

Intelligent Interaction Design: HCI PROJECT

201500118 (BIT/TI)

201500148 (CREATE)

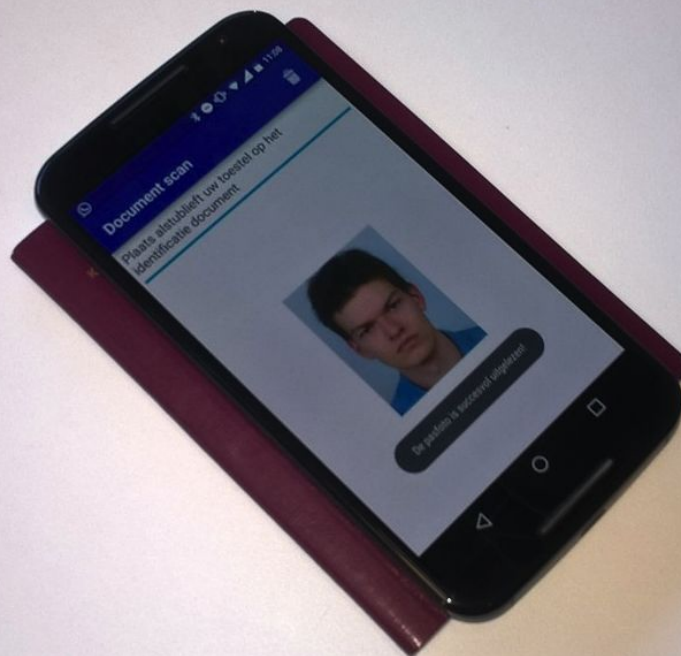
Deliverable 5.2

Final version of project report

Hand in date

19 January 2016

TOBI: The new Online Banking Identification



Passport reading + Facial recognition

Group 19

Selwyn Nypels	s1580329
Melcher Stikkelorum	s1560670
Max Mensing	s1479520
Kilian Ros	s1559168
Jan Jaap de Groot	s1758721

This page intentionally left blank

Abstract

In the context analysis it was found that many people and especially elderly struggle to use online banking. The main bottleneck is the way banks require people to authenticate to their banking account. We set out to design and evaluate a new way of authentication, essentially lowering the barrier for people to use online banking. We created low-fi prototypes for multiple ideas. After the first round of evaluations our prototype using face recognition came out as a winner.

At the point of creating our Hi-Fi prototype we reached out to Rabobank for detailed information on what a typical bank requires of a secure authentication mechanism. Evaluating our high-fi prototype, it became clear that our current prototype is not significantly better than traditional authentication methods. During this last evaluation we evaluated the aspects, feel of security, ease of use and efficiency.

Table of contents

1. Introduction	3
2. Context analysis and concept	7
2.1. Context analysis	7
2.1.1. Goals	7
2.1.2. Research questions	7
2.1.3. Approach	7
2.1.4. Details per method	8
2.1.5. Description of target user group and domain	9
2.1.6. Resulting product concept	11
3. Design and Evaluation of Lo-Fi Prototypes and Revised Product Concept	14
3.1. Lo-Fi prototypes	14
3.1.1. Concept	14
3.1.2. Goal	14
3.1.3. Evaluation questions	14
3.1.4. User tasks	14
3.1.5. Recruitment	14
3.1.6. Evaluation of the results	14
3.1.7. Briefing & debriefing of the experiment	15
3.1.8. Authentication in general	15
3.1.9. Detailed plan	16
3.1.10. Survey questions	19
3.1.11. Results	21
3.1.12. Conclusion	22
3.1.13. Revised product concept and requirements	23
4. Design of final Hi-Fi prototype	24
4.1. Architecture	25
4.1.1. Class diagram	26
4.1.2. Code flow	26
4.2. Interaction flow	27
4.3. Implementation	28
4.3.1. Facial recognition	28
4.3.2. KeyLemon communication	28
4.3.3. Taking pictures	28
4.3.4. Using NFC	29
4.4. Product	29
5. Expert evaluation	32
5.1. Conclusion	33
6. User evaluation	34
6.1. Goal	34
6.2. Evaluation question	34
6.3. Hypotheses	34
6.4. User tasks	34
6.5. Recruitment	34
6.6. Evaluation of the results	35

<u>6.7. Detailed plan</u>	<u>35</u>
<u>6.7.1. Facial recognition with NFC ID card and NFC debit card</u>	<u>36</u>
<u>6.8. Survey questions</u>	<u>37</u>
<u>6.9. Prototype analysis</u>	<u>44</u>
<u>6.10. Conclusion</u>	<u>45</u>
<u>7. Discussion</u>	<u>46</u>
<u>8. References</u>	<u>47</u>
<u>9. Appendices</u>	<u>48</u>

1. Introduction

Technology is making its way to objects all around us. There is a shift from physical media to digital media. During this shift, some people are left behind. Staying up to date with technology requires a significant time and learning investment. In order to stay connected with others and up to date with the latest news, the use of an internet connected device is required. For some, using such a device is not easy. Elderly in particular often struggle to keep up with the rapid technology advancements. Elderly are also the target group of this project. The aim of the project is to help this target group in use and interaction of electronic devices.

After context analysis and interviews with the target group, a specific problem was identified. Online banking is considered difficult and sometimes even scary by the target group, resulting in abandonment of the feature. However, banks are moving to an online only policy and soon managing a bank account can only be done online. During the research it was identified that authentication methods play a large role in the aversion of the target group.

Therefore the focus of this project is to develop an alternative authentication method for use with online banking. To gain further information about the subject, a conversation with the Rabobank was held. Taking this information into account, the decision to use facial recognition in combination with NFC - to be able to scan identification documents - was made.

This document describes the design and evaluation of the Hi-Fi prototype. Furthermore, this document describes scenarios, interactions; explanation of evaluation, results, and consequences.

2. Context analysis and concept

2.1. Context analysis

2.1.1. Goals

The goal of the system is to provide an experience for our target group that allows for *easier* access to certain features of a computer, with *easier* meaning that the target group is able to use features *faster* and more *extensively*. The user should prefer this system over the native windows environment.

The list of features includes things such as:

- email
- calendar
- web browsing
- file management
- online banking

2.1.2. Research questions

- Do elderly want to use computers in the first place ?
 - if not, what is keeping them from it?
 - if so, what do they expect to be able to do?
- What difficulties do elderly encounter when using a computer?
- What difficulties can people who work with elderly identify?
- What functions do elderly want to access regularly on their computer?
- What functions do elderly already access regularly on their computer?
- What kind of input method(s) do elderly prefer?

2.1.3. Approach

Interviews

It was chosen to use interviews as a method of analysis because

- Different stakeholders require different approaches
- Personal approach possible
- Possibility to ask follow up questions
- Verbal communication

A few different groups of people related to our problem will be interviewed. These groups consists of:

- Elderly not experienced with computers
- Elderly experienced with computers
- People working with elderly, teaching them about computers

Related work and literature

For related work the internet is searched for papers regarding user interfaces and elderly.

2.1.4. Details per method

This section describes each of the methods named above in more detail. For Interview questions and answers please see appendix A.

Related work and literature

In order to get an idea of the previous work done in this field, internet searches were performed. Specifically, Google Scholar was used to find papers that describe research in the area of user interfaces and their ease of use among elderly. Combinations of the following terms were entered in Scholar:

'user', 'interface', 'elderly', 'computer's', 'operating system'.

Method for analyzing

To evaluate the papers, both the introduction and the conclusions of the papers were studied. Both the reasons and the results of the research helped us understand the current situation with user interfaces and elderly.

The following papers were used:

1. Evaluating Touchscreen Interfaces of Tablet Computers for Elderly People [1]
2. Too old for technology? How the elderly of Lisbon use and perceive ICT [2]

Results & conclusions

Both papers focus on elderly and the use of electronic devices. In 'Evaluating Touchscreen Interfaces of Tablet Computers for Elderly People' [1] the authors describe the reason for the paper in the introduction. They describe research performed from which they conclude that the user interface of traditional computers is a barrier for elderly.

In 'Too old for technology? How the elderly of Lisbon use and perceive ICT' [2] the authors conclude that limited education is the cause of the barrier between elderly and ICT systems. From this it is possible to derive that the interfaces are too difficult to understand, because of the needed education. Simplifying the interface could lower the barrier.

Interview

For each user group a different interview was designed in line with the description of the specific group. For the elderly people the decision was made to start with some really basic questions about their affiliation with technology. To get comfortable they are also asked about their day and maybe about possible grandchildren. Some simple start up questions are used in the hope to get comfortable with our interviewee and start asking some more specific questions about their computer use.

The assumption is made that the people participating are motivated to speak to us and have enough time to be able to answer all of our questions and hope to find answers to all our research questions during these interviews.

For the computer lessons teachers a slightly more direct approach is used to get some deeper insights. These people are technically well-grounded so they can be asked harder questions.

Method for analyzing

For each interview compare it to the others to find similarities amongst the answers given. Making a list of problems described.

Evaluate the received answers from the interviews and eventually order them in categories.

Approach to get respondents

To get respondents in for the first usergroup, elderly in our direct vicinity will be contacted (grandparents and others). To interview people following computer lessons or teaching them a visit will be paid to an elderly home or community centre where people can follow computer lessons. Once there, any other people present belonging to our user group and willing to co-operate might also be approached for an interview.

Results & conclusions

Based on interviews with a number of people from our target group the project plan was changed. A problem was identified regarding online banking, many elderly struggle with it. Therefore the focus was shifted from helping elderly using a computer overall to specifically helping elderly with online banking, emphasising the authentication step when logging in and transferring money. There is no longer a focus on creating an interface that replaces various tasks.

2.1.5. Description of target user group and domain

It can be said that everyone not experienced with the use of computers, including elderly and people who avoided technology, is now confronted with online banking.

This group is broad due to the fact that every adult in the Netherlands who cannot operate a computer is affected by it, but the conducted research pointed out that elderly people as a whole have issues/troubles using computers which obviously has influence on their banking. Since data about common computer problems of elderly people had already been collected, the focus will now be on making the system (hardware + software) user friendly and intuitive for them.

Stakeholders

- Elderly not experienced with computers/not attending a computer course
- Elderly experienced with computers/attending to a computer course
- People working with elderly, teaching them about computers
- People struggling with online banking.
- Banks

Below you will find users of our target user group described in personas.



Nelly Nordin

Age: 74

Birthday: 13/03/1941

Status: Computer novice

Nelly Nordin used to be an elementary school teacher . She has now been retired for about 7 years. Computers never really interested her and she never really felt the need to use one.

Nelly's husband usually took care of computer related tasks like internet banking and sending emails. Unfortunately, Nelly's husband, Brian, passed away 2 years ago which consequently urged Nelly to do everything independently. Nelly's three children, who are in their forties, often help her using the computer to take care of the things Brian used to arrange. Since she started using the computer to settle important tasks she found out a computer can also be used for fun things. Nelly now regularly plays some simple card games like solitaire which she really enjoys. She now is eager to learn more about the broad range of possibilities she can use her computer for. Especially online banking is something she wants to learn, since soon it is no longer possible to do banking in any other way. The biggest obstacle for her is the complicated authentication system. She is scared that she will do something wrong and produce unwanted results.



Bob Spijkerman

Age: 52

Birthday : 21/11/1963

Status: Full time construction worker

Bob is a construction worker with more than 35 years of experience under his belt. Bob is used to getting paid in cash, and paying for everything he needs in cash.

However, he has realized that storing his cash on the bank is a safer option. He started his first bank account around 15 years ago. He fulfilled all of his banking needs at one of the branches. Unfortunately the banking branch in his city has closed down. Bob does now need to travel for 30 minutes to get to the nearest banking branch. Bob doesn't like this and wants to learn how to get his banking done online. Computers confuse him and he prefers getting everything done on paper.

2.1.6. Resulting product concept

For the interviews, the goal was to find specific computer problems encountered by elderly people. The results from the interviews led to the conclusion that online banking is a problem amongst elderly people. The hassle of logging in and verifying a transaction are the main problems with online banking.

According to the results of the interviews, banks make authentication too complicated and hard to understand for people with little to no knowledge about technology. After the interviews the conclusion was derived that the project would be narrowed down to the authentication process of an online system, online banking in particular. But this problem does not only occur with elderly people, so our user group can now be globally identified as “people who struggle with online banking”. Of course elderly people are still a large part of this group. After adjusting the project plan, new stakeholders can be identified. Most of which are the banks. Additional research is necessary in this particular field to get a clear view of our new designed concept.

Revised goal

The goal of the system is to provide an experience for our target group that allows for *easier* access to online banking tasks. Here *easier* means that the target group is able to authenticate to their banking account within a moment's notice. The user should prefer this method of authentication over the original method provided by the bank.

Revised research questions

- What are existing methods of online identification?
 - Which authentication systems are prone to fraud?
 - What are the problems with existing methods of identification?
 - What are the advantages of existing methods of identification?
- What elements of existing methods are usable in a new system?
- What do people require in order to improve the identification experience?

Problem description

Who has a problem

Elderly people were interviewed to find a problem which they have in the field of using a computer. A distinction between three different groups was made: people who don't use a computer, a number of people who follow computer lessons, which means they use a computer, and a number of people who teach elderly how to use a computer. During the interview it was identified that online banking is a problem.

What is the problem

The problem with online banking is that verification of the user is hard and that is scares users of actually using the online banking system. The human-computer interaction varies a lot between banks and they all use their own method for user authentication. For people not familiar with the latest technologies it can be very difficult to authenticate themselves in the online banking system.

When is it a problem

The problem occurs whenever a user wants to log in to their online banking account. After logging in, the problem does also occur when the user wants to transfer money to another account. To be able to transfer money, the user has to follow some verification steps. In general this transaction verification is the same as the login verification.

Where is it a problem

Online authentication is a problem in online banking. Besides online banking there are also companies, dealing with confidential documents and materials, that struggle with the problem of securely authenticating their users. Also government facilities have to deal with secure user authentication, for example the dutch DigID system.

Why is it a problem

Verification for online banking is a problem because interaction with the bank happens more and more often via the internet. Banks are decreasing their physical presence and capitalize on web presence. Furthermore, online shopping is more popular than ever and payment is only possible via online methods. People having problems with authentication methods used nowadays therefore have trouble catching up with modern trends.

Non-technical description

Elderly can no longer escape from technology. Whether they like it or not, everything is getting digitalized and many of the offline alternatives are getting phased out. Banks are closing branches and phasing out acceptgiro cards. People are forced to learn how to take care of their banking online. Many are struggling to catch up with the amount of change. It came to our attention that authentication is one of the main choke points to get people to use online banking. Our system will simplify the authentication process so that online banking becomes more accessible for people.

First of all the log-in procedure will be improved. At the ING-bank you use a randomly generated username (hard to remember) and the password must fit various requirements (hard to remember). At the Rabobank you use a Random Reader instead of a password, but you still need to fill in this secret number. Our prototype will aim to find a way to log-in faster and easier.

Global requirements

The requirements below have been ordered MoSCoW: Must, Should, Could, Won't.

Technical

- The system must be secure
- The system should provide clear and easy steps to user to accomplish their task
- The system should at no times take longer than 10 seconds to respond
- The system should clearly display its status
- The system should be available at all times
- The system won't replace the complete online banking experience

User

- The system must give the user appropriate feedback at all times
- The system must help prevent the user from making mistakes
- The system should be usable for novice computer users
- The system should support the users in doing their tasks
- The system should be easy to learn

These requirements are based on the aspects of usability; effectiveness, efficiency, utility, learnability, memorability and security. Also the design principles feedback, consistency, visibility, constraints and affordance were taken into account. Furthermore, results of the interviews were a valuable source of information to formulate requirements from.

3. Design and Evaluation of Lo-Fi Prototypes and Revised Product Concept

3.1. Lo-Fi prototypes

3.1.1. Concept

Aim is to create an appliance for secure authentication that is tailored to people above the age of 50, who are insecure with online banking.

3.1.2. Goal

The goal of the system is to provide an experience for our target group that allows for *easier* access to online banking tasks, with *easier* meaning that the target group is able to authenticate to their banking account within a moment's notice. The users should prefer this method of authentication over the original method provided by the bank.

3.1.3. Evaluation questions

- How much faster/slower is the prototype in comparison to the traditional method of authentication?
- How intuitive is the prototype compared to the traditional method of authentication?
- How clear is the look of the prototype; do the users instantly know what they need to do, to successfully use it?
- What, to the users, important information is not present in the prototype?

3.1.4. User tasks

- Logging in: The users are asked to log in to the a fake online bank using one of our prototype authentication methods.

3.1.5. Recruitment

For the evaluation of the prototypes, users will be recruited. To vastly increase the number of possible tests, the range of ages has been extended. The tests will be performed using with people above the age of 50. Each of the members of the group asks their relatives that fit our target-group profile to evaluate the prototype. These participants are readily approachable.

3.1.6. Evaluation of the results

To evaluate the results from the tests, the results from the survey for each prototype are combined with the literature about the security method.

After a test is performed, the participants are asked to fill out a survey with questions regarding speed, security and ease of use. The answers are in comparison to what method they use now. In order to do this comparison, the participants are asked at which bank they do their banking. For each aspect a score is noted. The weight of each score is determined with the help of research data of each security method used in the prototypes.

After evaluating both the research and the results from the survey, one prototype is chosen to continue working on.

3.1.7. Briefing & debriefing of the experiment

In order to have as little influence as possible on the participant, briefing will be kept short. Prior to evaluating a particular prototype a short explanation will be given. Initially there will be no guidelines for the participants during the experiment, which allows us to observe their actions and possibly spot issues with the prototype.

Answering questions during the evaluation should be avoided, but if participants are unable to complete the evaluation they should be given help. Participants will be stimulated to say out loud what they are currently doing while using the prototype. This is done in order to follow the train of thought of participants and take notes. After the evaluation, the participants will be asked to fill out a survey.

3.1.8. Authentication in general

Some additional research was done on the topic of authentication in general. With this information it is easier to come up with feasible ideas for Lo-Fi prototypes.

Generally, the way to authenticate customers is to have them present some sort of factor to prove their identity. Authentication factors include one or more of the following:

1. Something a person knows - commonly a password or PIN. If the user types in the correct password or PIN, access is granted.
2. Something a person has - most commonly a physical device referred to as a token. Tokens include self-contained devices that must be physically connected to a computer or devices that have a small screen where a one-time password (OTP) is displayed, which the user must enter to be authenticated.
3. Something a person is - most commonly a physical characteristic, such as a fingerprint, voice pattern, hand geometry, or the pattern of veins in the user's eye. This type of authentication is referred to as "biometrics" and often requires the installation of specific hardware on the system to be accessed.

Shared secrets

This technique relies on secret information which is only known by the consumer (*something a person knows*):

1. Password;
2. PIN;

3. Questions or queries that require specific customer knowledge.

Tokens

Tokens are physical devices (*something the person has*) and may be part of a multifactor authentication scheme. Three types of tokens:

1. USB Token Device;
2. Smart Card;
3. Password-Generating Token.

Biometrics

Biometric technologies identify or authenticate the identity of a living person on the basis of a physiological or physical characteristic (*something a person is*).

1. Fingerprint recognition;
2. Face recognition;
3. Voice recognition;
4. Keystroke and handwriting recognition;
5. Finger and hand geometry;
6. Retinal scan;
7. Iris scan.

From these authentication methods a selection has been made which will be used for the Lo-Fi prototypes. Based on accessibility, practicability and hardware restrictions the choice was made to use the following biometric methods: face recognition, voice recognition and fingerprint recognition. A non biometrical method that will be used for a prototype is a gesture pattern.

3.1.9. Detailed plan

Each prototype evaluation is followed by a survey corresponding to the relevant prototype. Note that, unless stated otherwise in the prototype description below, a Lo-Fi prototype in combination with a debit card and NFC is used.

Before starting the actual prototype test, the participants are asked to scan their debit card with a fake NFC reader. It is assumed that the use of a debit card has a certain effect on the user; 'the debit card holder is the boss'. Furthermore, this way of two-step-authentication is more secure than having only a single line of defence.

For each evaluation the participant should not know what programs are used.

Facial recognition

Setup

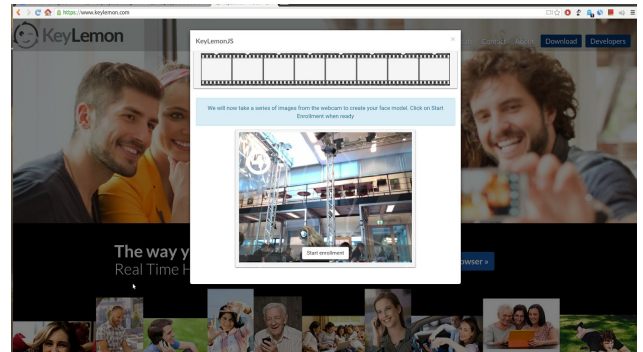
The tester browses to www.keylemon.com and completes the setup up to the moment at which authentication takes place.

Execution

The participants opens the PowerPoint and follows the on-screen instructions. The participants are asked to identify themselves using face recognition as previously set-up.

Explanation

Facial recognition is based on a reference image of the user that is stored in a database. When authenticating this image is compared to a new image that is taken from the authentication procedure. Intelligent algorithms can identify different positions and shapes of eyebrows, cheeks, eyes, jaws and noses which make the system very secure. Together with fingerprints and voice recognition it belongs to the three biometric authentication methods which can be considered as very safe in terms of forgery.



AirPattern

Setup

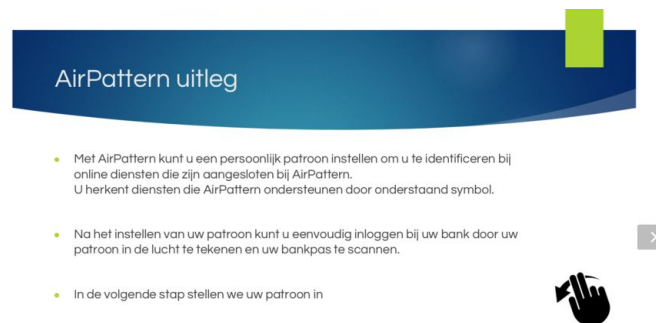
A PowerPoint with gesture instructions is set up. The tester (Wizard of Oz) uses the mouse out of sight from the participant to advance the PowerPoint through the steps.

Execution

The participants are asked to sit in front of a laptop and follow the instructions given in the PowerPoint. The participant is asked to record a pattern, and then repeat it to log in.

Explanation

Measuring air patterns requires a camera recording the motions of the user. This can be done using a Microsoft Kinect camera since it is easy to use but it is also able to track multiple different motions at the same time. Research in biometric authentication, using hand gestures, turned out to be a very promising and accurate method for verifying identity[3]. However measuring air patterns requires multiple tracking algorithms that translate motion into characters.



Voice Control verification

Setup

The tester uses a combination of Voice Attack and PowerPoint to conduct the test. Voice Attack is set to press spacebar when the participant says their specific pass phrase. The PowerPoint resembling the interface is started. The tester hands the participant a piece of paper with their personal pass phrase.



Execution

The participant is asked to follow the on-screen instructions and speak the pass phrase out loud.

Explanation

Same as fingerprints, voice controlled verification is based on the human biometrics which are individual for everyone. Usually there are two steps involved in voice controlled verification:

1. The person to identify provides personal verification data
2. The voice is compared to an older voice sample of that person

In order to protect voice authentication from fraud, the system can also ask the user to say a random word which could not be 'recorded' before which identifies the user as a person instead a computer or a recording.

Fingerprint

Setup

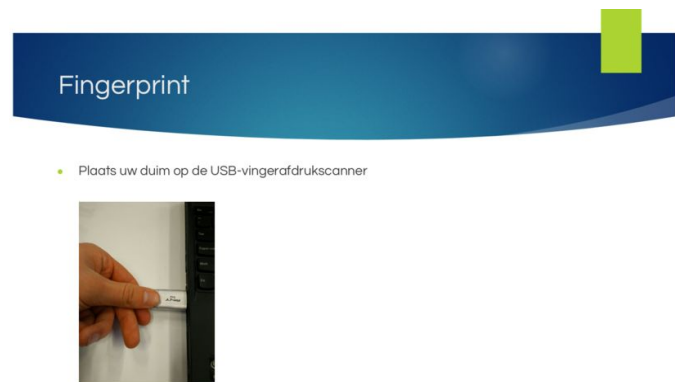
The tester needs a random USB-stick which will act as a fingerprint scanner. Next, the tester connects a phone with an NFC reader application opened to the laptop/computer using a usb cable.

Execution

Let the participant open the PowerPoint and follow the instructions.

Explanation

Fingerprint sensors are commonly used in security because they can be produced rather cheaply still providing meaningful/reliable results. Measuring the human biometrics all kinds of different sensors can be used for all kinds of different operations. Since the human fingerprint is unique for everyone it is difficult duplicate / forge the it which makes it a very safe verification method. When increasing the security level it is even possible to sense whether the finger is alive or dead (fraud). Additionally, fingerprint sensors are very compact and can be implemented in very small systems.



3.1.10. Survey questions

- **To what degree do you feel the method was safe? (scale 1-10)**
With this question participants are asked about their feeling of security of the prototype. from our interview evaluation the conclusion that people are scared of using online banking can be derived, because they think severe consequences could occur if they do something wrong. Our final prototype should make people feel safe to use online banking.
- **To what degree do you feel this method is faster than the method you normally use to sign in with your bank? (scale 1-10)**
This question should give us an impression about how fluently the participants can use the prototype. It is assumed that a fast method of authentication will lead to smoother use and a more satisfying experience when using online banking. This question is about how much faster it feels for the participants, not how much faster it really is.

- **To what degree do you think this method is easier to use than the method you normally use? (scale 1-10)**

If the prototype method is easier to use, it will take away confusion. This would improve authentication experience for the participants. The participants are asked to compare the method of their real bank with the method of our prototype. In the end the easiest method might probably be the best because our participants find authentication for online banking really difficult.

- **Was all information you needed to login available? (yes/no)**

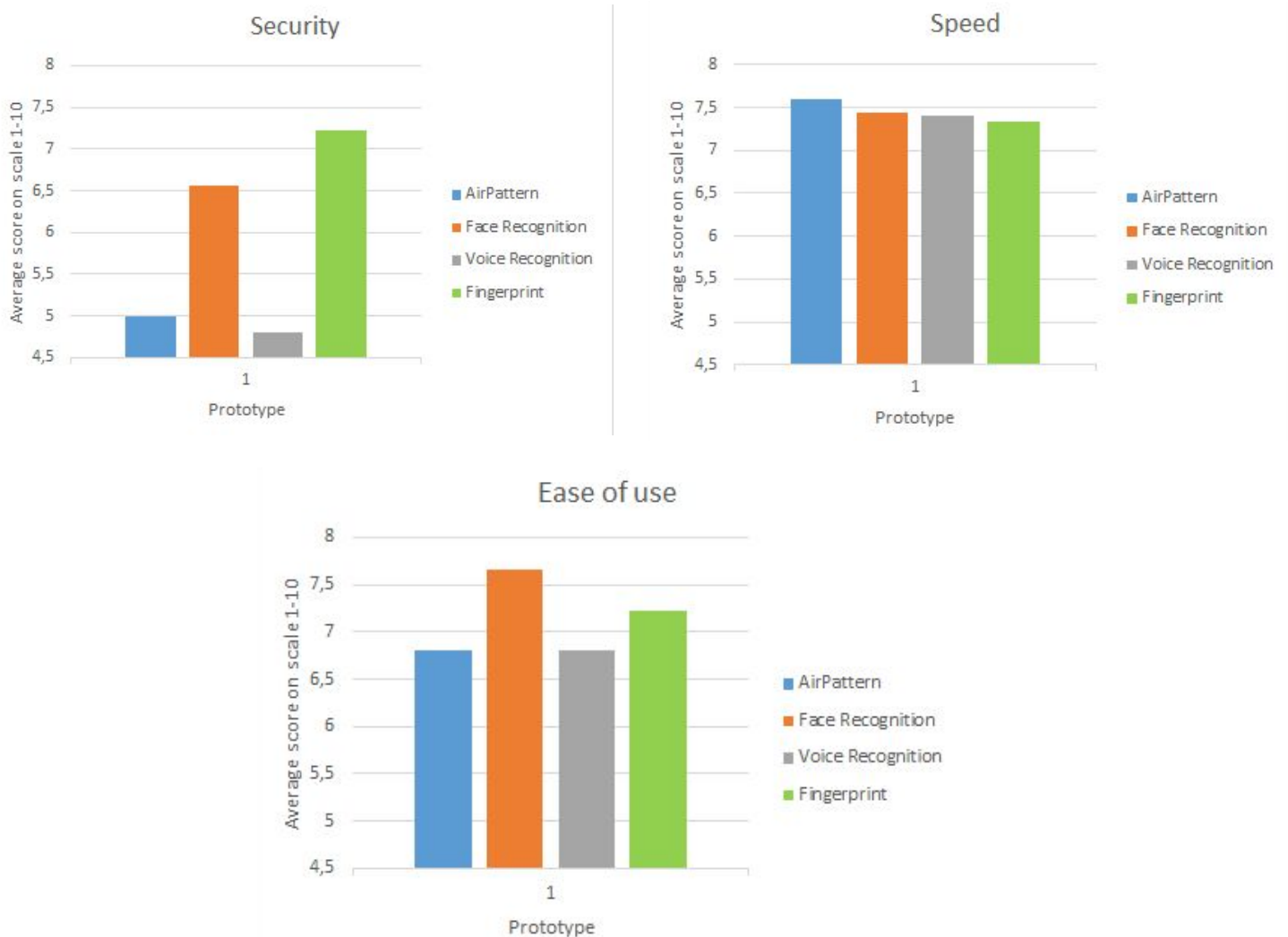
This question is asked to find out if our prototype contains all the necessary information for participants to successfully perform a login. If our prototype lacks information which the participant thinks is absolutely necessary to perform a login, it can't be fairly compared to the other prototypes. This is something to keep in mind when evaluating the answers.

- **Open question: what do you think was missing in this method?**

This question is basically a follow-up question of the last question. If the participants miss information in our prototype, they can provide this to us. Participants can also leave us suggestion in this question field. If this field is not used very often it could mean that our prototypes are well-designed. However, all the information provided in this field should be taken very serious because it affects the whole evaluation of the prototype testing.

3.1.11. Results

Below are the results of the surveys filled out after our evaluation sessions with our target group.



Based on the above information one may conclude that the perception of the speed for each of the prototypes is similar. Looking at the the feeling of being secure it immediately becomes clear that our participants prefer the face recognition and fingerprint methods. It seems that, because the method of fingerprint is more well known, our participants feel more secure using this method. Notice the ease of use score for both face recognition and fingerprint are also higher than our other prototypes. These methods are both biometric and do not require the user to remember a certain password. Not having to remember any password seems to be something our participants appreciate.

Reactions Facial Recognition

Multiple participants wondered how secure this method is when a doppelganger uses the system. Participants wearing glasses had some difficulty using the face recognition software. After one try, the system would not be able to detect 'a sign of life' since blinking was not detected.

Reactions AirPattern

Many of our participants were concerned about how secret their chosen pattern would be since it can be easily seen while logging in. Furthermore, the question arises if the direction in which the pattern is drawn makes a difference for authentication. Moreover, it can be quite hard to remember a secure pattern for use with this system which is something our target group does not want to waste brainpower on.

Reactions Voice Control verification

A question often heard was what happens if one loses their voice or when you catch a cold and sound hoarse. Moreover, it seems counter intuitive and insecure to speak your passphrase out loud.

Reactions Fingerprint

Some of the participants remarked that they found it obstructive that they had to plugin two different devices to complete the authentication. They told us that it makes authentication harder than it is with their bank's current method. The fact that the users need to carry around an extra USB device negatively affects the portability of this authentication method. Our participants want to be able to login at any place, at any time.

3.1.12. Conclusion

Almost every participants has concerns about the security of the authentication methods, they have a strong opinion about how they feel about security and let us know how they thought about it. This shows, once again, that the feeling of being secure should play a major role in our design.

As one can see in the graphs above, fingerprint and facial recognition have the best results in providing the feeling of a secure authentication. From this data it can be concluded that AirPattern and voice control are no feasible solutions to our problem because they just don't provide a secure feeling.

This leaves us with the other two prototypes, fingerprint and facial recognition. In both ease of use and speed they perform almost equal, this means our decision needs to be based on the remarks given by the participants. As described above, the participants dislike the fingerprint because it requires an additional USB device. Based on this it is decided that this method would not improve the current situation of online banking authentication.

On the other hand participants questioned the security and precision of facial recognition. This uncertainty is acknowledged and therefore the subject was researched[4]. From this research it is concluded that facial recognition actually can be secure and precise.

Altogether, the decision was made to improve our facial recognition prototype and continue designing this authentication method.

3.1.13. Revised product concept and requirements

After analyzing our prototypes it was concluded that facial recognition would be the best option for online banking authentication. The overall concept remains the same when using the facial recognition method: providing a smooth and safe online banking environment for people who are not well-known with online banking.

The technical requirements of our prototype remain the same because security and reliability are requirements which are obvious for an authentication method. Also the multiple steps authentication remains a requirement because the bank insisted on this during our meeting. The user requirements also remain the same because the goal is still for our system to be easier in use than the current online banking methods. Also the feedback requirement is an overall requirement which is still related to the facial recognition prototype.

The requirements below have been ordered MoSCoW: Must, Should, Could, Won't.

Technical

- The system must be secure
- The system should provide clear and easy steps to user to accomplish their task
- The system should at no times take longer than 10 seconds to respond
- The system should clearly display its status
- The system should be available at all times
- The system won't replace the complete online banking experience

User

- The system must give the user appropriate feedback at all times
- The system must help prevent the user from making mistakes
- The system should be usable for novice computer users
- The system should support the users in doing their tasks
- The system should be easy to learn

4. Design of final Hi-Fi prototype

In this section it will be elaborated how the Hi-Fi prototype is a result of earlier project phases. Previously it has been decided that our main focus was on online-banking authentication. Generally, the way to authenticate customers is to have them present some sort of factor to prove their identity. Authentication factors include one or more of the following[5]:

1. Something a person knows - commonly a password or PIN. If the user types in the correct password or PIN, access is granted.
2. Something a person has - most commonly a physical device referred to as a token. Tokens include self-contained devices that must be physically connected to a computer or devices that have a small screen where a one-time password (OTP) is displayed, which the user must enter to be authenticated.
3. Something a person is - most commonly a physical characteristic, such as a fingerprint, voice pattern, hand geometry, or the pattern of veins in the user's eye. This type of authentication is referred to as "biometrics" and often requires the installation of specific hardware on the system to be accessed.

After conducting evaluation session with users, it is concluded that the most interesting prototype to pursue is the one with NFC scanning and facial recognition. The Hi-Fi prototype combines something a person has (passport) with something a person is (facial recognition).

To get more insight in the subject of authentication, investigate possibilities and, feasibility of our prototype a conference call with the Rabobank has been arranged. This meeting took place at 10 December 2015. The project concept and results so far were explained during this meeting.

The Rabobank told us that they are always exploring new methods for online banking verification and that they have knowledge about the techniques used in our Lo-Fi prototypes. The biggest concern at the bank is, as may be expected, security. Regarding biometric verification methods, Rabobank told us that it is undesirable for the bank to have to keep a database of biometric records for their customers.

Furthermore, they elaborated on why they do not currently use any external USB peripherals for online banking authentication. The problem with an external USB-device is that it requires drivers or software to manage it. This would require the Rabobank to distribute and maintain software which is something the bank does not want to take care of.

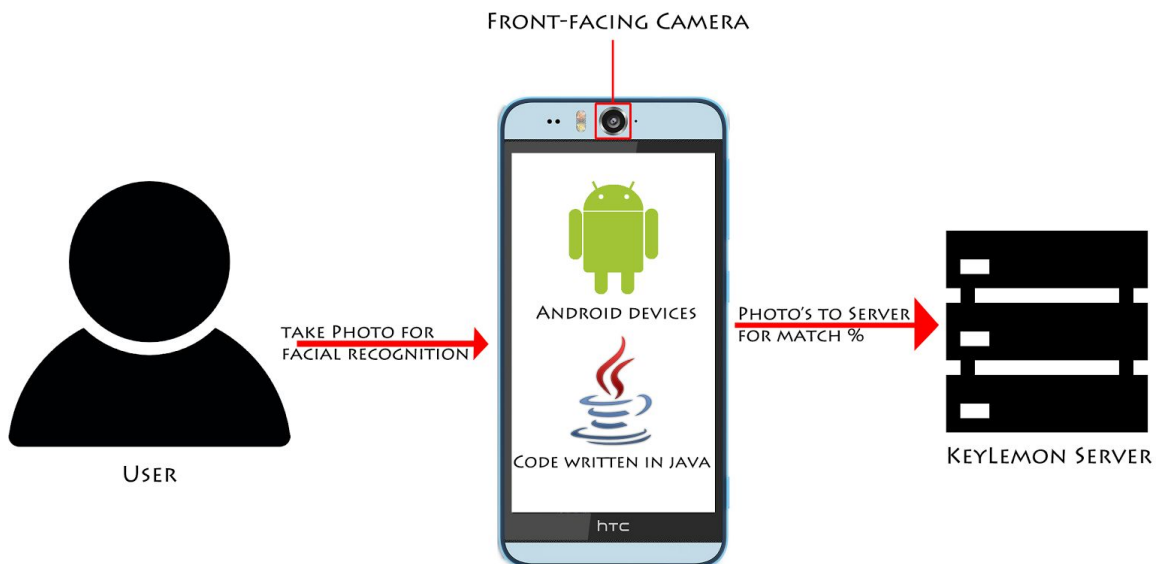
As a result of the above conversation it has been concluded that, if biometric verification would be used, the records would need to be stored locally for maximal security. Moreover, using a USB-device to read data from a debit card using NFC is a definite no-go.

Because a definite form of our solution has not yet been defined, it has been decided to focus our solution specifically for smartphones. A smartphone is not affected by the issue of needing drivers for the NFC chip since it is already available through the phone's API. Not all members of the target group might own a smartphone, but this form factor has been chosen in favour of security and based on feedback from Rabobank.

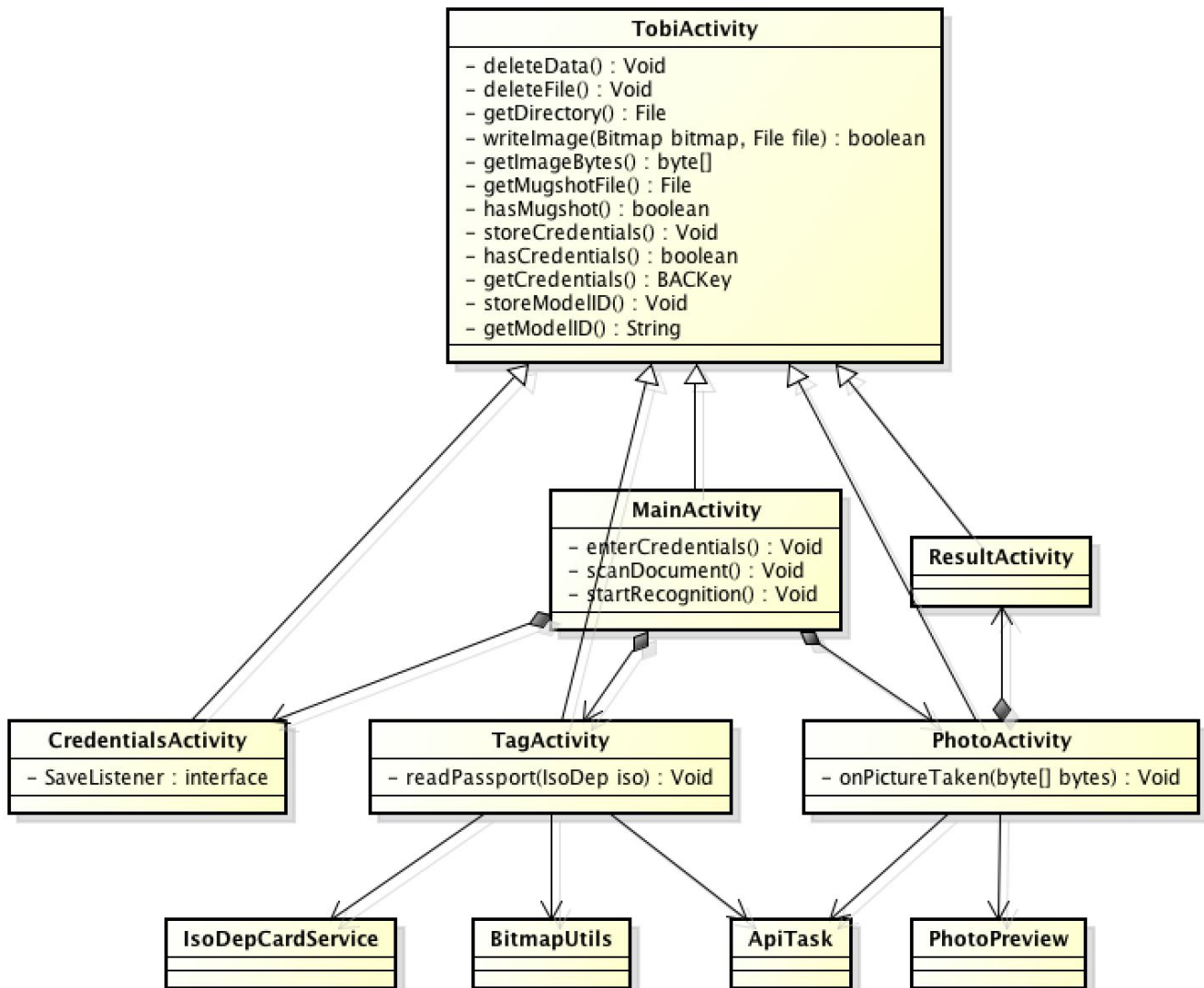
Refer to appendix B for the conference call notes (Dutch)

4.1. Architecture

The end result is an Android app, which will be written in Java. In order to use this app, the device needs to have a front facing camera and NFC capabilities. The app communicates with the online KeyLemon services by using their API, provided on their website.



4.1.1. Class diagram



4.1.2 Code flow

Each Activity inherits functionality from TobiActivity.

- MainActivity: checks which activity needs to be launched.
- CredentialActivity: filling in credentials.
- TagActivity: reading identification document with NFC.
- PhotoActivity: taking a selfie and uploading it
- ResultActivity: result of comparing selfie with model photo.

4.2. Interaction flow

After the user starts the application he is asked to scan his debit card with the phone's NFC reader to confirm his online banking account information. Next, the user needs to scan official identity document with integrated NFC chip provided by the government. Since a photo of the user is embedded in the NFC chip of such a document, it is used to create a model for the next step; face recognition. The user will have to look straight in the phone's camera. A photo will be taken and the model generated from this photo will be compared to the model generated using the reference photo from the official document. If the models match up, the user is successfully authenticated. Otherwise, authentication fails.



Wij lezen uit:
Rekeninghouder
Rekeningnummer
Pasnummer



Wij lezen uit:
Foto

1. Tweede foto, met 3d effect
2. Eerste foto, met reliëf



Wij controleren of het gezicht voor de camera overeenkomt met het gezicht op de ID-kaart.

4.3. Implementation

The Hi-Fi prototype will be implemented in the form of an Android application.

4.3.1. Facial recognition

Facial recognition is a rather complicated subject and there is only a limited amount of time to create our high-fidelity prototype. It was decided to rely on a third-party API provided by KeyLemon to recognize faces.

The API is free to use for up to 1.000 face verifications. The amount of requests is limited at 100 per hour. The limits prove no problem for our prototype. KeyLemon provides wrappers for various popular programming languages which help connecting to their API from our software solution.

KeyLemon provides a Java wrapper which will be used to interact with their API.

4.3.2. KeyLemon communication

No networking can be done on the main-thread in Android apps. The entire network will be using AsyncTask as assistance:

<http://developer.android.com/reference/android/os/AsyncTask.html>

Inside this AsyncTask, the wrapper of KeyLemon or Android's networking API's will be used:

<http://developer.android.com/reference/java/net/URLConnection.html>

Networking requires the following two permissions:

```
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
```

4.3.3. Taking pictures

In order to recognize a face, it is necessary to capture picture which can be used to compare. All modern Android smartphones have a front-facing and rear-facing camera. The Android Camera API will be used to capture the images:

<http://developer.android.com/reference/android/hardware/Camera.html>

The Camera API requires the following permission:

```
<uses-permission android:name="android.permission.CAMERA" />
```

It is also required for the Android device to have a camera:

```
<uses-feature android:name="android.hardware.camera" android:required="true" />
```

To store the taken pictures and read them, the following two permissions are required:

```
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
```

4.3.4. Using NFC

A captured face has to be compared to the 'original' face. A 'mugshot' works the best[5] for facial recognition. The new Dutch passport, driving license and ID card all have an NFC chip built-in. The Dutch government requires images on these documents to be a mugshot.

The Android NFC API will be used to read NFC tags:

<http://developer.android.com/reference/android/nfc/package-summary.html>

It is possible to obtain the picture used on all of three document. Taken pictures will be compared against this picture.

In order to use the NFC API, it is necessary to add the following permissions:

```
<uses-permission android:name="android.permission.NFC" />
```

Moreover, the Android devices will be required to have a NFC chip:

```
<uses-feature android:name="android.hardware.nfc" android:required="true" />
```

4.4. Product

While creating the product, it was tried to follow the guidelines mentioned above.

However, it turns out the KeyLemon Java Wrapper does not work in combination with Android. This is caused by a different implementation of Apache libraries and networking in general. Eventually it was necessary to write our own code to communicate with the KeyLemon API.

There was not enough time to write the code to scan an ID card, driving license or passport with the help of NFC. Instead, a photo picker was implemented, allowing the user to select a photo which will be used as the 'mugshot'. It will be tried to include the NFC scanning capabilities in a future version of the app.

It also turned out, the minimum Android API needed to be increased from 14 to 16 since our app requires some methods which require this API level.

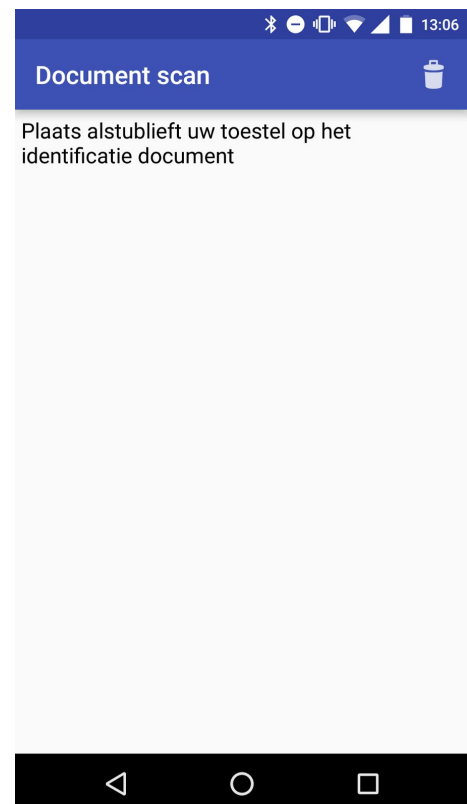
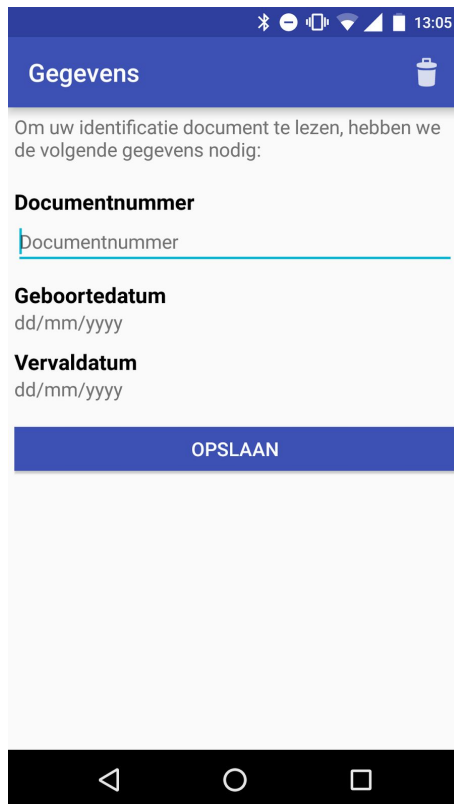
The biggest challenge was reading data from the identification document by using NFC. After many hours, JMRTD could successfully be implemented: An Open Source Java Implementation of Machine Readable Travel Documents.

Taking a photo with the front-facing camera is also harder than one might expect. It was necessary to determine which camera is the front-facing camera which caused some struggles with mirroring, aspect ratios and showing a preview to the user.

Step #1: Entering details of your identification document

The user needs to enter some details of their identification document. This information is needed in order to read their identification document with NFC.

Step #1



Step #2

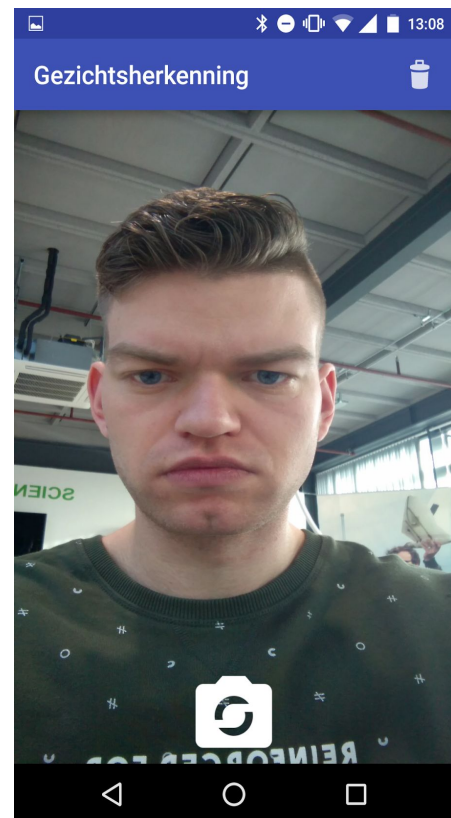
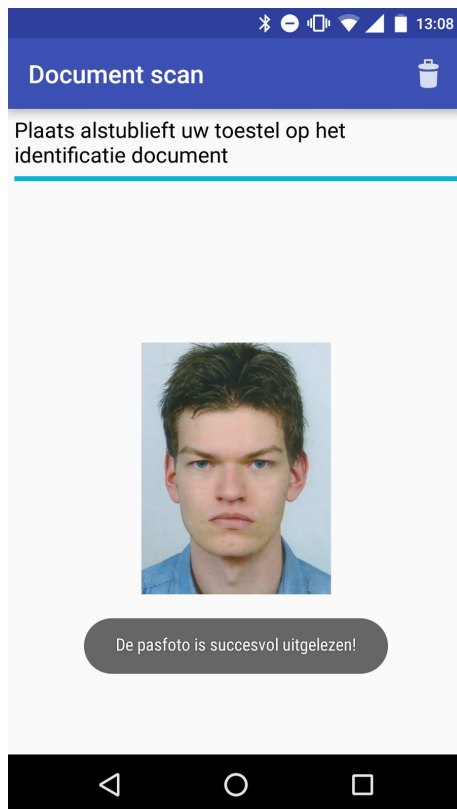
Step #2: Scanning your identification document

ePassport data is protected by a technique named Basic Access Control. The passport data can be read by generating a decryption key which is based on the document number, day of birth and expiry date.

Step #3: Retrieved photo from identification document

The photo should have been retrieved successfully from the identification document by now. This photo is uploaded to the KeyLemon servers, which returns a Model ID. The ID is stored on the device of the user.

Step #3



Step #4

Step #4: Taking a photo

The photo is uploaded to the KeyLemon servers in combination with the model ID. KeyLemon gives a response which tells us if the taken image matched the model image.

Step #5: Logged in

In case there is a high enough parity, the user will get logged in.

5. Expert evaluation

An expert evaluations was conducted with the members of group 34. The ten design heuristics were evaluated.

Visibility of system status

The status if the system is easily visible at all times. The toast notifications during authentication present the user with useful information.

Match between system and the real world

It is clear what information is needed from the user (e.g. document number, expiry date). And the application uses concise terms which are easy to understand.

User control and freedom

No remarks.

Consistency and standards

When tapping the back button it is to be expected that the app closes itself. This doesn't happen. Instead the app reopens itself again. Tapping the back button multiple times crashes the application.

Error prevention

The textbox provided for the document number allows for multiline input this should be corrected since there is no need for multiline here. Furthermore, the datepickers allow for an expiry date earlier than a birthdate.

Recognition rather than recall

Little to no aspects need to explicitly be remembered since the usage of the app speaks for itself. The app seems very simple to use and straightforward.

Flexibility and efficiency of use

Authentication is very simple after the initial setup steps. Scanning the identification card / passport takes quite some time. Maybe this could be made to work faster?

Aesthetic and minimalist design

The application's design is very... blue. Basic design guidelines for Android have been followed.

Help users recognize diagnose and recover from errors

No remarks.

Help and documentation

No help and/or documentation is present. Maybe the user could use a little help to set things up for the first time.

5.1. Conclusion

The prototype scores quite well on all the heuristics. All necessary methods and features are present to perform a good authentication. On some points the prototype definitely needs improvement, there is no help and documentation implemented, this is necessary to provide a satisfactory experience to the user. The error prevention of our prototype should also be increased so that the users are provided with a secure system. The prototype is good in line with the heuristics but it also leaves room for improvement.

6. User evaluation

6.1. Goal

The goal of the prototype is to gather information about the speed, ease of use, and security of our facial recognition method in an environment where a user logs in to do online banking.

6.2. Evaluation question

To what extent enhances face recognition, as authentication method, the user's log-in experience regarding the feeling of safety, speed (efficiency) and ease of use (compared to current methods)?

6.3. Hypotheses

H0: Authentication using facial recognition is considered as good as the traditional authentication methods in terms of efficiency, ease of use and feel of security.

H1: Authentication using facial recognition differs significantly in terms of efficiency, ease of use and feel of security from traditional authentication methods.

6.4. User tasks

- Logging in: The users are asked to log in to the a fake online bank using our prototype facial recognition authentication method.

6.5. Recruitment

In order to test the prototype on the desired target group, participants from the elderly people computer club in the library will be approached. Moreover, each of the members of the group asks their relatives that fit our target-group profile to evaluate the prototype. These participants are readily approachable.

Additionally a smaller group of adults will be asked in order to get broader results since the technology affects everyone who does online banking but mostly elderly who struggle with it. These adults will be recruited by field studies.

The aim is to recruit at least 20 participants.

6.6. Evaluation of the results

Evaluation of the prototype is to be done for three aspects:

- speed/efficiency
- ease of use
- feel of security

For each of these a description for evaluation is given.

Ease of use and efficiency

The evaluation of the ease of use and efficiency consists of three parts. The first part is the first half of our survey. Which will be taken before the test with the prototype. The survey includes questions about the user's experience with the online banking authentication method they currently use.

The second part is observation during the test. While the user is participating, observations will be made regarding, facial expressions (confusion, happiness, frustration etc.), cursor movement on screen (confidence, repetitive actions) and general body language.

The final part is the second half of the survey. This part includes questions specifically about the prototype they use had hands-on with.

Feel of security

The same survey is used as mentioned above to evaluate the feel of security. This means that the survey includes questions about what the user knows about the authentication methods that the user uses currently and about the method introduced in the prototype.

6.7. Detailed plan

The Hi-Fi prototype testing procedure will proceed according to the following pattern:

Before testing the prototype, every participant is asked to fill out the first half of a survey about their current online banking behaviour and pre-knowledge about the topic. This provides a baseline to evaluate from. During the prototype testing, the participant's behaviour, since it reveals emotions and reactions to what happens on the screen which cannot be captured using a survey, will be observed. The general experiment setup consists of a smartphone or tablet with a front faced camera. After testing the prototype, participants will be asked to fill out the second part of the survey. Moreover the participants will be asked about their personal impression of the system after answering the survey. By doing this, it is possible to talk about the weaknesses of the system since the participants already evaluated the interface.

6.7.1. Facial recognition with NFC ID card and NFC debit card

Setup

The participants are provided with a smartphone or tablet which has our prototype application installed. Make sure that the NFC settings are enabled and that the front facing camera is not blocked by anything. The participants need a modern identity card or passport with NFC chip.

In case they do not own a passport with NFC, a replacement passport featuring NFC will be provided.

The environment will be a close match to the usual situation in which people perform online banking. This means that the participants will be sitting down at a table in a reasonably quiet room.

Execution

Before starting the experiment, the participants will be introduced to the problem and the solution/ prototype operation will be explained in order to avoid confusion (since the participants are elderly people).

Then the participants are told to follow the instructions as provided by the application completing an online log-in procedure. The intention is to make the application as clear as possible so that every participant can easily perform the prototype test.

Step by step plan

1. Introduction to the topic of the experiment
2. Participant fills in Before-experiment survey
3. Execution
4. Observing participant's behaviour while doing the experiment
5. Participant fills in After-experiment survey
6. Group asks participant about more detailed impression of the system

Explanation

Facial recognition is based on a reference image of the user that is stored in a database. When authenticating this image is compared to a new image that is taken from the authentication procedure. Intelligent algorithms can identify different positions and shapes of eyebrows, cheeks, eyes, jaws and noses which make the system very secure. Together with fingerprints and voice recognition it belongs to the three biometric authentication methods which can be considered as very safe in terms of forgery.

The NFC method uses the NFC tag which is located in most modern identity cards. When authenticating this tag it will. If the the tag corresponds to the user it will send a signal to the system.

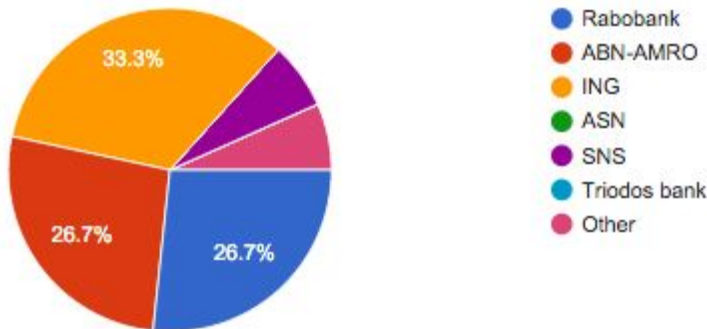
6.8. Survey questions

For evaluation one surveys will be used. This survey is divided into two parts. The participant is asked to fill out the first part of the survey before they use the prototype. The second part of the survey is filled out after. The survey questions can be found in appendix C.

Part one

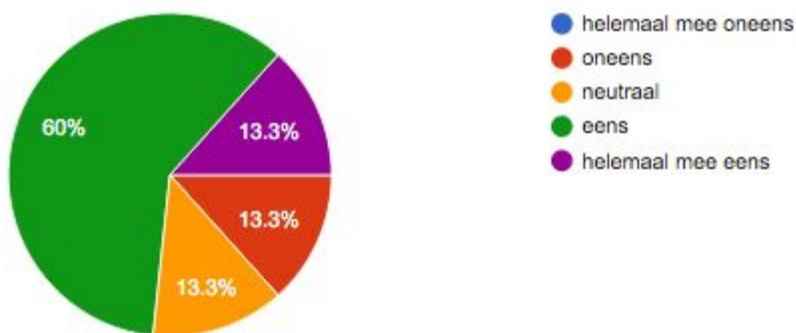
The prototype was tested and evaluated by fifteen participants that fitted our profile of the target group. During the testing participants were asked to fill out a short survey before they started testing our prototype. This was done to collect data about their current online banking authentication.

Bij welke bank maakt u gebruik van online bankieren? *Which bank do you use for online banking?*



5/15: ING
4/15: ABN-AMRO
4/15: Rabobank
1/15: SNS
1/15: Other

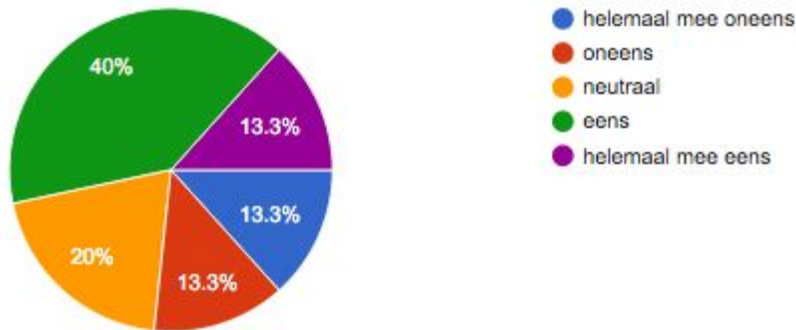
De huidige bankier methode voelt veilig. *The current banking method feels safe.*



2/15: feels totally safe
9/15: feels safe
2/15: neutral
2/15: not safe
0/15: not safe at all

13/15 participants experience their current banking method as safe.
2/15 participants experience their current banking method as unsafe.

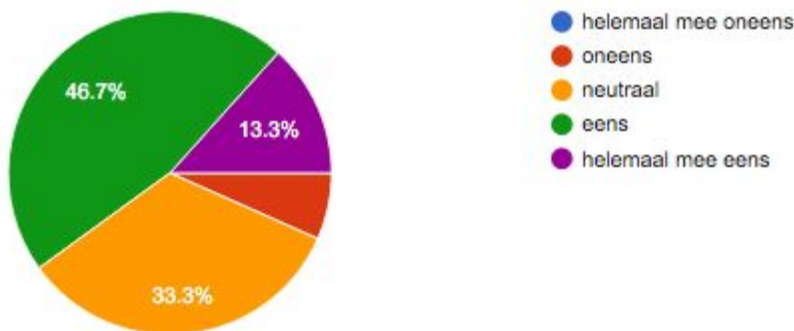
Ik begrijp hoe de huidige bankier methode technisch in elkaar steekt.
I understand the technical background of the current banking method.



2/15: understands completely
 6/15: understands
 3/15: neutral
 2/15: no understanding
 2/15: understands nothing

11/15 participants understands how their current banking method works.
 4/15 participants do not understand how their current banking method works.

De huidige bankier methode is efficient.
The current banking method is efficient.



2/15: totally efficient
 7/15: efficient
 5/15: neutral
 1/15: not efficient
 0/15: not efficient at all

14/15 participants agree their current banking method is efficient.
 1/15 participants finds their banking method inefficient.

Based on the open questions in which is asked what the participants like and dislike about their current method, it was identified that people dislike current methods because of the way

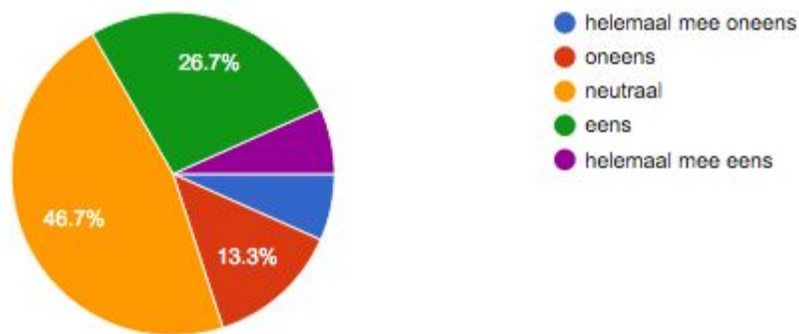
they have to authenticate but not the indistinctness of the steps that have to be executed. The steps which they have to follow to authenticate on their online bank account are clear, but they have trouble with executing the steps because of the devious methods that are being used.

Part two

After finishing the survey, the participants are asked to test the prototype. After testing the prototype they are asked to continue answering questions of our survey.

De methode van het prototype voelt veilig.

The method of the prototype feels safe.



1/15: feels completely safe

4/15: feels safe

7/15: neutral

2/15: feels unsafe

1/15: feels completely unsafe

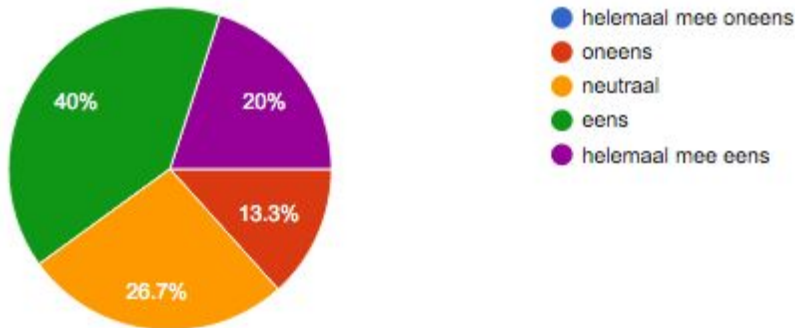
5/15 participants find our prototype method safe

7/15 participants are neutral

3/15 participants find our prototype methods unsafe

Ik begrijp hoe de methode van het prototype technisch in elkaar steekt.

I understand the technical background of the method used by the prototype.



3/15: understand completely

6/15: understand

4/15: neutral

2/15: do not understand

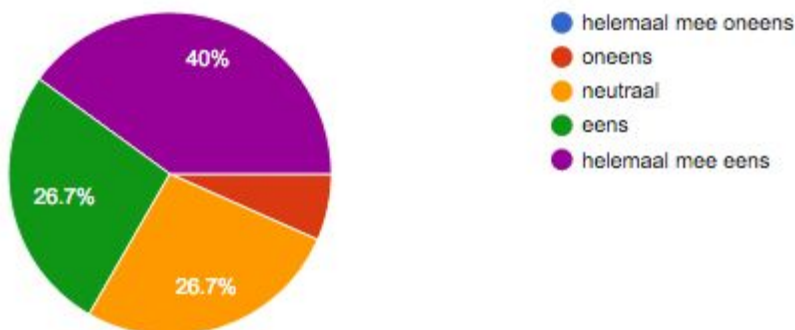
0/15: do not understand at all

13/15 participants understand the technical background of our prototype.

2/15 participants do not understand the technical background of our prototype.

De methode van het prototype is efficient.

The method used by the prototype is efficient.



6/15: completely efficient

4/15: efficient

4/15: neutral

1/15: not efficient

0/15: not efficient at all

14/15 participants experience our method as efficient.

1/15 participants experience our method as inefficient.

Participants were asked what they liked and disliked about our prototype method with open questions. The main result was that the participants liked the method for being really quick and that they had to give much less input than that they have to do with their current method.

The main concern our participants had was about security, they were wondering if another person could authenticate if they had a picture of them. This disliking can immediately be repaired by saying that in our prototype you had to take a picture which would then be used for facial recognition.

In the real product, the facial recognition would make use of a so called “sign of life” method where the user for example has to blink to authenticate. Implementing this would rectify this problem.

Statistical Analysis

To see whether the Hi-Fi prototype is significantly more secure, easier to understand or more efficient a paired sample t-test was performed on the data. Below is a comparison of the results from the current method data with the results of our prototype data.

The current banking method feels safe.

Paired Samples Statistics

	Mean	N	Std. Deviation	Std. Error Mean
Pair 1 Feeling about security	3,73	15	,884	,228
Feeling about security (Survey2)	3,13	15	,990	,256

Paired Samples Correlations

	N	Correlation	Sig.
Pair 1 Feeling about security & Feeling about security (Survey2)	15	,044	,878

Paired Samples Test

		Paired Differences				t	df	Sig. (2-tailed)	
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower				Upper
Pair 1	Feeling about security - Feeling about security (Survey2)	,600	1,298	,335	-,119	1,319	1,790	14	,095

*Survey2 refers to our prototype method

Looking at both means it seems that the participants feel safer using their current online banking method (3.73), rather than using our prototype method (3.13). This indicates that people do not feel safe using the facial recognition as implemented in our prototype. This can be caused by the innovative nature of our prototype, but also because of the earlier discussed disliking of our participants, which refers to the “sign of life” method of facial recognition.

From the results of the paired samples test it can be concluded that there is no significant difference between both methods as when sticking to the original alpha (Sig. (2-tailed)

boundary of 5%. The alpha in this case is 9,5%, this means that the hypothesis that there is no difference in feeling about security cannot be rejected.

I understand the technical background of the current banking method.

Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	Knowledge of technology	3,27	15	1,280	,330
	Knowledge_of_tech (Survey2)	3,53	15	1,060	,274

Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	Knowledge of technology & Knowledge_of_tech (Survey2)	15	,625	,013

Paired Samples Test

		Paired Differences				t	df	Sig. (2-tailed)	
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower				Upper
Pair 1	Knowledge of technology - Knowledge_of_tech (Survey2)	-,267	1,033	,267	-,839	,305	-1,000	14	,334

*Survey2 refers to our prototype method

From the first table it becomes apparent that the mean of the prototype method is in small favor this time. People seem to know more about the technology behind NFC and facial recognition than their current method. Although the difference is very small.

This is also shown by the paired samples test executed in table three. For alpha is 5 the hypothesis that the knowledge of technology differs cannot be rejected, because the calculated sig. (2-tailed) is 33.4%. Meaning there is no significant difference in knowledge of underlying technology of both methods.

The current banking method is efficient.

Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	Opinion on efficiency	3,67	15	,816	,211
	Opinion on efficiency (Survey2)	4,13	15	,834	,215

Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	Opinion on efficiency & Opinion on efficiency (Survey2)	15	-,245	,379

Paired Samples Test

		Paired Differences				t	df	Sig. (2-tailed)	
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower				Upper
Pair 1	Opinion on efficiency - Opinion on efficiency (Survey2)	-,467	1,302	,336	-1,188	,254	-1,388	14	,187

*Survey2 refers to our prototype method

In the first table, which refers to the participants opinion on efficiency of the authentication method, it states that the prototype method's mean (4.13) is greater than the mean of the participants current method (3.67). This is in line with the answers on the open questions referring to efficiency.

The difference in means is reason enough to test if this difference is also statistical significant. When a paired samples test is performed the result of sig. (2-tailed) is 18.7%. Which once again means that there is no reason to reject the hypothesis, if alpha is restricted to the standard alpha of 5%. Concluding that there is also no significant difference in efficiency of both prototype and current method.

6.9. Prototype analysis

Some of the problems or dislikings that participants pointed out were already acknowledged before testing. Such as the problem with a "sign of life" method as discussed in this chapter. It was also known that our facial recognition was not perfect and would not be able to recognize all of our participants. Therefore the system is implemented in our prototype in such a way that the participant would not notice that they were not really recognized. The facial recognition did not work as intended, because of the use of a free accessible API that is available on the internet. For future prototypes there is need for a more solid implementation of facial recognition.

Another aspect that has to be improved before this prototype can turn into a valuable product is the method of using your ID-card. In our prototype you only have to use your ID-card once to create a model of your face. Because of privacy this is not an optimal solution. If you only have to use your ID-card once, it means that your sensitive data is stored on your mobile phone, this might cause security issues if you lose your phone or get hacked. To solve this problem it is recommended to let the user use his ID-card every time he wants to log in. Then when the card touches the NFC reader, the application will be able to read information of the card, but when the card doesn't touch the NFC reader anymore, the data will no longer be accessible and deleted from your phone.

It is strongly recommended to use an ID-card in combination with facial recognition because a user should legally always carry a sort of ID-card. This can be a identity card, a passport or even a driver's license. In the future they will all be outfitted with an NFC tag. The application can easily link a citizens service number, taken from the ID-card, to every bank. This is possible because a bank collects your personal data whenever you open a bank account. It could also be possible to use a bank's debit-card instead of a ID-card, but this would mean that the bank has to store privacy sensitive information on a debit card, which they might not like because of privacy regulations. During the conversation with Rabobank, they told us that they do not want to be in charge of privacy sensitive information.

6.10. Conclusion

From the evaluation of the prototype tests, it can be concluded that the facial recognition needs further improvement to guarantee safety and to make our product easier to use. Although it could not significantly be proven that our prototype was more efficient than the participants current online banking method, there is reason to believe that it might be in the future. The participants might have been influenced by the way in which the system is implemented in the Hi-Fi prototype. In the open questions participants mostly stated that the method of our prototype was faster than their current method. When comparing the means of both efficiency datas, indeed a positive difference in favor of our prototype is visible, but not significant enough to prove this hypothesis.

7. Discussion

In the beginning the idea was to create a new user interface of the most frequently used computer operations for the elderly. Aim of that concept was to simplify user tasks so elderly people could use computers with more ease instead of getting confused or even indisposed to use computers.

However, since online banking is soon mandatory at all banks in the Netherlands, we decided to create an online authentication method which is less confusing for elderly than the current method. This was also the result of the first discussion when we visited a computer course for elderly people. Therefore we decided to stick with that concept and develop a new authentication method that is easier to use and does not require as many additional tools as online banking at present. Looking at the final prototype, an authentication device using facial recognition in combination with a NFC reader was developed.

Even though it could not be proven according to the statistics, the feedback on the design was rather good. The participants liked that the new method comes with less 'effort' from the user side but also works faster than the normal method. More participants are required in order to receive more significant results which would increase the accuracy of the surveys.

Most concerns regarded safety concerns which could be an issue in terms of forgery/hacking. Though, since the technology is still a prototype, for a final product these concerns would have to be abolished. Looking at the big picture of this, the problems can be removed, especially when cooperating with banks which use tremendously high safety measures to protect their users' privacy. However, some remarks questioned the improvement of speed, stating it would take equally long as filling in the account details which should be improved for a final product.

In general it can be said that facial recognition is a good alternative to the current authentication methods, especially when being applied to professional online banking, guaranteeing security for their users. Stepping up to the 'professional' level of online banking can remove most of the concerns received by the prototype testers which makes it a more easy to use authentication method. However it also requires technology (smartphones) that elderly people presumably do not know how to operate. Therefore currently there is no proper alternative to the 'classic' method for elderly people but facial recognition could be a good option for future use.

Improving this, it could be possible to create a device similar to random readers that can execute facial recognition tasks which can also be operated by the elderly. Though the problem of that is that then again a secondary device is necessary for online banking. Therefore it is not as efficient as the previous solution but probably easier to use for the elderly.

In terms of the testing itself, the following can be said: the amount of participants used to test our prototype might have influenced our statistical analysis, it was hard to find enough participants fitting our target group. Nevertheless, we think that we have been able to test

our prototype and evaluate it with our users good enough to see that our prototype might become a feasible product in the future.

8. References

[1] M. Burkhard and M. Koch, "Evaluating Touchscreen Interfaces of Tablet Computers for Elderly People", 2012.

[2] B. Neves and F. Amaro, "Too Old For Technology? How The Elderly Of Lisbon Use And Perceive ICT", The Journal of Community Informatics, vol. 8, no. 1, 2012.

[3] S. Fong, Y. Zhuang, I. Fister and I. Fister Jr, "A biometric authentication model using hand gesture images", Download.springer.com, 2016. [Online]. Available: <http://www.biomedical-engineering-online.com/content/12/1/111>. [Accessed: 19-Jan-2016].

[4] P. Pattanasethanon and C. Savithi, "Human Face Detection and Recognition using Web-Cam - ProQuest", Search.proquest.com, 2016. [Online]. Available: <http://search.proquest.com/openview/6d00fc5a3d4fc233b0f1d50f92b7777c/1>. [Accessed: 19-Jan-2016].

[5] "Authentication in an Internet Banking Environment", 2005. [Online]. Available: <http://assets.complianceexpert.com/fileserver/file/10640/filename/6-96G-CGPMTSYS-Appendix-10-image.pdf>. [Accessed: 19-Jan-2016].

9.0 Appendices

A - Interview questions & answers

Questions

Interview for Elderly who follow computer lessons

1. What do you like about using a computer?
2. What do you not like about using computer?
3. What features on a computer are most interesting to you? What features do you use most?
4. What about a computer do you find interesting to learn more about?
5. Do you have a computer or laptop at your home?
6. What caused you to start following computer lessons?
7. Did you have any knowledge prior to taking the lessons?
8. Do you own a mobile phone? Is it perhaps a smartphone? Do you ever use it to interact with your computer?
9. Does your family ever help you with your computer? What do they help you with?

Interview for Elderly who DO NOT follow computer lessons

1. Do you use a computer? If so, what do you use it for?
2. What features on a computer are most interesting to you?
3. What do you find difficult/frustrating about using a computer?
4. What about a computer do you find interesting to learn more about?
5. Do you have a computer or laptop at your home?
6. Would you consider following computer lessons? and why?
7. Do you own a mobile phone? Is it perhaps a smartphone? Do you ever use it to interact with your computer?
8. Does your family ever help you with your computer? What do they help you with?

Interview for people who teach computer lessons to elderly

1. How much experience do you have with using computers?
2. What caused you to start teaching elderly in using computers?
3. What is the age group which you teach the most?
4. What are your 'students' most interested about?
5. What do your 'students' find the most difficult about a computer?
6. What feature should benefit elderly people the most?

Follow-up questions to online banking

1. On which devices do you get your banking done?
2. Do you have any problems with online banking?
3. With what particular actions do you have problems? (logging in, transferring money, overview your accounts)

4. What do you think that would improve online banking

Answers

Grandmother of Melcher

Interview for people who teach computer lessons to elderly

1. Unexpected notifications are really annoying, not sure what to do with them. What happens when they are clicked?
Step for step is a must. If something has been explained one time, it probably needs to be explained another time.
2. Transferring photos
3. Owns a laptop
4. Owns a normal phone and iPad.
5. Family helps with updating computer applications.

Grandmother of Selwyn

Interview for people who teach computer lessons to elderly

1. Apple iPad not user friendly for the elderly. Confusing interface, too fast animations. Android preferred. Windows PC OS of choice due to familiarity.
2. Language barrier -- > English is often difficult to understand
3. Online banking often difficult and scary. Particularly SNS, because of their small 'pin device'. Elderly often ask others to do it for them, and bank often does not offer enough assistance.
4. Problems often arise after they have done something but do not remember what they did.

Great-aunt of Jan Jaap

Interview for Elderly who DO NOT follow computer lessons

1. Keep in contact with grandchildren
2. Does not like all the different colors and different interfaces
3. Most used feature is Facebook, e-mail and news
4. She wants to keep her knowledge up to date but does not require anything more of her computer, she is satisfied
5. She has a laptop, which is two years old
6. No, she is not very mobile and can do everything she wants
7. Does not own a mobile phone nor smartphone.
8. Yes, family helps cleaning the pc up, ordering files, keep the browser fast

Online banking

Not interested in doing online banking. Maybe if it was easy and secure, even for her.

Female computer lesson student #1

1. Has Windows 7 but wants to upgrade to Windows 10 before Summer because the upgrade will be for free
2. Transferring photo's is hard and she would like to learn how to do so, to keep all her photo's ordered. She wants to take pictures in museums, etc. Her daughter or friend has to help her at this point.
3. She is able to bank online (Rabobank) without much problems. She knows how to use the new Rabo Reader with a scanner inside. She doesn't like the post and notifications which she receives.

Female computer lesson student #2

1. E-mails a lot and this is quite easy for her nowadays. She can even send group e-mails.
2. She has a tablet and smartphone, and likes using them as well. She can do everything what she wants, but doesn't know about all the capabilities and is not interested in learning more.
3. Her biggest problem with computers is not learning new things, but to maintain the knowledge. If she needs to do a certain task after not having done it for a month, she usually doesn't succeed.
4. She has over 100 other hobbies so she doesn't necessarily want to learn more about computers.
5. She has never done online banking, and doesn't want to because she finds it scary. Her bank has an office in the city and she can do all her banking-related stuff in there.

Female computer lesson student #3

1. Likes using the computer to e-mail and to google things.
2. Does not like the different version of Windows, different interfaces, inconsistency
3. Most used feature is e-mail, google and read news
4. She wants to learn more about computers in general, and specifically how to order her files (e-mail attachment download)
5. She has a laptop at home, it's her 3rd computer and she bought it in the beginning of 2015.
6. She started following computer lessons to get more out of her laptop
7. Yes, she worked on a computer for her work, but in a very simple way.
8. Does own a mobile phone, does not own a smartphone.
9. She uses 'student aan huis' to get help at home

Online banking

She has a very bad internet connection and doesn't think it's going to get better anytime soon. This is one of the main reasons she doesn't want to start online banking. If she had a better connection she would consider it.

Male computer lesson teacher #1

1. Studied educational sciences at the University of Twente. This led to his first interactions with computers. Computer usage evolved into a hobby for him. He has been giving lessons in Enschede for five years now.
2. His background to teaching and his hobby for computers led to giving lessons
3. The average age is around 65-70 years old, but occasionally there are younger people taking lessons as well. Nowadays computer knowledge is pretty much a necessity. Sometimes 'pupils' used computers at work, but only for simple tasks using a single program.
4. The most popular lessons are: Organizing Files, Acquainting with the computer, Introduction to Windows 10. Less popular: Safety on the Internet, Skype tutorial and Tablet tutorials (iPad+Android).
5. The most difficult thing about a computer is usually getting used to using a mouse and keyboard. It's difficult to find the right keys on the keyboard, and to accurately point the mouse on the screen. When to use the right click button, when to use the left click button, navigating through interfaces, etc.
6. There are plans to set up an Online Banking Tutorial. But each bank has a different website, interface and structure. Perhaps we could re-create the interface, hook it up to a database so the pupils can actually do transactions and see the numbers in their accounts change. It would also be interesting to teach people how to order their files.

Male computer lesson teacher #2

1. Experienced with computers. He has been using them since he was 7 years old and follows an IT focussed study.
2. One of the main reasons he started with teaching elderly, is that it is guaranteed of a good income. Besides, he figured he could provide a better service than existing services such as *student aan huis*.
3. The people he teaches are often 60 or older, but there are exceptions: there are also people with ages ranging from 40-60.
4. The majority of the people attending his course wants to learn how to communicate with their children via the computer, and read online news articles.
5. Problems people encounter are often related to creating accounts for things such as Skype Facebook and configuring email accounts. The difficulty usually comes from the many fields that have to be filled in.
6. Elderly would benefit greatly from interfaces with less options, this makes it a lot easier. He had some students who started using a tablet, and never needed any help since. They understood the tablet much better than a traditional computer.

Online banking

- Elderly do either get how to do online banking, or they do not do any online banking at all. The group that knows how to do online banking knows it pretty well. The group that doesn't know how to do online banking doesn't have the knowledge, finds it scary or has another reason why not. There seems to be no middle way where users actually struggle or partially get it.
- They don't get how it works and are scared that they end up making a mistake, which could result in losing money
- The people that find it easy to do online banking usually use their computer. People that struggle with computers prefer using an app on their phone.
- Usually computer users seem to have a smartphone
- A hard part about online banking is the massive amount of input fields. Elderly find it cluttered and complicated. A solution could be to fill the input fields in step by step, only showing one field at the time.
- A new verification method would also help a lot. Using a random reader brings a lot of complication with it. The ING bank uses SMS-verification to verify legitimate use. For elderly this would be easier than using a random reader.

Appendix B - Conference call Rabobank

Donderdag 10 december 2015

Aanwezig:

Marijke Brouwers Distributie manager (namens particulieren)

Gerco Wolfswinkel Distributie manager (namens bedrijven)

Koen Overeem Rabo Corporate Connect

Killian Ros Bedrijfs Informatie Technologie

Jan Jaap de Groot Informatica

Selwyn Nypels Creative Technology

Melcher Stikkelorum Technische Informatica

Afwezig:

Max Mensing Creative Technology

--

Jan Jaap legt projectopzet uit:

1. Interview ouderen: online bankieren terugkerend probleem
2. Ons doel is om de authenticatie makkelijker te maken
3. Lo-fi prototypes gemaakt en getest
4. Hi-fi prototype uitwerken komende weken

Zijn mensen met visuele beperking binnen scope van het project?

Eigenlijk niet.

Achtergrond: Rabo had vroeger de RandomReader, nu de RaboScanner. Deze is echter niet geschikt voor mensen met visuele beperkingen. Daar was altijd de ComfortReader voor met braille en grote toetsen. Deze moet worden uitgefaseerd, want deze is verouderd. Nog geen nieuwe invulling.

Rabophone wordt nu ook nog gebruikt.

Killian legt prototypes uit

Hebben jullie veiligheid meegenomen?

Technische veiligheid is niet meegenomen in de tests, het gevoel van veiligheid wel.

Vingerafdruk opzich, werkt niet al te goed. Is te reproduceren.

Enkel biometrisch methode is te zwak.

Hebben jullie nagedacht over implementatie vingerafdrukscan? Vingerlijnen patroon scan of ook aderpatroon scan? Aderpatroonscan; moet aan een 'levend' lichaam vastzitten om te werken

Killian legt uit dat we van plan zijn om biometrische methoden te combineren met het scannen van een bankpas via NFC.

Killian vraagt waarom banken niet gebruik maken van USB-devices:

Er zijn slechte ervaringen met USB. Dit heeft voornamelijk te maken met het feit dat er drivers moeten zijn voor verschillende besturingssystemen. Software moet worden uitgegeven, bank wordt verantwoordelijk voor software. Wellicht kan lezer worden overgenomen op afstand en heeft echt niet de voorkeur.

Rekening houden met dat de klant altijd moet kunnen terugvallen op andere methode. Altijd een alternatief nodig (met vieze vingers werkt vingerafdruk niet).

Hoe wordt data veilig opgeslagen (vingerafdruk)? Privacy gevoelig.

Achtergrond: FIDO protocol voor biometrie. Ontwikkeld door Google. Win10 is al FIDO complaint met Windows Hello.

Bank wil niet verantwoordelijk zijn voor opslag vingerafdrucken van klanten. Liever alles lokaal opslaan en offline aan de persoon koppelen. Vingerafdruk gaat dus niet over de draad.

Jan Jaap legt idee over combi met bankpas, id-kaart en gezichtsherkenning uit. 'Mugshot' uit de id-kaart lezen, gezichtsherkenning toepassen.

Interessante combinatie. Los waren deze ideeën al wel gepitched
Innovalor gaat de id-kaart techniek volgende week pitchen. Innovalor zit in Enschede, mogelijk kunnen ze iets voor ons betekenen.

Opmerking: Niet zelf het wiel uitvinden. Gebruik maken van bestaande oplossingen.
Nadeel van dit idee is dat relatief weinig telefoons NFC ondersteunen.

Conclusie:

Wij gaan aan de slag met het uitwerken van een prototype waarbij gekeken wordt naar de combinatie van uitlezen van data uit een ID-bewijs (eigen bouw of aanhaken op Innovalor) en het doen van gezichtsherkenning, als eenvoudige en veilige manier van inloggen.

Begin januari nemen we weer contact op met de Rabobank om te kijken waar we staan.

Appendix C - TOBI Questionnaire

1. (closed) Ask whether the participant uses online banking

2: Pie chart

2. (multiple choice)(if answer to 1 was yes) Ask about the bank at which the participant currently does online banking

Indicate that the following questions will be about ease of use of the method the participant currently uses

3,4: Open questions cannot be statistically analysed

3. (open) Ask about what the participant likes about the current method

4. (open) Ask about what the participant dislikes about the current method

Indicate that the following questions will be about the feeling of security of the method the participant currently uses.

5, 6, 7: Histogram + Q-Q plot, testing for normality

5, 6: Paired sample t-test*

5. (Likert) This method of authentication feels secure

6. (Likert) I understand how this method works (technically)

Indicate that the following questions will be about the feeling of speed of the method the participant currently uses.

7. (Likert) This method is as efficient as it could be

Participant should stop here and use the prototype first

Indicate that the following questions will be about ease of use of the method the participant just tested

1,2: Open questions cannot be statistically analysed

1. (open) Ask about what the participant likes about the method compared to their current method
2. (open) Ask about what the participant dislikes about the method compared to their current method

3: Histogram

3. (Likert) This method of authentication is easier to use than the method I currently use

4: Pie chart

4. (closed) Ask whether the two-step verification method is experienced as being significantly more difficult than the single-step verification method.

Indicate that the following questions will be about the feeling of security of the method the participant just tested

5, 6, 7: Paired sample t-test*

5. (Likert) This method of authentication feels secure
6. (Likert) I understand how this method works (technically)

Indicate that the following questions will be about the feeling of speed of the method the participant currently uses.

7. (Likert) This method is as efficient as it could be

8, 9: Pie chart

8. (closed) Ask the participant whether the two-step verification (use of card in combination with face recognition) increased the feeling that the method is secure.

Indicate that the following questions will be about the feeling of speed of the method the participant currently uses.

9. (closed) Ask whether the participant experienced the two-step verification method as significantly slower than the single-step verification method.

All open questions: Since open questions are difficult to analyse in a statistical way, the use of positively and negatively connotated words will be observed in order to filter out (the user's/) a basic attitude. If certain terms are used more frequently this will be recorded.

*Paired samples t-test measures difference for a single group evaluated at two different moments. Since questions 5, 6 and 7 are the same in both surveys, we'd like to see the differences for both evaluations.

We chose to use the Likert scale for multiple of our questions. Initially we had planned to use a scale with 11-points, but we decided against this in the end. We think we will get more consistent results if we use a 5-point scale. Each of the 5 points is labeled;

- Strongly disagree
- Disagree
- Undecided

Appendix D - Summary of Peer-review remark

Due to its length both groups criticized the evaluation question which was therefore too hard to understand. Furthermore there were no expectations stated that describe the desired results of the experiment. Most of the remarks regarded the experimental setup and environment. It was not clear whether the participants would be isolated or tested in a group and what the testing environment would look like: "The setup should be more or less the same for every participant to reduce environmental influences regarding the test." A consent form was missing but as one of the groups already assumed it was not necessary for the experiment since no private data was saved. Moreover a step by step plan, describing the user tasks, was missing. The description of the target group was rather vague and it was remarked that more unrelated people should be tested in order to avoid bias: "It might be wise to also use some other participants, like people at a bank, etc. Relatives are more biased to give the answers you want." Last remark was to replace the survey after the experiment by an interview.

Summary of changes as reaction to the Peer-reviews

After receiving the Peer-reviews, a step by step plan was developed and the environmental setting was clarified. Moreover the recruitment / selection of participants is now broader, allowing to achieve unbiased results from different directions. The participants will now be given an introduction to the general problem which prevents confusion about the technology and/or authentication procedure. However, replacing the survey by an interview will not be done but after filling in the survey the participants will be asked some follow up questions on their impression. By doing this, we hope to get more useful results since the participants already dealt with the topic which (hopefully) gives more elaborated reviews. Eventually the evaluation question has been shortened, featuring now only the main aspects to be evaluated.