right to end the step.
Extra feedbacks are provided by small graphical elements such as small keys, locks and fountain pen tips that, using metaphors, help the user to better relate and understand the meaning of the action he/she is performing.
Finally, the eventuality of the use of tips and hints to inform the user about the logic behind the system were considered as a way to make the system perceived as more trustable and secure. The idea, in fact, was that, knowing the reasons why every step is strictly necessary and how the system reacts to his/her action, the user would be favorably disposed towards the system.
These mock-ups were used as a sort of preview to discuss some basic settings and ideas to base the actual prototype design on in order to also better understand the system.

3.3.2 Interaction framework

Once the concept ideas were set, the following step was to design the interaction framework in a way to define the exact hierarchy and flow of the system. The interaction framework defines not only the high-level structure of screen layouts but also the flow, behavior and organization of the product (Cooper, Reimann and Cronin, 2012).
In this case, many aspects of the interaction framework such as form factor, input methods and functional/data elements were already defined by the company so I focused on two main aspects: screen layout and interaction flow. For both aspects I kept the general concept ideas introduced in the first mock-up but further exploring every aspect in order to evaluate its feasibility.
The screen layout was mainly improved by re-placing the visual elements following an efficient logical path based on the eye movement from top to bottom and from left to right. The challenge code was moved from the bottom to the top and was followed, on the path, by a challenge instruction section right under it. Finally, on the bottom right, the "continue" button was kept to end each step. The reason is that, in my interpretation, the process could be read as a mutation of a code into a new code by passing through a sort of transformation process. The initial code, on the top, has to go through the transformation process constituted by the task on the token and represented on screen by the instructions in the middle before finishing its run into a "final box" at the top of a second screen.
About the interaction flow, the first critical aspect was the user identification step: in the first mock-up, in fact, the user ID was asked to be typed at the end of the login process as a final step. Analyzing the dynamics behind the system, this option turned out not to be technically possible considering the actual system's logic. In fact, in order for the response code to be validated, the user ID has to be related to the user's PIN code and specific token and this happens by incorpo-

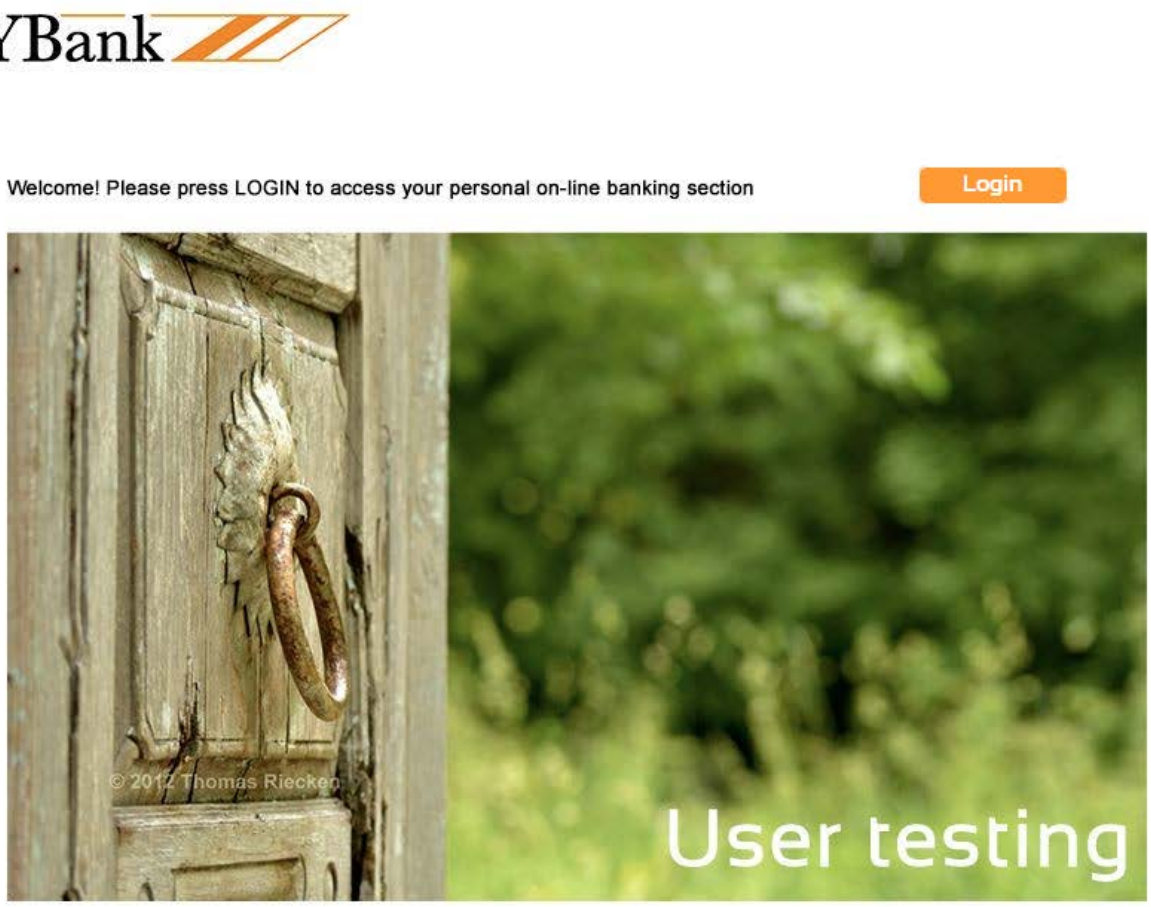
rating data about the user ID into the challenge code. For this reason the user ID typing step must be placed before or at the same time the challenge is generated.
The second aspect to consider was the use of check-digits to reduce the chance of errors during the process. A check digit is a form of redundancy check used for error detection on identification numbers that are manually input. It consists of one or more digits computed by an algorithm from the other digits in the sequence input in order to detect simple errors in the input of a series of characters (Kirtland, 2001).
In the current system, after typing the user ID and completing the challenge, if something wasn't typed correctly the user was forced to re-do the whole process independently from at which point the error happened. By having the user identification as a separate step before the challenge task, an effective use of check digit, which was already implemented in the user ID, could let the user directly spot typing mistakes. In fact, even if until the login is completed it is not possible to identify the user due to privacy restrictions, the system can recognize and give a direct feedback about whether or not the user ID is valid.
Beside for the user ID, the general interaction flow was kept close to the general idea presented in the first mock up. As shown in the flow chart below (Pic.6), the process is split into three screens: Internet bank main page, challenge and response.
Between the first screen, where the user is supposed to access to the e-banking service, and the challenge screen, a light box to input the user ID will appear. This decision was taken to make the system lighter by not adding an extra screen but will be changed during the actual prototyping phase. In case of a not valid user ID, the user can re-type it or go back to the bank's site. After a valid user ID is inserted, the challenge screen invite the user to perform the challenge on the device before proceeding to the final screen where he/she is asked to report the response code obtained on the device. At this stage, if the code is entered correctly, the user access the e-bank, otherwise he/she can choose to start again by typing the user ID or exit the system. The process has to start again from that stage since one of the possible causes of failure could be that the entered user ID, still being valid, wasn't the one associated to the used token so the chance to review it must be open.
The analyzed interaction flow is shown refereed to the login phase that is only one of the two considered use cases but the same dynamics is applied to signing phase as well.

Pic.6 (on the next page) - Interaction flow chart


Web-site navigation
1st screen
Internet banking
User ID (Lightbox)
Challenge on screen
2nd screen
Switch on the device
Press log-in
Type the challenge
Press OK
3 tries
Insert PIN code
Press OK
Challenge
Type response
3rd screen
Press LOGIN
LOGIN
FAIL
*
ACTS ON SCREEN
ACTS ON TOKEN
√ Correct
X Wrong
Check digit
* Generic:
- Right user, wrong device
Wrong re-sponse
- Typing error

Pic.6

3.3.3 Prototype overview

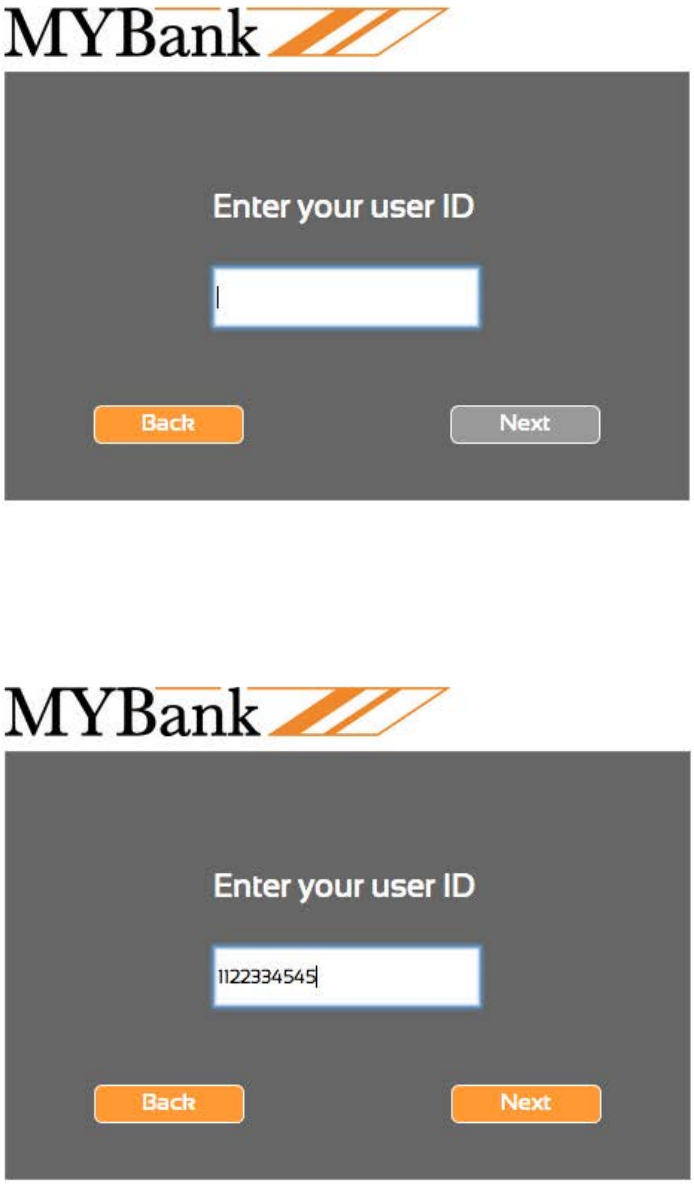


Pic.7 - Homepage of the prototype. Since, in a real system, this screen is related to the bank's website, and the prototype was specifically set for the usability testing, this homepage welcomes the users to the test.

The prototype is developed using Axure software and can be tried at: http://share.axure.com/BP-WX0S/Home.html. It's designed following the visual framework introduced in the mock up but, for copyright reasons, it's referring to a fictitious bank's website called Mybank. The first page should simulate a web bank home page where the user accesses his/her own private area by pressing a Login button.
The visual properties such as shapes and colors are coherent to the corporate image: the color orange is taken from Gemalto's main color palette and is applied whenever a new action is available as a sort of "green light". The system, not having a big amount of elements to choose from, is very linear and usually allows two kinds of actions: going ahead or going back. For this reason the visual elements are quite homogeneous in size, shape orientation and texture but are mainly distinguished by the hue. While, as said before, "Gemalto Orange" means "go ahead", a light grey is used for disabled buttons and red for error messages and help. Finally the rollover style of the buttons uses a bright blue, which is obtained by inverting the orange. Usually, dynamic visual hinting such as rollover is used to communicate the pliancy of an object but, since while clicking the buttons they keep their original properties, in this case it's used to communicate its affordance (Cooper, Reimann and Cronin, 2012). Norman (2002) defines affordance as "the perceived and actual properties of the thing, primarily those fundamental properties that determine just how the thing could possibly be used". The elimination of persistence affordance by showing the behavior of a button passing the cursor over it,

helps reducing visual clutter making the interface simpler and lighter (Cooper, Reimann and Cronin, 2012).
Text panels, together with text fields, are the only squared elements and are automatically selected when the page is loaded. Selected elements are indicated by a soft-shaded blue outline.
The user ID step (Pic.8) was originally intended to appear as a light box or dialog box but, due to practical aspects related to the actual prototype development, it's been added on an extra page.

Since, as stated before, in the real scenario the user IDs contain a check digit to provide a direct feedback about their validity, I simulated it by defining a fixed ID to access the system. By doing that I could test the reaction towards the eventuality of a typing mistake without coding any complicate logic. When the page is loaded, the "Next" button is disabled until ten digits are entered in the text panel. Once the field is filled, the button turns orange and ready to end the step.



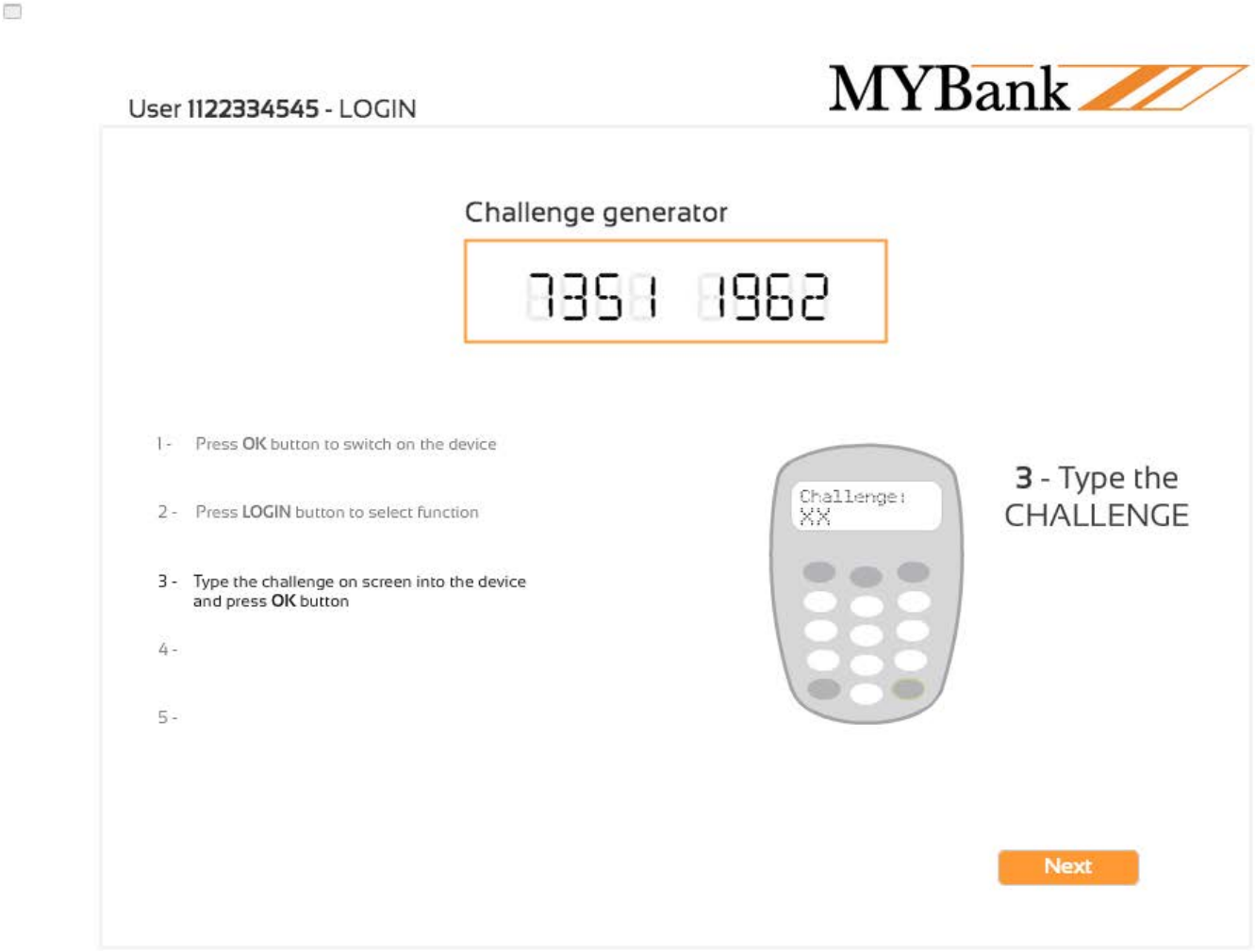
Pic.8 - User ID screen before (top) and after (bottom) a valid user ID is typed.

In case of a wrong user ID (Pic.9), a message of error appears between the text panel and the buttons. Even though the use of error messages should me replaced by re-designing applications in a way that makes impossible for the user to make mistakes (Cooper, Reimann and Cronin, 2012), in this case it is strictly necessary to give a direct feedback about the entered user ID. The error message doesn't pop up as an alert box that requires an extra action in order to continue but is presented as a visual modeless feedback. This type of feedback visually gives exact information about the status of the process being modeless in the sense that the user doesn't have to perform any special or extra step beside checking and correcting the inserted data in order to fix the error and continue (Cooper, Reimann and Cronin, 2012).

Pic.9 - Message of error when a not valid User ID is entered.

Once the "Next" button is clicked, the challenge page is opened. The goal of this page is to let the user perform the challenge task on the device before pressing the "Next" button once a response code is shown. This step was quite long discussed since, according to the "economy of form" principle, one of the elements of good interface design is to use only the screens and widgets necessary to accomplish a task (Cooper, Reimann and Cronin, 2012). In my case, I decided to separate the challenge instructions from the response typing screen in order to test the eventuality of usability value by reducing the range of possible actions on every screen to one. My idea was to verify if a longer but, theoretically, simpler process would optimize the user's performance even requiring a slightly longer time to be completed.
From the top to the bottom, there is a scrolling challenge box, a dynamic instruction panel and a "Next" button. The scrolling challenge box uses animation to visually show to the user that the challenge code is generated "casually" everytime. This should let him/her understand better its security purpose and without doubting about the possibility of using it more than once.
Right under it, another animation panel provide visual instructions about the process required in order to obtain a response code. The panel is composed by two parts: the left one where a dynamic bullet list explains the process with words and the right one where an animation graphically shows each step.
The dynamic bullet list is composed by five steps and has two different animation cycles. In the beginning, in fact, every point fades in from transparency to 100% of opacity to fade back to 60% when the following point comes up. In this cycle, the only part of list that appears from the

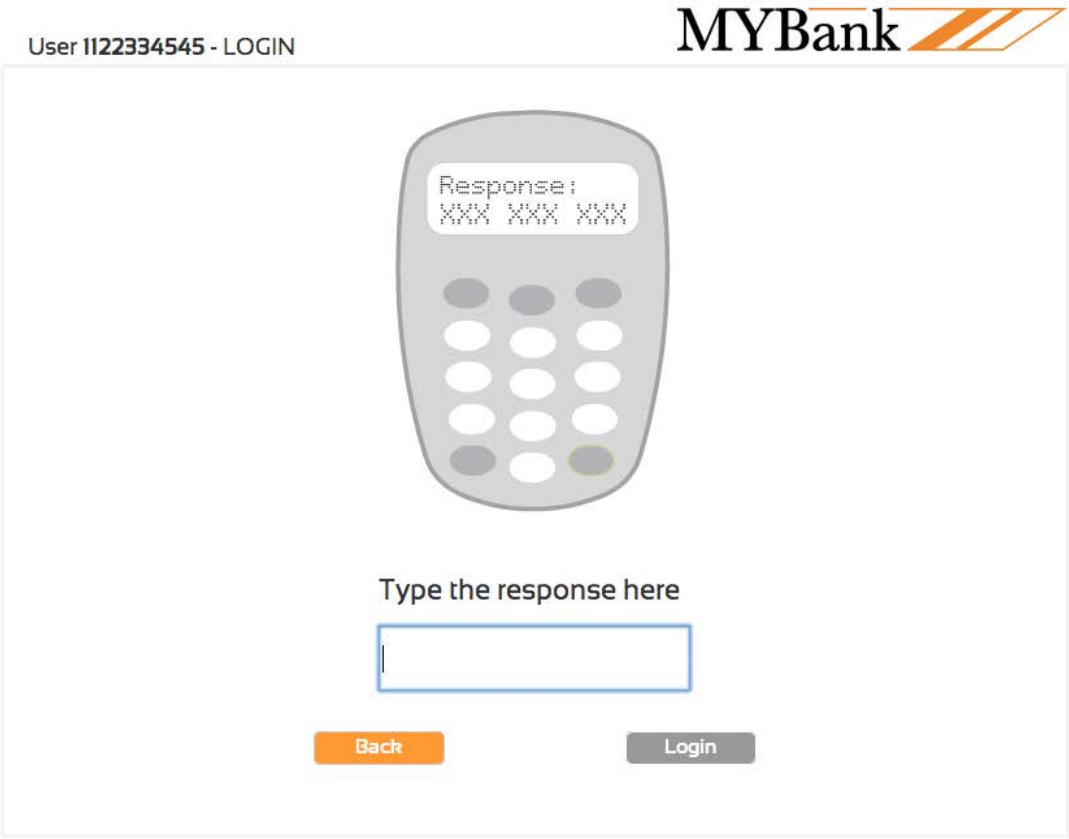
beginning is the list number before each step in order to tell the user from the beginning how many steps are going to appear. After the first cycle is completed, and all the points are appeared, a second cycle of animation starts. In this second part the points stay still on the screen with an opacity value of 60% before fading in to 100% when highlighted. This solution helps the user to follow the steps with a precise order in the beginning while leaving the possibility to go back and forth through the list at a second time.



Pic.10 - Overview of the challenge page. The animation is at its first cycle and the 3st step has appeared in the dynamic bullet list (left) while visually showed by the animation (right).

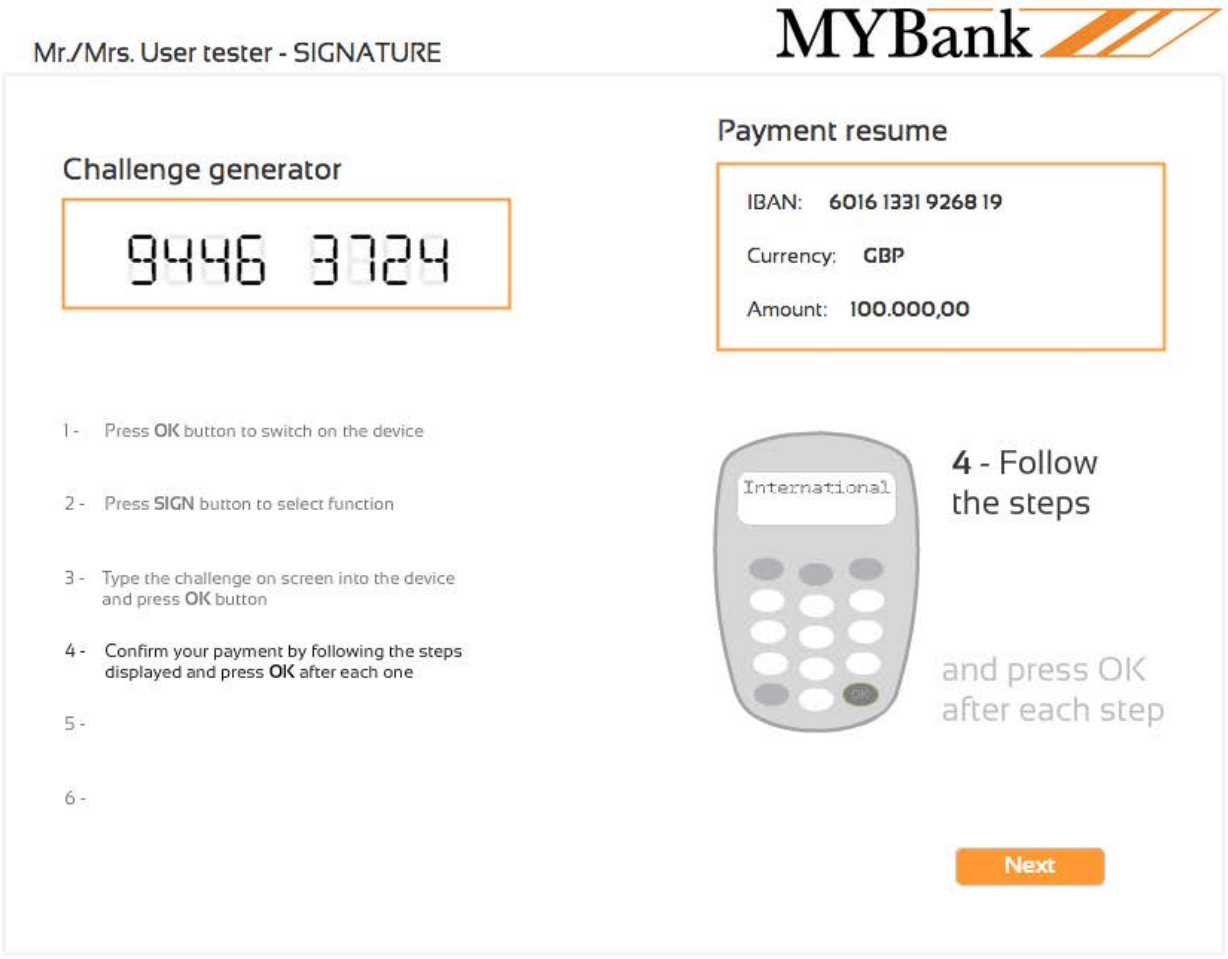
On the right side of the screen, synchronized with the bullet list tempo, every step is illustrated graphically to actually show the meaning of the instructions to the user. This part is intended to help the users with no experience with technology such as old people or just people having issues regarding the instruction's language. As an extra help, each point is summarized around the device animation in order to allow the user to follow only that part of the screen without missing some written instructions.
On the top-left side of the screen, outside a small outline defining the working area, the user's provided ID is reported giving the possibility to double check it. Once the response code has appeared on the token's screen, the user is invited to press "Next" to proceed.
In the response screen (Pic.11), keeping the same layout as the previous page, there's a graphical representation of the token with an animated pulsing response that once again shows what "response code" is referred to and where is it located. Right under it there's a selected text panel, with the same visual properties as the one where

the challenge was showed before, where the user is asked to type the response code back. Finally, beside the "Login" button to end the process, a "Back" button let the user go back to the previous step in case he accessed the screen without having inserted the challenge on the token.
The use of metaphoric elements to give extra feedback about the system has been avoided to keep the interface as simple as possible.
After the login phase, the user is invited to perform ether a national or an international payment even though this section of the site, not being part of the use case, was kept as in the current TryEzio system.
Once a payment is selected the signing process is conducted with the same modalities as for the login phase with the exception of the international payment (Pic.12). In fact, being necessary as stated before to re-type the payment data into the token, the interface presents a dynamic text field resuming everything the user is asked to confirm. On the top-left part of the screen, since the user is now logged in, he/she is identified by his/her name substituting the user ID.

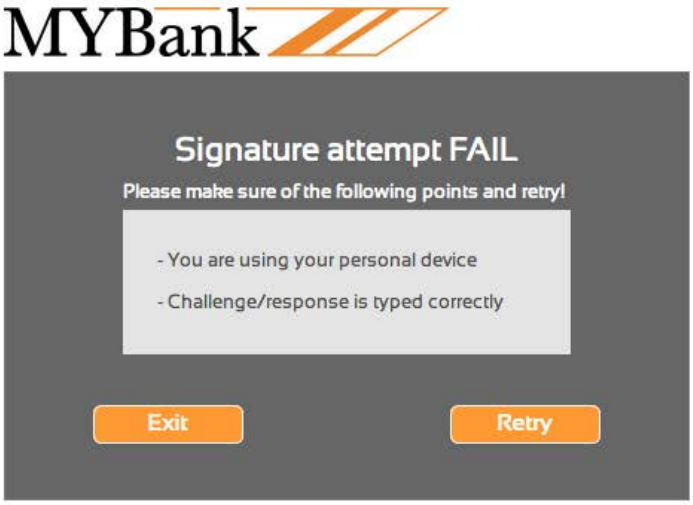


Pic.11 - Overview of the response page during login. On the animation's device screen, the digits are represented with an "X" to not let the user confuse the example with the response obtained with the token. Since the token is not connected to the system in any way, in fact, it wouldn't be possible to show the actual response number on screen.

If an error occurs at the end of a login or signing phase, the user is redirected to an error screen (Pic.13) where he can ether choose to re-try or to exit the system. The error message, keeping a positive approach, gives the user the information he/she needs to make an appropriate plan to solve the program's problem (Cooper, Reimann and Cronin, 2012). While in case of a failure during the login, the user is asked to start from the beginning (user ID identification), if an error occurs during the signing phase he has the chance to try to perform the signature again while being still logged in into the system.



Pic.12 - Overview of the challenge page during signature for international payment.



Pic.13 - Message of error for signature attempt failure.

3.4 Usability test

Once the first prototype was developed and published, I set up the main part of the usability study: the usability test.
The test was conducted in English, as standard language adopted for my research, in order to let any user be able to perform it.

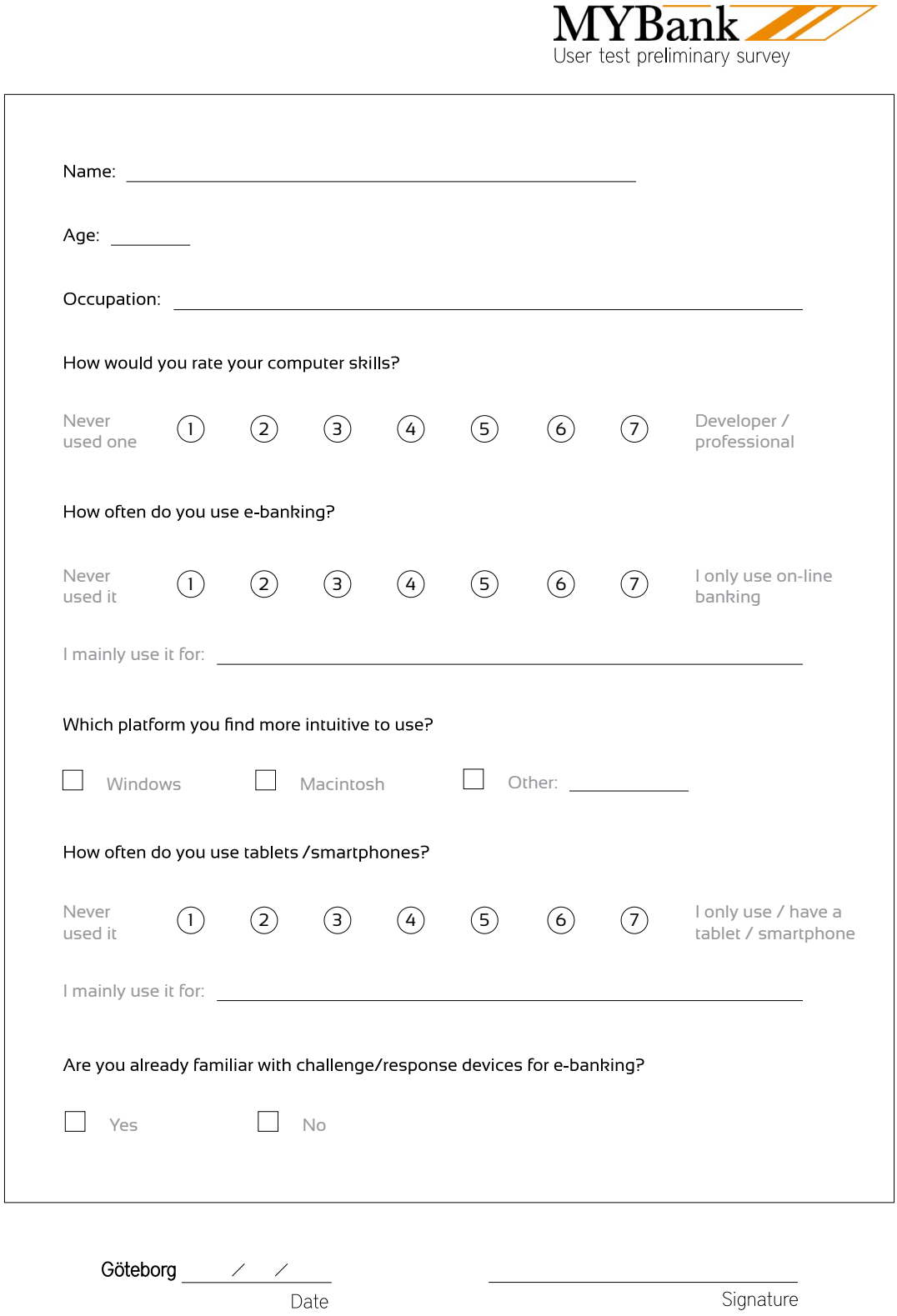
3.4.1 Goal

The goal of the usability test was to measure how well different users succeed to complete both a national and an international payment using the new system's prototype from both laptop and tablet. Since the current system hasn't been tested, the expected results aren't concerning any comparative values between that and the prototype. The test, in fact, is mainly aimed to reveal areas where users have problems understanding and utilizing the system, as well as places where users are more likely to be successful (Cooper, Reimann and Cronin, 2012) in order to delineate design guidelines.

3.4.2 Preliminary questionnaire

The test settings were defined focusing on the main idea of tracing a sort of profile of the participants in order to observe possible patterns and relations between behaviors and personal backgrounds.
For this reason the test session starts with a short questionnaire to fill in (Pic.14).
The point of the questionnaire is to collect basic demographic data and details on personal user experience to be used as background information to find out the range within the sample group (Preece, Rogers, Sharp, 2002).
Different questions in the questionnaire are presented with different response formats. In particular, it features open questions, semantic differential scales and check boxes.
The first three points are purely demographic and have an open format. I chose to not provide any range to choose from about age and occupation in order to make it quicker to answer and, possibly, more precise. Even though many people don't like to give exact indication of their age or occupation, since the testing environment was quite close and reserved I let the participants declare exactly these parameters. While age, as it will be shown in the next paragraph, was the main parameter on recruiting participants, the question about occupation was intended to help verifying possible patterns in the use of the system compared to type of everyday working environment.
The first core-question is closed and presents a semantic differential scale response format. This kind of format in aimed to explore a range of bipolar attitudes, represented as a pair of adjectives, about a particular item (Preece, Rogers, Sharp, 2002). In this case the question asks the user to self-evaluate his/her computer skills in a range between the "never used one" and the professional level as in the case of a developer. This question is based on the assumption that computer professionals have a complete different approach towards digital systems than people that use computers just as a tool in everyday life.
After finding out the level of expertise towards computers, the following question keeps the same format to locate the users' internet baking habits in a range between the ones that perform every bank activity via telephone or by going to the physical bank and the users that perform every task using internet banking. The question is followed by an open sub-question about the personal main e-banking operations. This step is aimed to explore whether the users usually use e-banking just for some simple tasks such as checking their account and paying bills or they actually make use of the whole functionalities such as managing accounts and savings.
After that the user is asked to answer a check boxes-structured question about the operative system he/she finds more intuitive and is intended to connect possible behaviors to personal habits related to the each system's specific dynamics.
Since part of the test will be conducted on a tablet or smartphone, following the same structure and logic as for the e-banking question, the following question features a semantic differential scale and an open sub-question to evaluate users' attitude and habits about the use of touch screen based

devices. The point of this step is based on the idea that users which are not used to such devices may fail to perform the requested task for different causes than the system's design. Finally, in the last question the user is asked to check a box whether already familiar or not with challenge/response devices. While familiar users could assume how the system works before reading the instructions, at the same time they could be used to different logics and get confused by the actual task.


MYBank
User test preliminary survey

Name: _____

Age: _____

Occupation: _____

How would you rate your computer skills?

Never used one ① ② ③ ④ ⑤ ⑥ ⑦ Developer / professional

How often do you use e-banking?

Never used it ① ② ③ ④ ⑤ ⑥ ⑦ I only use on-line banking

I mainly use it for: _____

Which platform you find more intuitive to use?

☐ Windows ☐ Macintosh ☐ Other: _____

How often do you use tablets /smartphones?

Never used it ① ② ③ ④ ⑤ ⑥ ⑦ I only use / have a tablet / smartphone

I mainly use it for: _____

Are you already familiar with challenge/response devices for e-banking?

☐ Yes ☐ No

Göteborg ___/___/___ Date

_____ Signature

Pic.14 - Preliminary questionnaire.

3.4.3 The task

The actual test consisted in two tasks:

- To perform a national payment running the on-line system on a laptop
- To perform an international payment running the on-line system on a tablet

The idea behind this test structure was to let the participant first approach the system with an easier task on a bigger screen in order to let him understand the basic logics. When approaching the second part, users tend to feel quite more secure about the system and to go quicker trough the task. For this reason, I wanted to keep the task quite challenging by gradually introducing extra elements to keep the participants focused. In fact, if using a tablet instead of a computer could already be felt as difficult for some users, once they come to the signature step in the international payment, they are required to perform some extra steps. At this point, even the users who felt completely able to perform the task without taking care of the instructions, were forced to observe them. In this way I wanted to evaluate the actual effectiveness of the interface to introduce new aspects of the system to the user.

3.4.3 Un-structured interview

After the test is completed, the session ends with an un-structured interview where the user is asked to talk about his experience.
Following a general interview agenda to guide the conversation through the study goals and questions while leaving the user free to follow new lines of inquiry, the un-structured interview is a very effective way to generate rich data (Preece, Rogers, Sharp, 2002). In fact, the interviewee often mentions aspects and points that the interviewer may not have considered and can be further explored.
The interview agenda was meant as general and to be adapted depending on my observations on the user's performance and on the user's comments and answers. The main points are:

- Was the task easy? First impressions about the system.
- Is this system similar to the one you're used to?
- Did you mostly follow the instructions bullet list on the left or the graphical animation on the right?
- Did you notice the graphical animation? Was it useful?
- What was the most difficult part of the test?
- Compared to your e-banking site, would you say this was easier?
- Did you feel the process to be long/stressful?
- Final comments

Since most people are incapable of accurately assessing their own behaviors (Pinker, 1999) and many, out of fear of seeming inappropriate, may avoid talking about software behaviors that they find problematic or incomprehensible, an efficient technique to collect qualitative user data is to combine observation with interviews (Cooper, Reimann and Cronin, 2012). In my case the interview, being performed right after the observation, not only is intended to complete the observed behavior with comments and to provide extra input, but also to clarify direct inquiries I had the opportunity to notice during the test.
In order to take trace of the interview in an effective way without distract the users or let them behave differently (Cooper, Reimann and Cronin, 2012), the interviews are recorded from the cameras' built-in microphones in the same take as the test. In this way, even if the user is aware of the recording, he doesn't notice any actual difference in the environment and tending to not feel the effects of recording.

3.4.4 Participants

An e-banking system is a product that is intended to be used universally by a bank's customers. A bank has different types of customers and different services to fulfill their different needs but everyone is asked to login into the system and sign transactions at the same way. For this reason I had to recruit participants in a way to represent as much as possible heterogeneity of the users range.

Starting from this idea, and observing other examples of studies concerning bank's services such as Online banking and demography (Dapp, 2012) and Online banking, what we learn from the differences in Europe (Meyer, 2006), I decided to cluster the test participants by age. In fact, although age seems to not affect the overall attitudes towards computers, it affects the dimensions of comfort, efficacy, dehumanization and control in general (Czaja, Sharit, 2013). Since one of the main factors that affects attitude towards computers is experience (Czaja, Sharit, 2013), I outlined three age clusters by assuming a relation between their average experience with computers and the diffusion of such technology in the time they grew up.
In particular, starting from the adult age, the age clusters were defined as follows:

- *Between 18 and 34 years old*: people that had experienced personal computers connected to the Internet while growing up. Participants within this cluster usually perform basic e-banking actions such as paying bills and receiving salary but rarely perform big financial moves and manage serious amounts of money.
- *Between 35 and 54 years old*: core e-banking users, they probably faced computer technology and Internet connection from adult age or while working but they became quite used to it.
-*Over 55 years old*: the most critical segment of users for e-banking, many of them has never really performed an internet action (O'Really, 2008). Average banking users, they usually relate to the physical bank institution.

Within each cluster, I tried to keep gender diversity equal in order to obtain more complete results. Even though there are no apparent gender related attitude differences between male and female users, male users tend to have more experience in advanced computer-related fields (Busch, 1995).
About recruiting test users, since many professionals recommend from five to twelve people (Dumas, Redish, 1999), I planned to test twelve participants for each test iteration in order to have four representatives for each cluster (possibly two males and two females). Participants were recruited by informal invites within my personal network and two cinema tickets were offered as a reward.

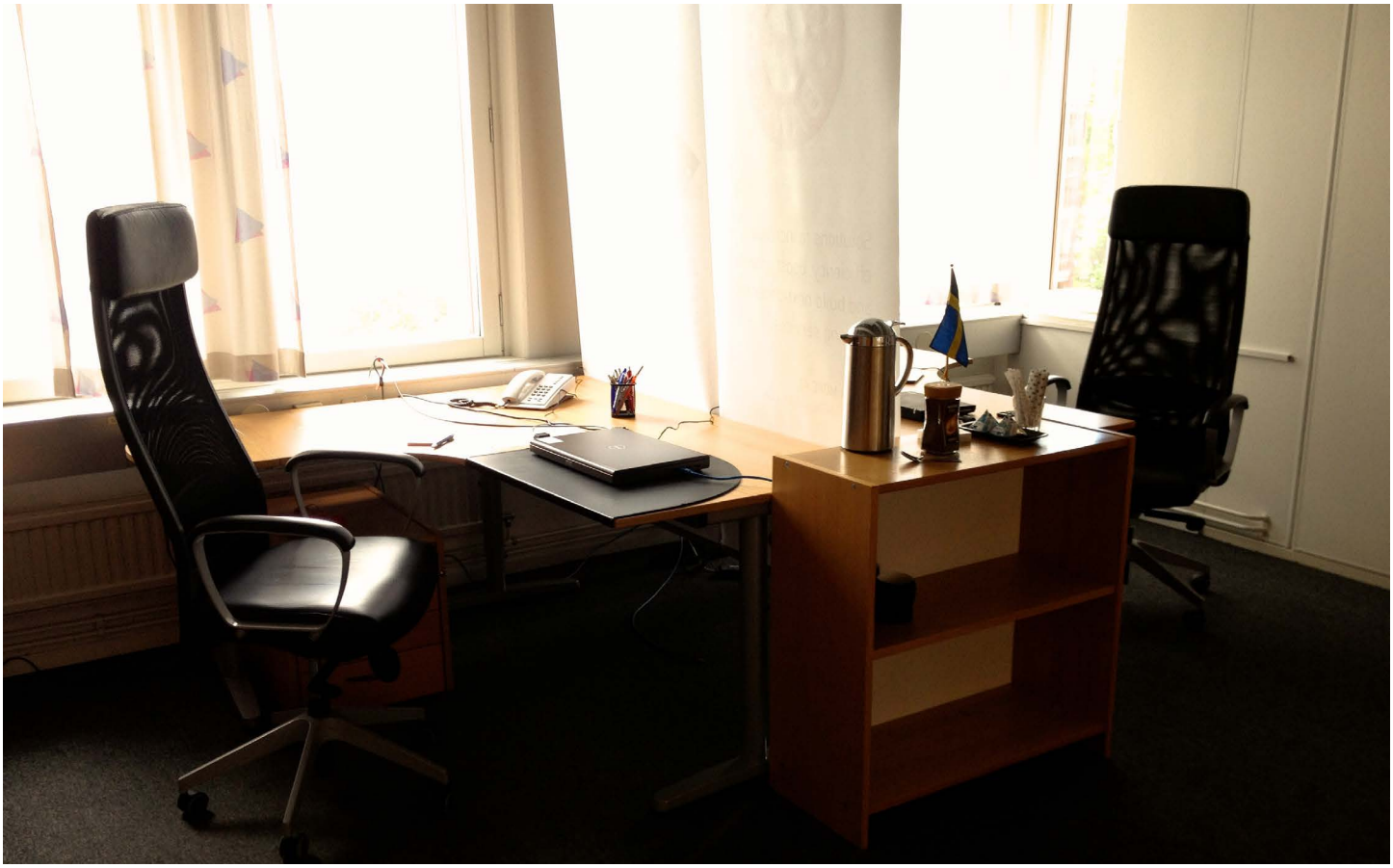
3.4.5 Test lab configuration

The test lab was set up together with the company and is fully equipped to be portable. It is composed by two positions placed one in front of another and separated by a cover that makes it impossible for the tester and the participant to see each other (Pic.15).
The test station, on the right side (Pic.16), features two cameras with incorporated microphones and a screen-recoding device plugged into a laptop. While the first camera points to the participant's face to observe his reaction during the test session, the second camera points to his/her hands to observe his/her interaction with the token. Since the test is meant to be performed with different devices, the second camera is also used as main screen detector for tablets or smartphones. On the test side, a paper card with a user ID and a PIN code to use during the test and a short text to help the user to remind the basic given instructions were provided.
All the observing devices are connected via USB to the observing station on the left side of the table. Here, a professional observation software called "The observer xt" is installed and allows the tester to synchronize and record different devices at the same time (Pic.17).
When the first part of the test regarding the user performing an international payment using the laptop is concluded, the software settings are changed to ignore the screen detection and augment the quality of the second camera pointing on the device's screen.

Pic.15 - Test lab overview.

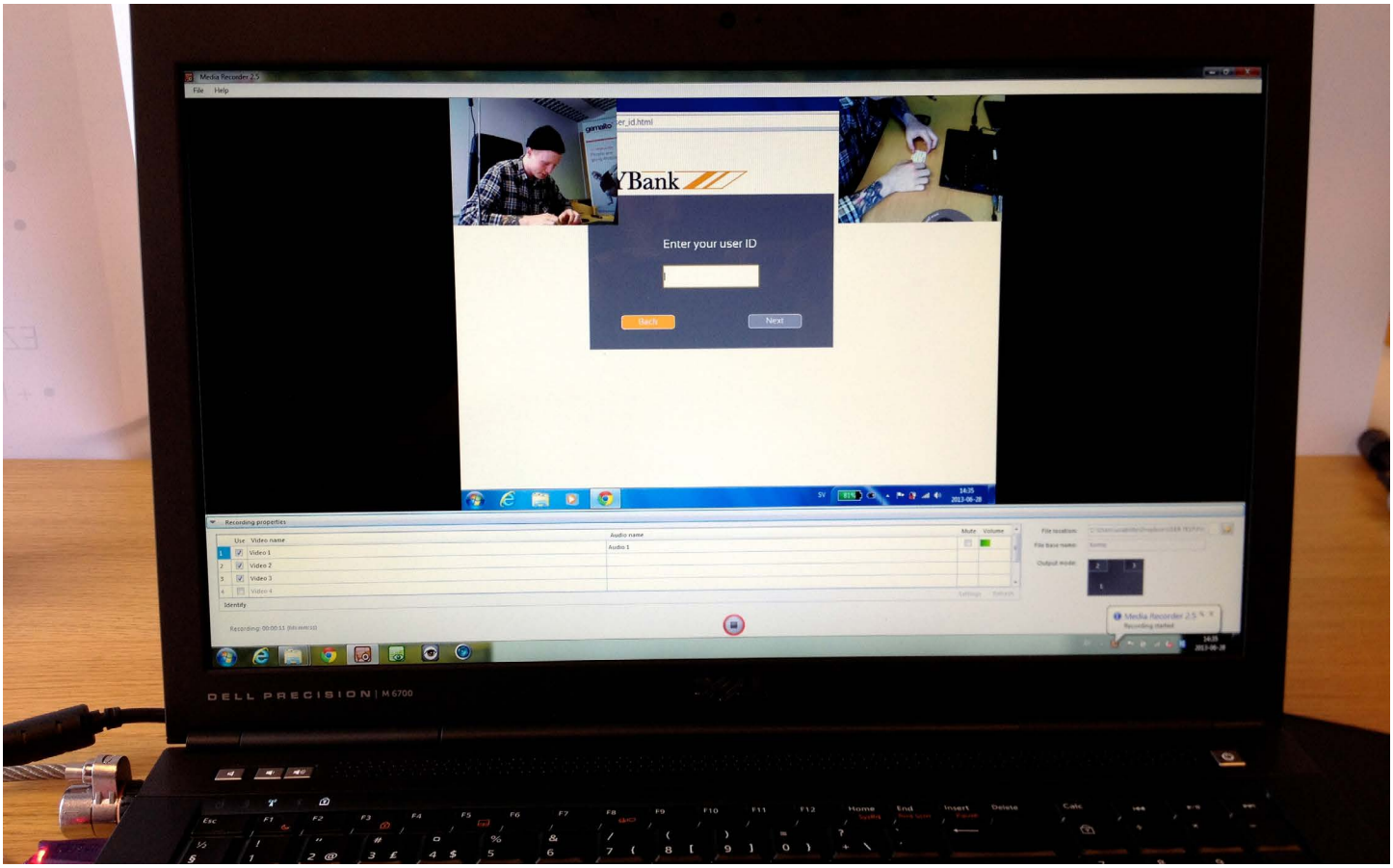
Pic.16 - A participant sits by the test station to fill in the preliminary questionnaire.

Pic.17 - Observing station configuration for login and national transaction signing with system ran on a laptop.



Pic.15

Pic.16



Pic.17

3.4.6 First test and results

The first test was conducted in two weeks for a total of nine participants. Since the first few test sessions, a quite clear pattern was observable both in behavior during the actual performance and as feedbacks from the interviews. In fact, since the feedbacks were quite homogeneous and the need of a prototype refinement followed by another test iteration was clear, I decided to end the test after the first cycle of booked participants was concluded.
The results were analyzed by relating the observation of the test recordings to the preliminary questionnaires and the final interviews. Each user's performance was resumed into an analysis form composed by a user's profile, first task observations, second task observations and personal feedbacks.
The first age range (18-34 years old) featured 5 users (3 males and 2 females) between 20 and 31 years old, the second one (35-54) 3 users (2 males and 1 female) between 35 and 46 years old and the third one (55+) just one 58 years old male user.
While no particular relation between gender, different backgrounds, computer skills, habits towards technology and test performance was noticed, some critical aspects clearly delineated. For what concerns the first age cluster, no particular problems were observed during the first laptop based task since all the users carefully followed the instructions at least for the login phase. Two users seemed quite confused by the animations showed in the challenge page while the others didn't show any clear sign of emotion. During the second task with the tablet, most users kept carefully following the instructions while two users (both computer experts), tried to speed up the process and one of them pressed the "Next" button in the challenge page without taking care of completing the process into the token. All the users had quite serious difficulty performing the international payment. This happened also because, in the payment resume box, I named the account number "IBAN" while the device was

asking for "Account number" in the first screen. Most users reported to have been quite confused by that inconsistency issue.
The main feedbacks from the interviews were concerning the amount of motion in the interface that happened to be annoying and stressful for the majority of the users. None declared to have observed the graphical demo animation on the right side of the screen that, while in few cases was completely ignored due to add-blindness phenomena, in others was perceived as stressful and confusing since it was repeating the same information present in the list. Everyone found the bullet list to be very useful and few users declared that the dynamic list animation was helping to follow the steps. Besides these issues, most users declared to perceive the system as quite easy and in some cases trustful and secure even though not better than the one they were used to.
The users within the second age range generally approached the system in a less careful way. Two of them just read the instructions in the first login phase and then quickly performed the rest of the tasks without bothering instructions anymore.
No particular issues were noticed even while performing the international payment. The main comments from the interviews were again related to the amount of animations and motion and two out of three users felt stressed or annoyed by the use of an extra screen where to type the response back. One user declared that she felt nervous about it because she thought she didn't have enough time to type the response back before it would expire and two users believed they did something wrong when the international payment variation appeared on the token's screen.
As for the younger participants the entirety of the users declared to have used only the instructions bullet list as guide through the process.
Finally the only user within the older age range had some problems to understand the process in the first login phase due to a misinterpretation of the word "challenge" (he had to ask me what was the meaning of it in order to advance). Once he completed the first login phase he managed to go through both tasks in a quite flawless way being the only one to intuitively and immediately understand the international payment step. In the interview, he claimed that the system's flow was quite logic he didn't have any particular issue besides that for the first step.

** For complete 1st test results see attached "Appendix 1"*

3.5 Second iteration

3.5.1 From results to guide-lines

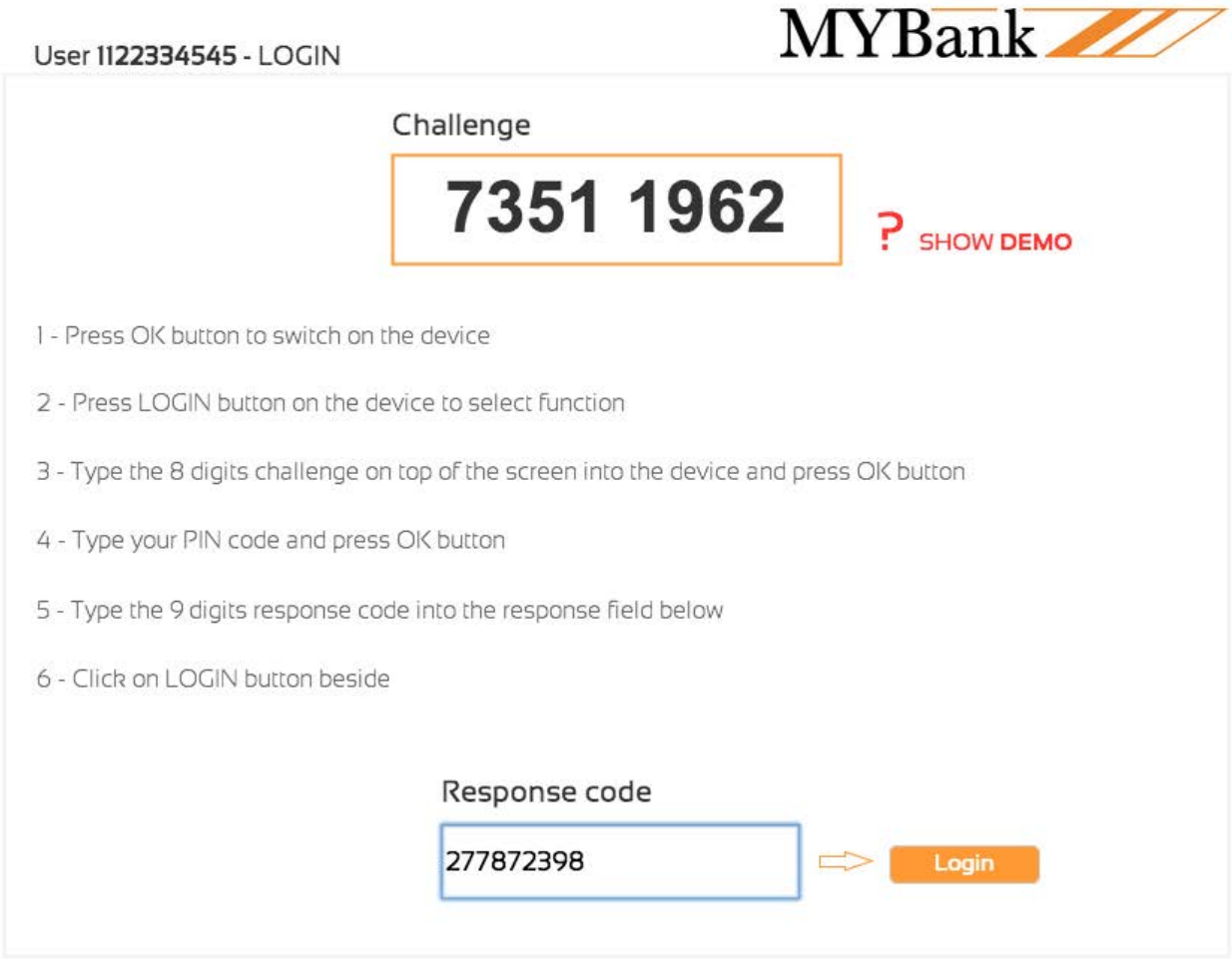
The test results delineated some critical aspects in the prototype. This led to the need of a design refinement based on the feedbacks obtained from the first test iteration to be once again tested in order to evaluate the efficiency of the improvements by the comparison of the performances.
Since, as stated before, the observations and feedbacks showed a quite homogeneous pattern of behavior and perception, it was quite easy and natural to delineate the design guidelines that led to the second prototype version.
The main points are:

- Strong reduction of motion
- Graphical demo animation as an option
- Challenge and response screens merging
- Better instructions for international payment

These design guidelines are sorted in a hierarchic order of importance derived by the test results in order to constitute a sort of precise design work schedule.

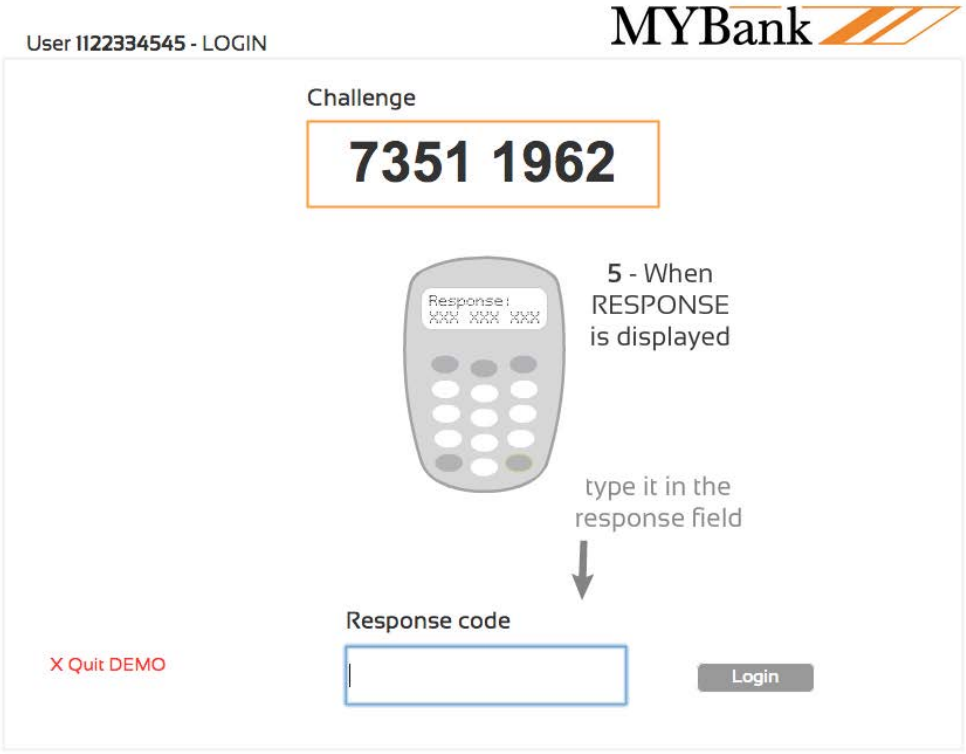
3.5.2 Prototype re-design

Considering the design guidelines point by point, the re-design of the prototype started by focusing on strongly reducing the amount of motion in the interface (Pic.18).
Even if the scrolling challenge was intended to hint the logic behind it to the user in order to let him feel more secure about it, it was actually perceived as stressful and, as declared by a user, could be intended as something too dynamic that would quickly disappear. For this reason, keeping the same visual properties, it was replaced with a static challenge indicator.
The central space was entirely dedicated to the instructions bullet list. The list was re-designed



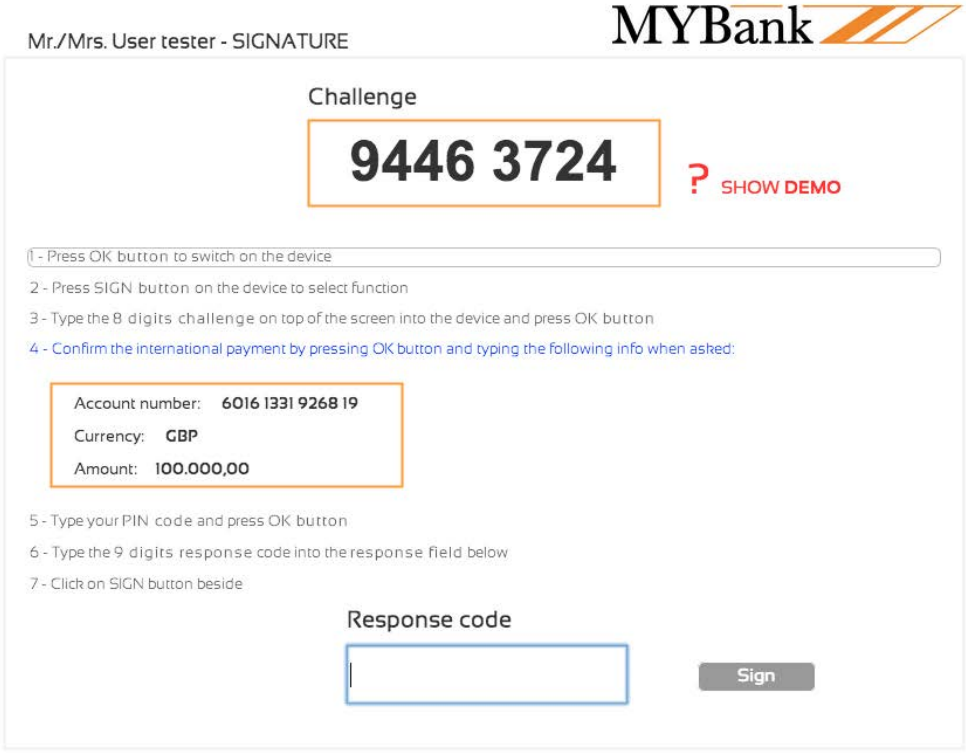
Pic.18 - Re-designed interface of login challenge/response screen.

to be static but a hidden feature has been added in order to keep assisting the user to follow the steps as claimed by some users during the interviews. On page load, in fact, the first point of the bullet list is highlighted by a light contour. The user, by scrolling over the list with the mouse pointer, can highlight each step in order to not loose the focus while shifting his attention between the token and the screen.
The graphical demo animation was kept as an extra optional (Pic.19) help since no user declared to actually have looked at it but I was still convinced that it could constitute a helpful tool for user with language difficulty or completely not used to technology. A "? SHOW DEMO" button placed on the top right corner, beside the challenge box, is used to make the demo animation start, using the whole central screen area and replacing the bullet list. Since, on the bottom part of the screen, the response box is now added, the animation ends by graphically pointing towards it and the "Login" button by the use of two arrows in order to more clearly show the whole process. The instructions bullet list can be reset at every time by pressing the "X Quit DEMO" button on the bottom left of the screen.
By placing the response box on the bottom part of the page, after the bullet list, the whole challenge/response process is now performed in one screen but, at the same time, the visual layout helps defining the interaction flow.
While the response has been typed, an extra orange arrow appears and points to the "Login" button, constituting an extra feedback for the user (Pic.18).
Finally, to make the international payment step more intuitive, the payment resume box was incorporated in the bullet list and the point con-



Pic.19 - Optional graphical demo animation.

cerning the extra steps was colored with the same blue used for the rollover style. In this way the user can directly relate the payment resume data with the part of the process where it would be needed following a mono-directional top-to-bottom flow (Pic.20).



Pic.20 - Re-designed international payment's signature interface.

3.5.3 Second test and results

The second test was conducted with the same modalities and settings as the first one but no participants from the first iteration were tested again to not maintain the same level of basic knowledge of the system while approaching it. Eleven participants between 23 and 56 years old took part of this test iteration: 5 users within the "young" age cluster, 4 within the "middle aged" and 2 within the "elderly". Even though, once again, I was ideally supposed to reach the number of four participants for each cluster, the recruiting difficulty together with the short amount of time and the uniformity of the results led me to end the test before reaching it. The quite wide range of age, backgrounds and attitudes towards technology provided me a good sample to evaluate the quality of the improvements.
The test was very successful since no user reported any specific issue or difficulty as in the previous version. No mistakes were made at any step of the process proving that even if, being the challenge and response in the same screen, the system was slightly more open to mistakes, the flow seemed to be very clear.
From the observations, the process was performed quite flawlessly by the majority of users besides the two older participants that had some minor issues regarding the dimension of the text and the written language.
Just few users declared to have noticed the Demo button. One 55 years old user, not feeling comfortable to let me notice she wasn't confident enough with written English language, explored the Demo function that, as I assumed when I implemented it, happened to be very useful in such scenarios. No users, on the other side, stated to have noticed the bullet list hidden highlighting function even though few stated its usefulness once introduced to it afterwards.
The international payment, still being perceived as slightly annoying and tricky for the amount of information to re-type, was performed quickly and correctly by the totality of the users. None, in fact, reported to have perceived it as a difficulty, proving the efficiency of the new layout configuration.

** For complete 2nd test results see attached "Appendix 2"*

4. Final observations

The test settings seemed to be quite effective to collect both observations and feedbacks. The participants were comfortable enough to behave in a natural way thanks also to the welcoming environment. The experience, in fact, revealed that warmly and informally welcoming the participants, offering them a nice place to seat and something to eat or drink, enhance the conversation flow and, then, the feedbacks' quality. The different nature and level of relationship with me (the test leader) was also effecting the way each person behaved and closer friends felt more free to openly talk about their opinion. On the other hand, strangers and people from different environments from the ones I'm into, happened to provide interesting feedbacks and may be more inclined to constructive feedbacks.
Even if the need of a specific app to run the system on tablets and smartphones was clear from the beginning, the second task was still performed on such devices (mostly tablet). The point of it was to collect observations and feedbacks about users' behavior and tendencies while interacting with the regular version of the website to spot eventual useful patterns to apply in the implementation of a future mobile version. The main feedbacks were about the need to constantly zoom in and out the interface and the keyboard dynamics. In fact, while users mostly declared to have performed the task quite easily anyway, the constant automatic appearing of the

screen keyboard was radically reducing the part of screen for the actual interface, especially if the device was hold horizontally, making the use of scrolling and zooming even more required and difficult at the same time. Another point to develop was the amount of data to load for each page that, mostly in the case of the first interface, was making the pages very slow to load due to the use of animations.
Comparing the different version of the prototype in relation to the test observations, a clear and incremental improvement can be noticed. In fact, the decisions taken to define the last prototype version matched the expected results. The main decisions such as the way motion was radically reduced and the challenge/response screens were merged resulted to be successful.
The bullet list highlighting hidden feature wasn't noticed by any user and three options can be considered: removing it, keeping it or trying to introduce the users to it. Even though I couldn't observe it during the test, I think it could help users having quite serious issues to more easily follow the steps while using the token. The feature can be kept as hidden while some small hinting could be added after a certain amount of time that the screen is loaded in order to not overload the screen and interrupt the flow for expert users.
The visual demo mode button wasn't noticed by many users and could be moved or other ways to trigger the demo modality can be explored. For example, it can appear as an assistant during the first access attempts with the option of not showing it again. Another way, could be to let the "Show DEMO" button dynamically appear after a certain amount of time the user doesn't seem to progress. In this way it can be placed in a more central position and it would be clearly visible for the user having difficulties.

5. Discussion

5.1 Discussion around methodology

The master's thesis was conducted within a corporate environment and has always followed a quite strict business oriented approach. Since the scope of my task was limited to explore the graphical user interface of the web-site, I have not explored the possibility to change the eco-system or the security token itself.
The current system settings, especially the limitations imposed by the need to keep a high level of consistancy between the web interface and the token, have driven and affected the interaction flow. This can be seen as supporting the idea that security and usability cannot be considered as additional features to be applied at the end of the design process but they have to be incorporated simultaneously through the whole process (Yee, 2004). On the other hand, since no other solutions but the ones designed to fulfill the imposed parameters have been tested, this point didn't lead to a design guideline. In order to explore this point, a totally new system including both interface and token could be designed as a concept to compare to the results currently obtained.
In the beginning of the research, I had many different ideas about how to implement the system by radically modifying its logics from the roots. A big amount of time and research together with different professionals was required to comprehend the actual boundaries of the task. For this

reasons, while some decisions have been taken to delineate the focus of the research, some possible aspects have been excluded. In fact, the following research questions, stated in the beginning of the process, weren't further explored in order to focus on other aspects:

- Is it needed to make the users understand the dynamics of on-line frauds and the importance of safety precautions in order to let them feel safe and comfortable? How can it be done without overloading the system of not-core information?

- How can the interaction of the system eventually help the user to more closely relate the virtual to the tangible transactions affecting not only the flow but the actual perception of money value?

Thanks to the test being set as quite open to investigate different aspects, in particular during the un-structured interviews, I had the opportunity to collect data and observation contributing to the first sub-question I avoided. In fact, many users showed a clear change of attitude towards the extra-efforts they were asked to perform during international payments once informed of the reasons why they were required to protect them. This observation was not reported as a guide-line since this point of inquiry was decided to not be explored during this research.
In order to explore these points, in fact, I think that the process should have been approached in a more abstract way in order to deeper investigate the attitude of the user towards a certain kind of inputs rather than the efficiency of the system. For instance, small different prototypes of single steps could have been developed and different kinds of tests could have been explored. While the test I developed to evaluate the efficiency of the prototype focuses on observing how the users relate to it, a psychological investigation of personal dynamics towards the perception of safety and money value would have been required to investigate these aspects.
A preliminary study about perception, related to the actual process, could have led to a quicker development of an efficient prototype. In fact, the issues related to the first prototype's amount of motion could have been predicted before the test, leaving the chance to investigate other aspects.
Another improvement in the process would be to actually have tested the current TryEzio platform provided by Gemalto. In fact, due to lack of time and the difficulty to set up a test and recruit participants, I carefully analyzed the current system, relating my observations to theory and formulating assumptions but no actual test on users has been conducted. This led to not have any comparable data between the current system and the prototypes but only between the first and the second version I developed.
The test participants were mostly Swedish but no actual distinction was made based on nationality during the recruiting. The test was also conducted in English in order to be performed by anyone. These factors could have affected the results in both good and bad ways. From one point of view, in fact, having only Swedish participants testing a system in Swedish, would have been more effective towards the pure evaluation of the interface making it easier to compare the results. On the other hand, the fact that some users weren't able to completely understand the written instructions, resulted in the possibility to evaluate the efficiency of the visual demos in such eventuality. Since the final users of an e-banking system, even if mostly, will not be only people from the same country, the fact to not have considered nationality as a relevant recruiting parameter, could actually have helped to represent the user group.
The recruiting of users within purely demographic age clusters could be improved by defining different types of clusters. Even though the first test results didn't show any particular pattern between users' profiles and their performances and the demographic parameter to define clusters revealed to be quite effective, some models such as personas and scenarios could actually be implemented to define user categories even if the use case focuses on a system that cannot be shaped on specific users as stated at the point 4.3.3.
The methodology of the process was specifically shaped to investigate the final research question focusing on each of the points introduced in the research-sub-questions. The prototype, in fact, has been designed and refined in order to make observations aimed to state a list of guidelines with the goal of optimizing the interaction flow and user experience during the use case as stat-

ed in the main question. While the observations were mainly conducted to find out the general attitude and performance while performing the task, the questions asked during the interview were quite specifically oriented to explore the points of interest stated in the related sub-questions. The un-structured interview, in fact, being a really good tool to find out certain focus points without limiting the range of answers, strongly contributed to obtain quite specific answers to quite broad questions.

5.2 Discussion around user test results

The list of design guidelines obtained as an outcome of this research, being quite specific, are directed to interaction designers that operate within the company Gemalto as users. In fact, the whole research was intended as an operative tool to improve future internal development of specific products offered by this company.
The results of the tests provided a quite big amount of feedbacks and big part of them were obtained from the un-structured interview. From this type of observation, a lot of unstructured data is generated, which can be very difficult and time-consuming to analyze besides being almost impossible to replicate (Preece, Rogers, Sharp, 2002). During interviews, in fact, users felt quite free to provide comments even if, in some occasions, they were concerning something out of the use case. Even in such occasions, I decided to not interrupt them but to just let them notice it afterwards. This strategy was motivated by the fact that the more feedbacks were collected, the more knowledge about the whole system was generated which could be used within future research scenarios.
Many users, if not almost everyone, asked me about the need to re-type payment information while performing an international payment. After giving them an explanation of the reasons why that step is required in order to provide a safe environment, the users tended to seem way more inclined to perform the extra step. This result, which I didn't include in the final result, showed the relevance of aspect that I decided to not explore within the current research: the need of making the users understand the dynamics of on-line frauds and the importance of safety precautions in order to let them feel safe and comfortable.
Another point of interest that could have been explored for research purposes was the token's interface. In fact, many users reported questions or provided feedbacks about the token's behavior with a particular focus on the role of the "OK" button. A structured report about the tests' results concerning the users' interaction with the token could have been provided together with a general concept idea about possible improvements.
The results of the first test showed that the first prototype was quite inefficient in some points and especially about the international payment step. This led to re-design the interface making a quite big step back compared to the direction I was going towards. In fact, two big aspects that were making the system way different from the actual one were actually re-considered: the challenge/response process divided in two different screens and the visual approach to instructions. This need to get back to something more similar to the initial state was perceived as quite frustrating since it was stating a sort of failure in the attempt of radically changing the state of the system. On the other hand, this result was quite constructive since, even though the results it wasn't matching my assumptions, it provided me a quite clear feedback that led to define the design guidelines.
The design guidelines constitute a quite direct answer to the main research question:

"How can Gemalto e-bank service be designed in order to optimize the interaction flow and user experience during safe login and signing actions through external devices on different platforms such as laptops, tablets and smartphones?".

In fact, they are intended as a list of directions to be considered when designing a Gemalto e-bank service in order to optimize it in such way, following the different focus points listed in the research sub-questions.

- *While banks constantly research and implement high-security systems to avoid on-line frauds, users might perceive them as barriers to overcome. Can*

usability meet security to design a high-flow system where safety precautions, beside actually protect the user, will let him feel safe and comfortable?

This point can be considered as a common aspect that has been investigated and answered trough the whole guidelines list. In fact, every guideline is intended as a way to make the user feel safe and comfortable while going through a high-secure process. This can be particularly related to the step-by-step interaction flow and its related possibilities. In fact, following the Path of Least Resistance design principle introduced by Yee (2002), adding some apparent inconveniences, such as a longer process, a payoff is provided in form of reduced error possibility thanks to the use of checkdigits and constant feedbacks after each step.
After analyzing the observations and the results from the tests, it can be said that usability can meet security in terms of user´s perception of the system. In fact, almost the totality of the users declared to have felt comfortable and also safe. In some cases, the users stated to have felt even more secure while performing the longer steps such as the international payment resume.
In order to further improve the system from this focus point, a future system has to be designed taking into account both usability and security from the start for the whole system composed by both devices, as stated by Yee (2004).

- Is it efficient, in terms of usability, to guide the users through the login and signing process by articulating the interaction flow on a longer but easier process? Does the use of dynamic visual assistance help or confuse the users?

The comparison of the observations and results from the first and the second test iteration has brought to a quite clear answer for this point. In fact, as stated in the design guidelines, articulating the process through a step-by-step interface structure can be effective even though it is important that related actions are grouped in the same step.
The use of dynamic visual assistance can be useful but, at the same time, quite stressful and confusing. For this reason, it has to be moderated and, possibly, available as an optional extra help that each user can choose to use.

- Are different users from different age ranges familiar with secure on-line banking devices? How they perceive the use of this kind of solution? Which level of help do they actually need?

Different users from different age ranges had taken part of the test and everyone showed to be quite familiar or at least inclined to the use of this kind of solution. No user declared to have any sort of issue with the device in itself and the majority was already using something similar at home. Even though different users needs different level of help, generally they showed to need basic and clear instructions to introduce them to the specific system in detail in order to let them be able to compare the new solution with the already known one.

6. Conclusions

This master's thesis research was conducted together with Gemalto, a digital security company that focuses, among other things, in secure home banking services. The point of the research was to investigate usability in secure login and secure transaction signing use cases. The research question was "How can an e-bank service be designed in order to optimize the interaction flow and user experience during safe login and signing actions through external devices on different platforms such as laptops, tablets and smartphones?". To answer this question, after having analyzed the actual system provided by the company, a working prototype was developed and tested to define a final improved version once again tested.
As a final result, the observations and feedbacks obtained during the first test iteration were compared to the once obtained from the second and final one in order to draw up a list of design guidelines. These guidelines are intended as universal directions to implement the design of future products which specific needs and parameters change from case to case.
By first trying to make the login and signature processes longer in order to guide user's attention and supported by a strong use of visual motions I after made a step back to a simpler interface. This led me to evaluate that users should be guided through an interaction flow where each action is concluded in a separate step and instructions are static, clear and consistent but, at

the same time, the possibility to have extra visual assistance is provided.

6.1 Design guidelines

As stated in the beginning, the final core result As stated in the beginning, the final core result of the research work wasn't a final product to be developed but a list of design guidelines to implement the design of the future products. In fact, security solutions for home banking are strictly related to each bank's needs and strategies and have to be specifically designed depending on these factors. The main research question was **"How can Gemalto e-banking service be designed in order to optimize the interaction flow and user experience during safe login and signing actions through external devices on different platforms such as laptops, tablets and smartphones?"** The following guidelines are the answer to this question based on the conducted research in form of a list of aspects to be considered during the design of such service in matter of login and transaction signing.

- *Step-by-step interaction flow:* Even if the process can be longer, to assist the user by the use of single-action screens can be effective. Quoting the research sub-questions, I observed that it is efficient, in term of usability, to guide the users through the process by articulating the interaction flow through a step-by-step interface. In fact, by doing so, the chance of committing errors, especially the ones related to a lack of concentration, is reduced. It is important, on the other hand, to not make the user confused about the utility of the step he or she is performing. Related actions have to be performed preferably on the same screen.

- *Moderate the use of dynamic visual assistance:* Animations can be very useful to show how to perform an action to the users whom are not comfortable or familiar with technology in general, but have to be used carefully. In fact, moving elements can be perceived as stressful and annoying or be ignored because confused for advertisements. For this reason a good solution would be to leave the possibility to show animations as an optional extra help.

- *Use of both clear written and visual instructions:* Even though most of the observed participants seemed to perceive the use of challenge/response solutions as easy and familiar, different users from different age ranges can have different needs in terms of assistance. To face this problematic, the use of both clear written instructions and visual assistance is effective to help users at different levels. Instructions, to be effective have to be simple and not conflicting. Visual demonstrations and written instructions have to appear separately in order to not be confusing for the user that wouldn't know which one to follow. In written lists, repetitive actions can be grouped but no step has to be taken for granted or avoided.

- *Use of check digit steps:* The use of check digits to confirm the validity of the entered identification data is very effective to reduce failures during the process. While used within a step-by-step interface structure, check digits are intended to stop the process in case of errors such as typing mistakes, giving the possibility to the user to re-try a single step instead of having to perform the whole process again. This point constitutes an example of how usability can meet security since the check digit steps, besides protecting the user, help him or her feeling safe and comfortable by giving constant feedbacks about the process he or she is performing.

- *Guide attention through straight directional flow:* Maintain the information flow linear and don't force the user to look around the screen to find information. Every important data has to be shown in the right order within the visual flow in order to not interrupt the user's interaction flow. Every element has to be visually found at the right point in order to refer to the related step in the general process. This optimizes the interaction flow making the system efficient and reducing the feeling of stress that the users can perceive while being unsure about how to act to complete the task.

- *Multi-device consistency:* Since the system asks

the user to relate two different devices, it is very important to maintain a high level of consistency between them. This can be achieved by using the same terminology in the written instructions and by reproducing the same elements and modalities in the visual demonstrations. Even though it is a universal value for interface design, this guideline becomes even more essential in this case to optimize the flow between different devices.

6.3 Future works

Since the system is composed not only by the web-interface, but also by the token, an interesting field of future research would definitely be a similar exploration with the focus on the token. The token can be analyzed considering both aspects related to the physical design and to the graphical interface. Besides developing a working prototype with final physical properties, an efficient way to test usability on both sides has to be specifically developed. This research could lead to a strong contribution towards the design of product-service systems and, in particular for the specific e-banking field. Specifically designed usability test methods and settings could be explored in order to define an efficient way to evaluate, not only the products, but the way users perceive the value of money and risks during transactions.
For what concerns the actual product innovation, the entire system could be explored from its roots and re-designed considering not only security-driven technology but also user's interaction. Different ways such as haptic, visual or sound feedbacks could be implemented in order to let the user more naturally perform the login or transaction signing actions. New secure solutions can be explored in the directions to hide more and more the actual computational process behind human gestures.

References

Busch, T. (1995). *Gender Differences in Self-Efficacy and Attitudes Toward Computers*, Journal of Educational Computing Research.

Cooper, A., Reimann, R., & Cronin, D. (2007). *About Face 3: The Essentials of Interaction Design*, Wiley Publishing, Inc.

Czaja, S., Sharit, J. (1998). *Age differences in attitudes toward computers,* The journal of Gerontology, Gerontological Society of America

Dapp, T. F. (2012). *Online banking and demography,* Banking and Technology Snapshot, Deutsche Bank AG

DeWitt, A., & Kuljis, J. (2006). *Aligning usability and security: a usability study of Polaris*, School of Information Systems, Computing and Mathematics, Brunel University

Dumas, J. S., Redishj,. C. (1999). *A Practical Guide to Usability Testing*, Intellect Books

Galitz, W. O. (2007). *The essential guide to user*

interface design, Wiley Publishing, Inc.

Gemalto (2013). *Fraud Mitigation Methods for E-banking and E-commerce*

Kirtland, J., (2001). *Identification Numbers and Check Digit Schemes*, The mathematical association of America

Löwgren, J., & Stolterman, E. (2004). *Thoughtful Interaction Design: A Design Perspective on Information Technology*, The MIT Press

Meyer, T. (2006). *What we learn from the differences in Europe*. Banking and Technology Snapshot, Deutsche Bank AG

Nielsen, J. (2000). *Security & human factors*, Nielsen Norman Group

Norman, D. A. (2002). *The Design of Everyday Things*. Basic Books

Pinker, S. (1999). *How the Mind Works*, W. W. Norton & Company.

Preece, J., Rogers, Y., & Sharp, H. (2002). *Interaction Design: Beyond Human-Computer Interaction*, Design, John Wiley and Sons, Inc.

O'Reilly, P. (2008). *Use of Internet Banking by the Elderly – Time to Rise to the Challenge*, Financial Services Innovation Centre, UCC

Rubin, J., Chisnell, D. (2008). *Handbook of usability testing: how to Plan, Design, and Conduct Effective Tests*, Wiley Publishing, Inc.

Wagner, D., Tribble, D. (2002). *A Security Analysis of the Combex DarpaBrowser Architecture*, Darpa

Yee, K. P. (2002). *User interaction design for secure systems*, Computer Science Division (EECS), University of California

Yee, K. (2004). *Aligning security and usability*, IEEE Security & Privacy Magazine, The IEEE Computer Society

Appendix 1

FIRST USABILITY TEST ITERATION RESULTS

AGE GROUP: 18-34
AGE RANGE: 20-31
AVERAGE AGE: 25

Kaspar - 31, IXD/graphic designer/software developer, Linux user, computer developer/technology expert, already familiar with tokens

Laptop

- Was quite much surprised/entertained by the challenge page
- Was reading the steps but wasn't getting exactly what the animation was for
- Managed to complete the task with the laptop pretty quickly (approx 3.30 min)

Tablet

- Pressed next without making the challenge
- During the signing he pressed next without checking the device screen but then went back and quickly found the info

User Feedbacks

- If you read a space on the screen, you might look for a way to put a space on the device too
- Too much animation and speed caused ad-blinding to me
- Maybe the animation could be just something you can open in case you need
- The pin should be before on the device

Sara – 27, IXD designer, Mac user, high computer skills/technology expert, not familiar with tokens

Laptop

- Was shocked by the challenge page
- Was following the steps
- Felt kind of stuck for a second when she was supposed to press next before putting the challenge back
- Managed to complete the task with the laptop pretty quickly (approx 3.30 min)

Tablet

- Quick login with almost no screen checking

Was quite surprised and annoyed that she was asked to type more data
- Found the info pretty quickly

More feedbacks

- I felt stressed with the scrolling challenge
- Not so much add-blinding since the animation is the main window of the page
- The animation makes it stressful
- There are two times the same info (list+animation) so it's not clear where you're supposed to look
- You need to make it less moving

Kim – 24, shoe designer, Windows user, medium computer skills and familiarity with tablets and smartphones, already familiar with tokens

Laptop

- Carefully followed the instruction list
- No particular issues noted
- The process took approx. 5 min

Tablet

- Carefully followed the instruction list again
- Some difficulties during the international signing answering the additional steps

More feedbacks

- It felt easy, sophisticated and trustful
- It's easy to follow the instructions step by step thanks also to the dynamic list
- I followed the left part rather than the animation
- I didn't find it easier than my bank but I felt it was safer and I want to feel the security
- It was difficult, during the international payment, to follow the part on the device cause having two devices you don't know where you're supposed to look at

Rebecca – 22, economy student, Windows user, average computer skills and familiarity with tablets and smartphones, already familiar with tokens

Laptop

- Bending to read the small instruction list
- Relied only on the instruction list. No attention to the device screen
- On the signing still mostly looking at the instructions
- Pretty quick - approx 3 min

Tablet

- Carefully followed the instruction list again
- Got completely lost during the international payment cause she didn't get what account number was referring to (on the resume it says IBAN instead)

More feedbacks

- I didn't get the account number thing
- It was pretty easy
- Followed the left part rather than the animation
- I felt a little bit stressed about the "blinking"

Jesper – 20, carpenter, Windows user, average computer skills and average use of tablets and smartphones, already familiar with tokens

Laptop

- Waited for the animation to complete one loop before starting and then tried to follow it
- On the signing, was still mostly looking at the instructions
- Pretty quick - approx 3.10 min

Tablet

- Still looking at the instruction list again
- After scrolling the page to check if there was some more information, he quite easily followed the steps on the screen and completed the task

More feedbacks

- It was easy thanks to the instructions
- I followed the left part rather than the animation
- The animation switched all the time so I didn't bother to look at it
- It wasn't easier than my bank cause I'm used to that one
- It wasn't stressful and the process wasn't long
- The steps in the dynamic bullet list are good cause you keep track of everything you do

AGE GROUP: 35-54
AGE RANGE: 35-46
AVERAGE AGE: 41

Joakim – 46, software developer, Windows user, professional computer skills and average use of tablets and smartphones, already familiar with tokens

Laptop

- Looked at the instructions at first and made sure to get the process
- During the signing he knew already what to do and just waited for the animation to show to press the "sign" button (to be sure) and continue
- Didn't look at the animation anymore

Tablet

- Logged in without any look at the instructions
- When the device asked "international?" he scrolled to the instructions to see if there was some guide about it. Then he tried pressing ok and started the process

More feedbacks

- It was easy
- I looked at the instructions only the first time and the I was expected to have it always the same way
- I looked only at the left part since I could follow it with my own speed
- Too much scrolling text in the device
- Animation/scrolling is nice for the few first times but then they become annoying
- Keep it simpler and maybe have two different configurations: one for beginners and the other one for who wants to be quicker. Like a pop-up that you can decide to not be shown again by un-checking it

Matt – 41, warehouse worker, Windows user, average computer skills and average use of tablets and smart-phones, already familiar with tokens

Laptop

- Quickly read the instructions list while performing the task
- Perfect signing

Tablet

- Logged in without any look at the instructions
- When the device asked "international?" he scrolled to the instructions to see if there was some guide about it. Then he tried pressing ok and started the process

More feedbacks

- It was easy cause it was almost the same as the one I'm used to
- I looked at the instructions only the first time and the I was expected to have it always the same way
- When it asked for international I thought something was wrong but then I soon realized what I was supposed to do
- Just looked at the steps on the bullet list
- It was annoying to go to another page to put the response in

Pille – 35, researcher, Mac OSX user, average/good computer skills and average use of tablets and smartphones, already familiar with tokens

Laptop

- Went through the instructions to log in
- Followed the steps during signing too

Tablet

- Waited for the instructions to come up before starting
- Completed the international payment quite easy thanks also to the fact that she was looking at the instructions

More feedbacks

- The challenge section made me nervous cause I thought it would disappear soon (because of the moving)
- I liked the arrow that showed me to press next
- When it asked for international I thought something was wrong and then I tried to go back
- Just looked at the steps
- When I was asked to go to another page to type the response I felt a little bit nervous cause the challenge usually expires after some seconds

AGE GROUP: 55+
AGE RANGE: 58
AVERAGE AGE: 58

Klauss Raats – 58, IT , Linux user, professional computer skills and low use of tablets and smartphones, already familiar with tokens

Laptop

- Had some problems with the term challenge and also to understand how to start the process
- Didn't look at the steps during signing

Tablet

- Even before starting the signing he zoomed the info box and completed the task without instructions

More feedbacks

- Just read the instructions once
- The interface was quite logic
- I was looking for a way to put a space after the first 4 codes on the token

Appendix 2

SECOND USABILITY TEST ITERATION RESULTS

AGE GROUP: 18-34
AGE RANGE: 23-29
AVERAGE AGE: 25

Emma - 25, Human Ecology student, Windows user, medium/high computer skills and very used to tablets and smartphones, already familiar with tokens

Laptop

- Very fast and flawless performance

Tablet

- Flawless performance as for the first task

More feedbacks

- I read the steps just the first time
- I didn't notice about the demo button
- I did it as fast as I could without making sure I was doing it right because I always trust the system and if I do something wrong I expect it to tell me or stop the process

Angelica – 23, unemployed, Windows user, high computer skills and knowledge of tablets and smartphones, already familiar with tokens

Laptop

- Fast and flawless performance

Tablet

- Slowed down a bit during the international step but no particular problem noticed

More feedbacks

- It was really easy
- Really similar to my bank but with few less steps
- Every info you need is easy to find
- I didn't notice the demo button

- I didn't notice the bullet list highlighting feature but, afterwards, I think it's a good idea

Cecilia – 25, elder care, Windows user, medium computer skills and familiarity with tablets and smartphones, not familiar with tokens

Laptop

- Fast and flawless performance

Tablet

- Fast and flawless performance

More feedbacks

- It was easy
- I've followed the steps
- I didn't notice the demo button
- I didn't notice the bullet list highlighting feature

Tommy – 25, technology student, Mac user, high computer skills and familiarity with tablets and smartphones, already familiar with tokens

Laptop

- Fast and flawless performance

Tablet

- Fast and flawless performance

More feedbacks

- It was easy
- I've read the steps just the first time
- I didn't notice the demo button
- I didn't notice the bullet list highlighting feature

Sabina – 29, physiotherapist, Windows user, average computer skills and average use of tablets and smartphones, already familiar with tokens

Laptop

- Quite careful approach but fast performance

Tablet

- Quite careful approach but fast performance

More feedbacks

- It was easy
- I followed the steps
- If you're used to tokens it's always quite easy since the processes are all working similarly
- I noticed the demo button but I didn't press it
- I didn't notice the bullet list highlighting feature

AGE GROUP: 35-54
AGE RANGE: 35-53
AVERAGE AGE: 43

Lisa – 35, internal communications, Windows user, medium computer skills and intensive use of tablets and smartphones, already familiar with tokens

Laptop

- Fast and flawless performance

Tablet

- Fast and flawless performance

More feedbacks

- It was easy
- It was clear from the beginning
- I didn't feel any stress or pressure
- I felt a bit insecure during the second task because of the Android based tablet which I'm not used to.
- I didn't notice the demo button
- I didn't notice the bullet list highlighting feature

Mats – 53, engineer (Gemalto), Mac user, high computer skills and high familiarity with tablets and smartphones, already familiar with tokens

Laptop

- Fast and flawless performance

Tablet

- Fast and flawless performance

More feedbacks

- It was easy also because I already knew the product
- I'd prefer to know what kind of process I'm about to perform (challenge/response) in advance
- I might have preferred to see the animation from the start instead of the instructions list
- I didn't notice the demo button
- I didn't notice the bullet list highlighting feature

Gunilla – 45, physiotherapist, Windows user, average computer skills and average use of tablets and smartphones, not familiar with tokens

Laptop

- Quite careful approach but no particular problem to be reported

Tablet

- Quite careful approach but no particular problem to be reported

More feedbacks

- It was easy
- I followed the steps
- I wasn't used to press an OK button to confirm every step on the token so I was waiting for it to react to my inputs
- I didn't noticed that in the instructions it was explained that I was asked to press ok after each step because I didn't read them carefully
- I didn't notice the demo button
- I didn't notice the bullet list highlighting feature

Magnus – 40, solution architect (Gemalto), Windows user, professional computer skills and intensive use of tablets and smartphones, already familiar with tokens

Laptop

- Fast and flawless performance

Tablet

- Fast and flawless performance

More feedbacks

- I had no problems using the laptop but the automatic triggering of the keyboard and the dimension of the tablet really bothered me
- I'd like to see a payment resume while signing in every kind of payment
- I'd prefer the process in one screen but it depends on the banks
- The information is good but after the first couple of times I would prefer to not have it

AGE GROUP: 55+
AGE RANGE: 55-56
AVERAGE AGE: 55-56

Irene – 56, - , Windows user, medium computer skills and medium use of tablets and smartphones, already familiar with tokens

Laptop

- Tried to type the PIN code on the laptop's keyboard at first but quickly noticed the mistake
- Carefully followed the instructions during every step
- No particular problem during the process

Tablet

- Still followed the instructions
- Quite flawless process

More feedbacks

- II had problems with the English written English and, because of it, I didn't feel sure and safe
- I felt unsure using the tablet because of the touch keyboard popping up but I wouldn't make a payment on a tablet or smartphone
- Why do you use the word "challenge"?
- 6 instructions point on the list felt like quite a lot to read
- I wasn't used to scrolling instructions on the token
- I didn't notice the demo button
- The process is quite logic and, even if I didn't understand the language well, it felt like almost impossible to do wrong

Christina – 55, social worker , Windows user, average computer skills and medium use of tablets and smartphones, already familiar with tokens

Laptop

- Tried to type the challenge code into the response box
- Couldn't understand how to start the process until opened the demo mode but, probably thinking to have understood it, closed it quite quickly without following the whole instruction

- While using the token, she couldn't understand what "Challenge" was asking her to do and pressed ok instead of typing it in.
- After quite many attempts she managed to complete the process
- Signed quite easily

Tablet

- She logged in without particular problems
- Once at the international payment step she looked like having forgotten the whole process so she started to try to press sign without performing the challenge/response
- She tried to ask me what she was supposed to do and, after reminding her that she was supposed to perform the same action as in the past examples, she said she thought to have done it
- Pressed login instead of sign button on the token
- After I let her notice that she was supposed to press sign instead, she slowly managed to complete the process correctly

More feedbacks

- I couldn't understand the instructions because it was in English
- The demo mode was very helpful and I found it quite easily
- The process it's quite easy once you understand it
- Using laptop or tablet didn't make any difference to me
- During the international payment I didn't read the instructions because it takes time and effort to me to read in English and I thought the process was the same
- Even if I got confused during the international payment, thinking about it afterwards, it felt as the best step to make me feel secure