UNIVERSITY OF OSLO
Department of Informatics

Authentication methods

INF5261

Final report

Hans-Joachim
Jelena Mirkovic
Ivica Milanovic
Øyvind Bakkeli

Spring 2010

UNIVERSITAS OSLOENSIS MDCCCXI

Table of Contents

1 Introduction

With mobile devices constantly taking a bigger part in our everyday life, the convenience of accessing a bank account, paying for any services or even checking medical journals independently of current time and place is getting more and more feasible. Having in mind that these kinds of services require access to the user's personal information, the logical major requirement is high security and strong user authentication methods.

Through our project we want to address following questions:

- What are most common and accepted authentication methods for mobile services?
- What are differences, opportunities and challenges concerning user authentication for mobile services compared with traditional stationary computers?
- How do people accept them and what are their opinions regarding security on mobile device?
- Evaluation of security / usability / privacy trade-offs for different authentication mechanisms.

We recognize the potential of new mobile services that are emerging (e.g. mHealth, mBanking, mLearning), but we would like to find out if security is on a sufficiently high enough level to provide adequate support for them or they can provide more threats and problems to users than benefits.

2 Methods

The first phase of our project was to perform research on what is already developed and available in the area of user authentication for mobile service. For research we used Internet browsing, as well as search of research databases (e.g. IEEE, ACM, Elsevier). We saw that field of user authentication for mobile device is very wide and tried to organize our findings in four groups:

- Authentication methods based on something the user knows
- Authentication methods based on something the user has
- Authentication methods based on something the user is
- Authentication methods based on users location

For every group we tried to capture the main characteristics and summarize the theory findings through covering four main topics: implementation for stationary devices, implementation for mobile devices, security level that is provided, and usability issues. Based on these results it was easier for us to identify the main challenges, advantages and problems regarding each specific authentication approach. Results of the performed research are described in section three.

Beside theory overview that gave us background information on what is done in the area of authentication for mobile services and enabled us to identify the main characteristics of each of them; we also wanted to gain knowledge about users and their acceptance of authentication methods on mobile devices. For this purpose, we created a questionnaire for usability testing of mobile users. Using the questionnaire we identified main requirements and satisfactions with different user authentication methods. We also found out what are their impressions about authentication requirements for different types of services, what they view as sufficiently secure for different services and what difficulties usually arise when they interact with (mobile) authentication methods. Descriptions of questionnaire and testing scenario are in section four.

When we finished questionnaire we saw that there are some additional questions and unresolved findings that we wanted to investigate further. So we developed simple prototype that simulates different authentication methods and performed interviews with users to gain more descriptive description about their needs and thoughts. The interview and results we gathered are presented in section five.

At the end of the project we evaluated and summarized our findings and presented different types of authentication methods looked from different angles (security they provide, usability, acceptance by users, adaptation to mobile devices). The goal through this project was to see whether usability and security represent two opposing sides of a continuum, what the required balance between them is, and how they are related to types of the services or applications and privacy issues. Final discussion about results we gathered is in section six, and summary of the whole report is presented in section seven.

3 Authentication methods used on mobile and stationary devices

3.1 Introduction

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be [1]. Authentication processes are common these days, as online banking, online services (email, facebook) or even online access to medical journals and similar become more and more usual. The traditional way of authenticating per today depends on three factors that could be something you have, something you are and something you know [2]. The authentication process could include one of these factors or a combination of them all.

3.2 Something the user knows

Methods based on something the user knows are often associated with a password, multiple passwords, or a combination of a password and a username [3]. The user has usually chosen a password before he/she starts using the service. This same password has to be provided by the user for every future use of the service.

3.2.1 Stationary computer approach

In computer-security systems this is the most common method for authentication of users. For most of web applications and services password authentication presents well enough solution. Even though this authentication mechanism does not provide high level of security, it is very easy for implementation, and user is usually free to choose password that is simple for him/her to remember.

3.2.2 Mobile device approach

Based on the success of password authentication on stationary devices, the same approach has also been adopted and used on mobile devices. The first example you can see when you turn on your mobile phone. The first thing that usually happens is that you are prompted for the PIN code, before you can start using your mobile phone. On that manner the user is authenticated to the mobile network, and he/she is protected from loss and theft of the mobile device.

3.2.3 Security level

Security level provided by this approach is not very high. There are numerous of attacks that can jeopardize user’s confidentiality and security. Some of the attacks are: brute force attacks where an attacker try to log in to the service with every possible password until he/she succeeds, dictionary attack where an attacker try only passwords from the previous prepared lists, rainbow attack that present more sophisticated version of dictionary attack where passwords are hashed before and these values are used for attacks. Additionally, more threats can emerge due to improper storage of the passwords provided by the user at the time of registration.

One major problem with password and security is user factor. In most cases user is required to choose password that he/she will use on the system and remember it. The password that is chosen can greatly influence security of the user, and because of that it is very important for user to choose a strong password. On the other hand if the user is forced to choose a complicated and inconvenient password there is another problem with writing it down and forgetting it.

3.2.4 Usability issue

We saw that authentication using passwords provide really low level of security. But also we said that this approach is very popular and widely accepted for stationary and mobile device. The biggest reason for this is high usability and easy implementation. For the user, it is required to remember password that he/she choose, but there is no complicated and demanding authentication process and privacy issues.

3.3 Something the user has

User authentication in this case is based on something that user has, a physical object. An object could be a mobile device or a token. Using this approach, a user is not required to reveal any private information about him/her (like in biometrics) nor is it required remembering some secret information (password).

3.3.1 Stationary device approach

A token could be a small physical device[4] that is often used to authenticate on a website or a similar services. They are used to prove one’s identity electronically, and they exist in different sizes and shapes, and are often small devices that can easily be carried around. Tokens can store different kind of data that is often implemented in a chip and can perform various authentication methods. The four types [4] of tokens are: static passwords, synchronous dynamic passwords, asynchronous passwords and challenge response. The tokens could work as stand alone, or they can be connected to a computer using the USB mechanism or some kind of wireless technology like Bluetooth. The mobile phone itself can also be used as a token for user authentication for services and applications on stationary devices.

3.3.2 Mobile device approach

This approach for user authentication is especially suitable for authentication of a user for mobile applications and services. The biggest reason for this is that mobile device is usually considered as private device that belong just to one person, and because of that is ideal example of “something the user has”. In this manner, the mobile device is functioning as both the terminal providing the service as well as the user authentication token.

There is couple of possibilities how this authentication method can be implemented on mobile devices. The biggest difference lies in how a user's private authentication information is stored or delivered to the mobile phone. The possible approaches are:

- Private information is stored on hardware (e.g. SIM card),
- Private information is stored on the specific file on the mobile device´s file system, and
- Private information is received through mobile service operation (SMS message).

Authentication of the user based on private information stored on a SIM card is usually used by network operator to authenticate subscribers. This approach provides very high level of security because user's private information is stored on tamper resistant cards. For this reason, this approach is becoming more and more popular for authentication of the user for different mobile services (e.g. mobile banking). The biggest disadvantage is that all changes and additions to SIM cards must go through a network operator.

Authentication of the user based on private information stored on mobile device's memory is not dependent on the mobile network provider and user or service provider can more freely install and/or store user's authentication information on mobile device. The secret information can be in different formats depending on the type of services. For example, the user can use certificate that is stored on the mobile phone for authentication or install a specific application that contain user's private information and generate authentication token based on this information. The problem with this approach is that private information is stored on the mobile phone, so if the user changes mobile phone he/she has to acquire the same private information again.

SMS message is an example of authentication of the user based on private information that is received through mobile service operation. The most common scenario is that One Time Password (OTP) is delivered to user during authentication process, which afterwards must be inputted in the log in screen in the original application. Also other scenarios are developed. For example, when user receives a SMS message with the OTP he/she can just reply to the SMS message on the mobile phone. In this approach user is not required to retype OTP, but utilize the telephone network for the second factor of authentication [5] Even thought this approach provides great usability to regular users (there is no need to use complicated application and functionalities of the mobile, but just SMS service that is well known to everybody), there are great trade-offs that this approach introduce . First, there are problems with latency of the SMS services especially during peak SMS usage as holidays. Another one is that text is transferred without any encryption and is visible to service provider. Also, a service provider has the right to store SMS messages on their side (for example when user is not accessible, so the message can be forwarded later on). Finally, there are also serious security vulnerabilities that this kind of authentication introduces e.g. man-in-the-middle attack [6].

3.3.3 Security level

Security level that is provided by using only this method is not so high. If an attacker steals the user's token or mobile device, he or she may gain full access to the user’s private information and services. And today it is not so unlikely scenario that mobile phones are lost or stolen because of their small size and wide deployment in people everyday life. Mainly for this reason, this approach for user authentication is usually used in combination with some other authentication method (most commonly with authentication based on something that user know e.g. password, PIN number). This approach is called two-factor authentication and is frequently used for user authentication for mobile services.

3.3.4 Usability issue

Usability of this authentication approach can vary greatly depending on the type of token used. For example, if authentication token is well chosen and the user is always in possession of token (for example if the token is the mobile phone), the whole authentication process can be very simple and easy for the user. But on the other hand we have examples where token is some stand-alone device which the user does not use very frequently and does not carry with herself/himself at all times. In these situations the user will often be unable to use the service, since he/she does not have the token present at that moment.

3.4 Something the user is

Ways to authenticate a user based on something he/she is are often based on scanning and analysis. These methods, referred to as biometrics, centers around authentication based on that person's unique traits. Traits can be physical, such as fingerprints or behavior, such as walking patterns or typing patterns.

Biometric authentication methods have been developed to counter the possibility that unauthorized persons may gain access when traditional security methods like security pass cards or passwords are used. In the article Making Palm Print Matching Mobile we can read[7] that “the most critical flaw of these systems is that since they do not use any inherent characteristics or attributes of the individual user, they are unable to differentiate between an authorized personnel and an impostor who have fraudulently come to possess the token or knowledge (such as stolen credit card or lost password)." For this reason, various biometric methods have been developed in order to discern legitimate users. These methods include "fingerprint-based systems and iris, retina, face, palm print, voice, handwriting and DNA technologies"[7].

3.4.1 Stationary device approach

Several computer or keyboard models come equipped with finger-print-readers. They offer an alternative to authenticate the user of the machine in addition to traditional passwords. There are also some solutions that require the user to swipe their finger in order to get access to an area or similar. In these cases the readers are attached to or close to doors.

3.4.2 Mobile device approach

In addition to desktop computers, many laptop models ship with fingerprint scanners that can be used for user authentication. With mobile phones, a few models are available with fingerprint scanners [8].

There have been and is ongoing research in this area, and as the technology improves, biometric scanners on mobile devices might be more widespread than what it is today. Some experiments, such as [7] have been able to authenticate users based on palm print scanning using a mobile camera. Also ongoing research is conducted on authentication of users by scanning their wrist veins [9] and recognizing their handwritten signature [10].

3.4.3 Security level

. Some readers are easy to fool, requiring only a glove with an attached fingerprint according to Veum and Flesland[11] Some scanners may also accept cut-off fingers. Other scanners are more thorough and will not fall for simple tricks as this.

In addition, biometric solutions may pose a threat to the user itself. Imagine if unauthorized persons wanting access become aware that the only thing the user needs in order to gain access is to swipe one of his or her fingers. The user now runs the risk of having one of his fingers removed in order for the unauthorized persons to be able to gain access.

Until now there are also known attacks on fingerprint readers, using different materials to simulate finger (e.g. gummy bears)[12]

Biometrics might be best suited for additional security, or as a second factor in an authentication process, rather than being used on its own.

3.4.4 Usability issue

The use of biometrics can be quick and effective. Since it is based on something the user is, it is virtually impossible to loose or forget like tokens or passwords. After all, the user will always have his or her finger available for scanning. However, disabled people might not be able to utilize all biometric solutions. For instance a user in a wheelchair might not be able to utilize solutions based on walk patterns or a person with a broken arm will have trouble with maintaining the typing pattern he or she would have with both hands available.

Some people might value their privacy more than the ability to use a convenient authentication method such as fingerprint scanning. Since this is unique information that might be tied to a single person, their concerns may be justified. For a given solution, which information and how detailed as well as who might have access to this information might affect how a user reacts to such solutions. For one, it might be limited who really needs to store biometric information, like when entering schools [13] Disneyland [14] or even gyms [15]. Another concern is if their information is somehow compromised, the users will not be able to change their fingerprint, like they would their password.

3.5 Location based authentication

Location based authentication is not used much directly in present times, other than for instance limiting access for services such as ATMs. Since we focus on authentication related to mobile devices, we do not discuss other methods such as the use of optical devices for user recognition.

To find the users location some suggested methods involve using GPS capable devices, for instance a newer cell phone, relying on the cell network or using Bluetooth or other range limited technology as a beacon. The different methods have advantages, disadvantages regarding granularity and range and different uses.

3.5.1 Stationary device approach

For stationary use one can see if the user is in proximity of the device being used. One method [16] presented suggests using IP geo location services to get the terminals location. This can then be used directly as a part of the authentication, the user’s phone and the terminal has to be in proximity to get authenticated. It can also be used to suggest what level of authentication one need, if the location is in a workplace or similar perhaps a one-factor authentication could be enough.

One of the patents [16] also suggest multiple mobile device works together with authentication on a stationary device, but one can be in possession of multiple mobile devices and one can check if these are in proximity of each other.

3.5.2 Mobile use

When interacting with a terminal of some sort (using a mobile device for payment or similar), the stationary and mobile methods overlap.

When applied purely in a mobile context, location based authentication would probably move toward determining if a user is at a location. Using some form of automatic positioning systems are one option, using passphrases or secrets located at the location is another.

3.5.3 Security

The security achieved by using mobile devices for authentication depends on the method of determining a user’s location. For instance GPS devices can be tampered with, and depends on the client side environment. Using a cell phone network and checking which antenna a user is connected to would be better, but has low granularity. Signals emitted from a beacon can be spoofed and transmitted to other places.

Some privacy concerns may arise when considering how location is found. Constantly tracking the users would give good precision and security, but would result in poor privacy.

3.5.4 Usability

Location based authentication can be transparent for the user, so when it comes to usability it isn't really an obstacle. However, considering the low degree of usage and support today, one can think that location based authentication processes would be dependent on third party application.

These applications may not integrate well with the devices, and then exclude certain user groups. When using some knowledge that only exists at the location however, there may be some challenges.

3.6 Differences between mobile devices and traditional computers

In this part of the report we would like to focus more on difference between stationary and mobile devices. In the whitepaper by Trend Micro [17] it is described one example how security issues regarding authentication is handled on mobile devices and what risks or challenges are present on mobile devices compared to traditional computers.

Firstly it is suggested that the company network protected by a central firewall is no longer sufficient when mobile devices is used to access business applications. This includes applications such as Customer Relationship Management (CRM) or Enterprise Resource Planning (ERP), which can frequently include sensitive data. Additional security measures must be implemented to provide adequate protection for these kind of applications.

The worst threat can occur if a device is lost or stolen from an employee, sensitive data stored on it might be compromised. Encrypting the data in question or erasing data on the device (remotely or by some other policy) can prevent this problem.

While computers have a known history of dealing with viruses and malware, far less problems have been recorded with mobile devices. However, this might be an increasing problem in the years to come. Maybe the biggest threat for mobile devices can be programs that record keystrokes, passwords or offer unauthorized access to a mobile device.

In addition, if the mobile device's operating system or the services contains flaws, these might be exploited by crackers. They will also be susceptible to Denial of Service attacks, in which the device or service receives more requests than it can handle, thus rendering it unusable as long as the DoS attack lasts.

It is important to note that secure solutions do not consist of purely technical solutions. In addition to technical means such as anti-malware protection, transfer data of secure connections and firewalls, it is additionally required the establishment of clear policies for use of mobile devices, authentication of users and devices for data access.

3.7 Summary

From research that we conducted and summarized in previous part of the paper, we can see that there are many approaches for performing user authentication, both for mobile and stationary devices. We saw that there is no unique solution that is appropriate to every situation. There are numerous factors that must be taken in consideration when selecting authentication method, as for instance: usability, security, specific functionality of the application/service, privacy, user requirements. The biggest challenge is finding the right balance between these factors, and selecting the authentication method that is suitable for the specific service and accepted by the users.

4 Questionnaire

Next logical step in our project was to involve users and found out what are their thoughts on this topic. Our goal was to determine what users expect and tolerate from different mobile and stationary services regarding protection of their personal information. For this purpose we created the questionnaire that we used to find out users' acceptance of different authentication methods described in previous chapter.

4.1 Questionnaire – process description

During our literature search we found couple of articles that are addressing very similar issues, and we used their descriptions of procedures and questions in questionnaire as base for creating our own questionnaire. The papers [18] [19] describe surveys that focus on users needs for security in mobile devices and their acceptance attitudes toward current and possible future alternative methods. We used questionnaire from this research as starting point and we adjusted it to our needs and goals.

During development of the questionnaire, we tried to find the right questions for users, and do not ask more than it is absolutely necessary for our research. Also we tried not to ask any questions that user might experience as privacy violations. Users were not required to respond to all questions, and were able to leave some of them unanswered if he/she wanted.

The questionnaire was distributed to users as hard copies and in online version. The first version of the questionnaire was distributed to other students on the course INF5261 as hard copies. In this first trial our goal was to gain both answers to the questionnaire and also feedback about content of the questionnaire, and detect possible bad formulation and misunderstanding of the questions. There was couple of suggestions for improvements that we received from our classmates that we used to improve questionnaire and create final online version.

For creating the online version of our questionnaire we investigated a couple of different approaches. The first approach was to make questionnaire as HTML page and run it on one of our private servers where we would store results. Other option was to find some online questionnaire tool that will allow us to create a questionnaire and access results that we gathered. We choose other option mostly because of more advanced options for processing of results that would take time for implementing on our own servers. Through Internet search we found couple of solutions that provided us access to full or trial version of their tools. In the end we decided to use the open source tool “Kwik Surveys” (http://www.kwiksurveys.com/) that enable us full access to gathered data and all tool’s functions (e.g. filtering results using different condition that we find very useful during processing of data, printing results, access to each specific user’s response).

We did not want to pose any limitation on respondents for taking part in our questionnaire, but because of time and resource limitation the major part of people that took part in our questionnaire was between 18 and 35 years old. We decided on this because the most mobile users are from this age group regarding research [20]and we hope to get the more valuable feedback from them. Only stipulation was that respondents are current or previous user of mobile handsets.

4.2 Questionnaire description

In the Appendix A we enclose the final version of the questionnaire. Here we will describe questionnaire in more details and explain what we wanted to find out with each question.

Age, gender and education questions are usually starting point in every questionnaire and we included them to see if and how respondent’s responses vary for different user groups.

With questions about factors that influence choice of network operator and mobile handsets, we wanted to find out how aware users are about security issues and with what they relate security.

Questions about current and future usages of mobile phones show us how much users are acquainted with their mobile phone capabilities and are they interested in future deployment.

In the next set of questions we ask users about current authentication methods: which are used, in what manner, do they think there is need for higher level of security and would they accept other authentication methods. Through these questions we want to see how they accept different authentication methods and what their impressions are.

Also we added one question that addresses privacy issue, concerning the users´ opinions regarding the storage of his/hers private information on different places (mobile phone, network).

4.3 Questionnaire results

The questionnaire was available for online completion for a period of three weeks and 73 people gave their answers. We tried to promote the questionnaire to our colleagues and fellow students. In next sections we present and discuss results we gathered. For those who are interested, the raw results are enclosed as Appendix B.

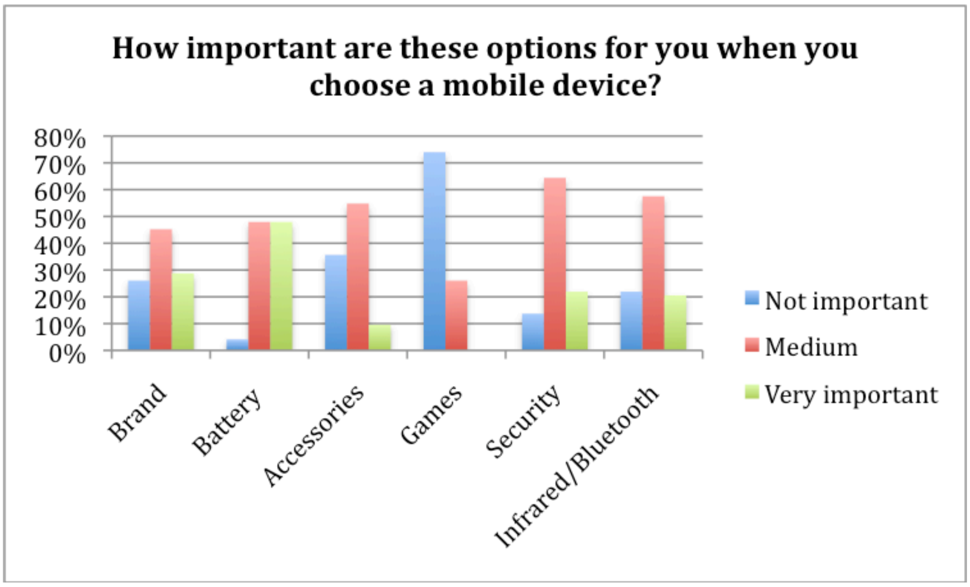
4.3.1 Overall questionnaire results

This part will cover the general results drawn from the questionnaire. Later, we will also highlight some interesting findings when grouping the respondents by gender or age. We choose to group the results by these two factors in order to see if there were any interesting differences. While our main target group; informatics students usually would consist of males, in this survey 66% of the respondents were male, while 34% female. While there is still an overweight of male, we still wish to see if we can draw some interesting results by looking at the different answers filtered by gender.

Age proved more evenly distributed. 51% was in the age category 18-24, while 48% was between 25 and 34, and 1 % above 34. None was younger than 18. These two categories give us a good basis to look at the differences between the age groups, both in usage patterns and views.

We also looked at education level, where 40% had finished high school, 37% had a Bachelor's degree, and 23% held a Master's degree. Since the questionnaire was distributed mainly to other students, we expected high education levels. Though, we have been unable to discern any interesting differences from the education differences, so we will not include a section for this.

When choosing a network operator, most respondents seem to consider price and network coverage most important, with 81% and 62%, respectively. Though, security is still considered medium important by 49% and very important by 33%. So it seems the convenience of price and coverage is most important, security is a part of the considerations. It might also be noteworthy that nearly half (47%) of the respondents do not consider operator loyalty important at all.

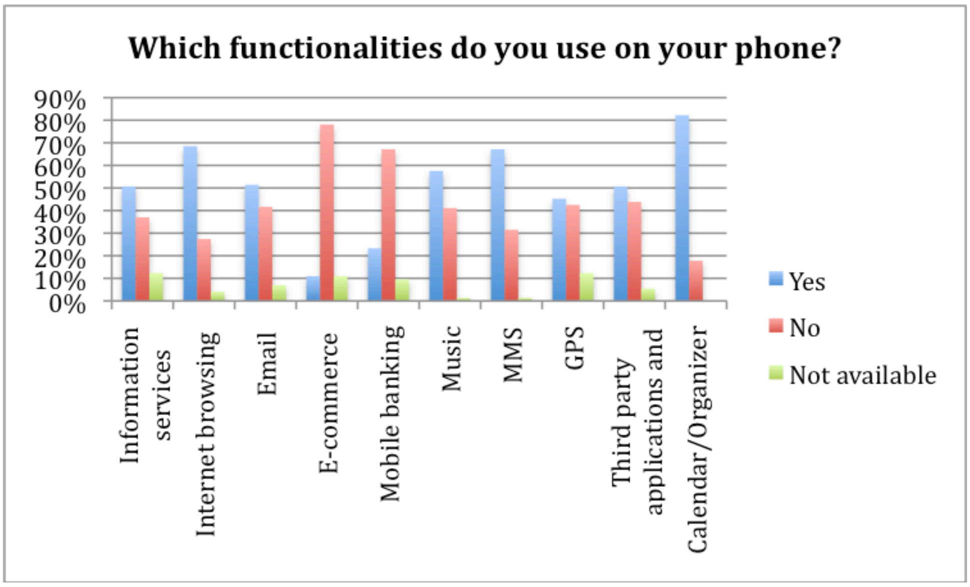


Graph 1 Responses on question "How important are these options for you when you choose a mobile device?"

When choosing a mobile device, it seems the most important aspect is battery, which 48% consider very important and 48% consider medium important. Games are the least important aspect, which 74% consider not important. Security is considered very important by 22% and medium important by 64%. So while less respondents consider security very important for the device, more consider it medium important. This might indicate that while the security of the device is somewhat important to most, some consider it very important that the network operator has necessary security in place.

Also the importance of battery of mobile devices might put constraints on future authentication methods. If the increased security will in turn require more processing (for instance for maintaining encrypted connections) this will affect battery life and might scare potential customers away. On the other hand, as batteries evolve, they might be better fit to deal with heavier computing tasks such as encryption.

Additionally, since price is the main consideration when choosing an operator, the amount of data different authentication methods need to transmit might affect the outcome. Some methods, such as location-based might transfer more data through the network, thus raising the price a user would need to pay. Instead, one might want to focus on lower-cost methods or alternatively look into ways of reducing the amounts of transferred data or look into what can be performed locally without the need to transfer data.

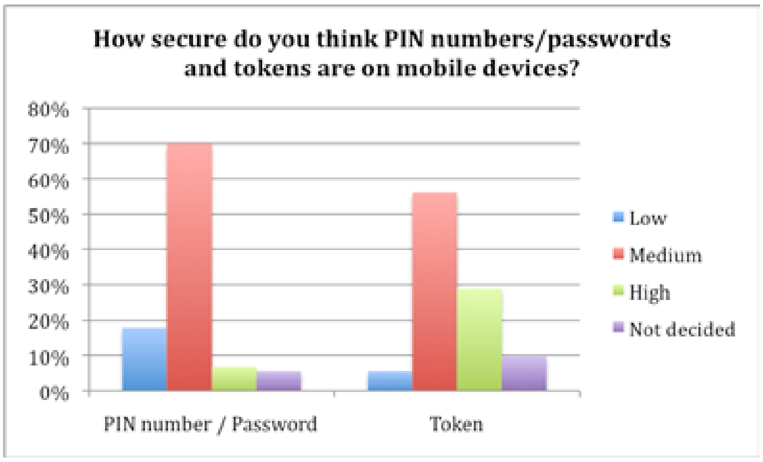


Graph 2. Responses on question "Which functionalities do you use on your phone?"

By looking at what functionalities the respondents use on their phone, we can say something about their usage pattern. From the graph above, we see that while most use their phones for calendar, browsing, mail and multimedia (mms/music), few use it for mobile banking or e-commerce even though only 10% do not have support for this kind of functionality. So while it seems the respondents are active users of their phones and the various functionalities it offers, some areas are less used than others.

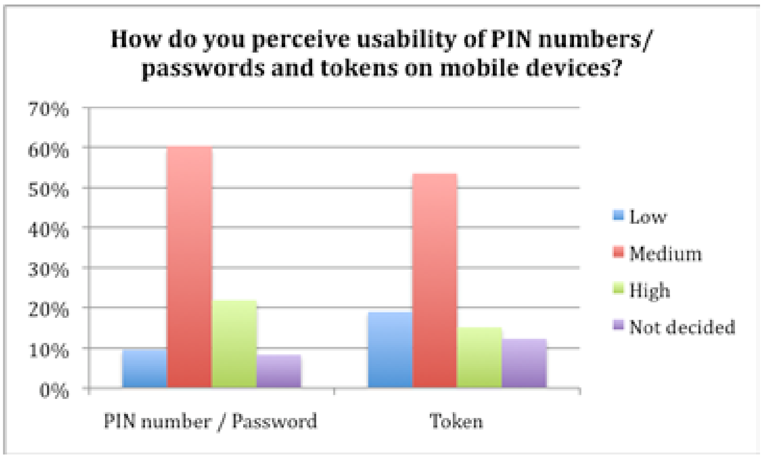
When asked what kind of services the respondents would use in the future, the winner was mobile payment, which 60% would use. Second came video conferencing and video on demand which 41% and 40%, respectively, would use in the future. This seems to indicate the respondents in general are not that much interested in future services, though they do not reject them outright.

Presently, 52% of the respondents access social networking from a mobile device, however only 19% use it for banking. Compared to stationary, the difference between use of social networking and banking is much less, 90% compared to 86%. This is an interesting gap, since it seems to indicate a different usage pattern on mobile devices than stationary. It might also be interesting to see if this gap closes in the future, as mobile services becomes more widespread than they are today. It also seems to indicate the respondents are primarily using services that do not require advanced authentication methods on mobile devices. We do not know if this is because of complicated usage or just because these kinds of services are not that adjusted to mobile device.



Graph 3. Responses on question "How secure do you think PIN numbers/passwords and tokens are on mobile devices?"

When asked to judge the security of passwords and tokens, more respondents view tokens as highly secure (29%) than passwords (7%). Most seem to view passwords as a medium secure solution (70%), while 56% view tokens as medium secure. According to this, the respondents seem to view passwords as medium secure, and tokens slightly more secure.

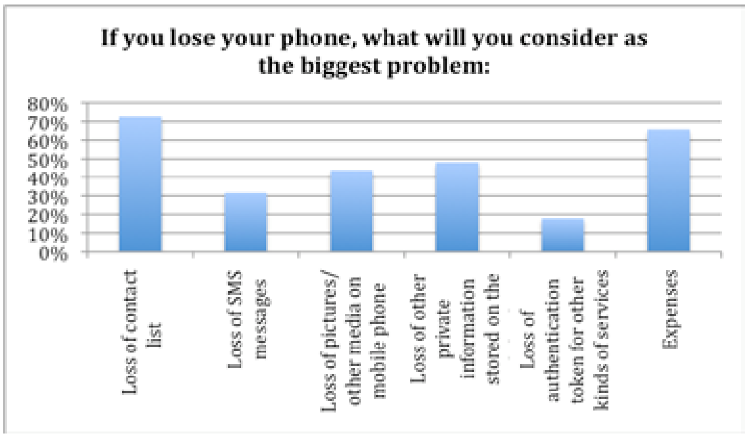


Graph 4. Responses on question "How do you perceive usability of PIN numbers/passwords and tokens on mobile devices?"

The perceived usability, however, goes in the favor of passwords. 22% regards the usability of passwords as high compared to 15% for tokens, though the gap is smaller for medium usability which amounts to 60% for passwords and 53% for tokens. Low usability is reversed, where more respondents considers tokens to have low usability over passwords, 19% versus 10%.

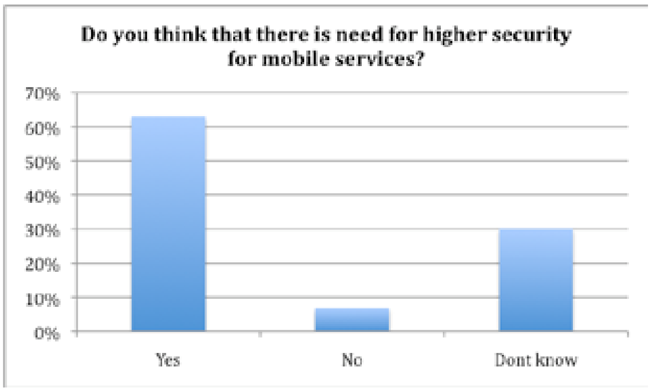
All in all, the respondents view tokens as more secure, though with poorer usability than passwords/PIN codes. This might indicate that while a solution might be seen as more secure, it might also be considered more inconvenient for the user, which is something that might affect the usage pattern and users preferences for authentication methods. However, passwords are the most common form of authentication, and it is likely this is the form the respondents are most familiar with. It is hard to say if the respondents view passwords to have better usability because that is their honest opinion or if it has been shaped by the fact they have been using passwords for a long time.

Nearly half (49%) of the respondents never use the functionality to automatically remember passwords for them. Furthermore, 30% stores the password depending on the service, while 14% do it sometimes. Only 3% claims to always store their login passwords. This might also indicate that the respondents are aware of the problems of storing their passwords on their devices. If the device is lost or stolen other people might get access to the services, since the passwords are stored without any additional protection. It might also indicate that the respondents prefer the security of knowing their password cannot be compromised this way above the convenience of not having to type your password each time. In other words they would rather have a secure solution, than solution with higher usability but less security.



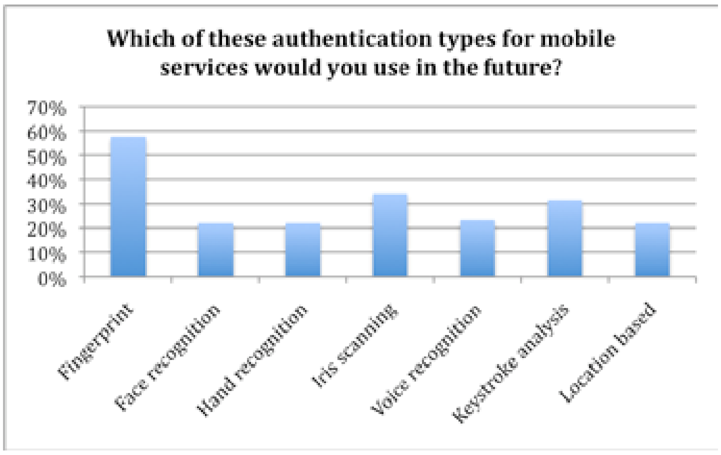
Graph 5. Responses on question "If you lose your phone, what will you consider as the biggest problem:"

If the phone is lost, the respondents rate contact list as the biggest loss, shortly followed by expenses and other private information, pictures and other media, SMS messages and lastly, the loss of authentication tokens. This might provide an overview over what kind of data is stored on the respondent's mobile phone, which includes private information and pictures. While authentication tokens are considered the least serious loss (only 18%), we are unsure of the cause. We have seen earlier that only a minority uses the phones for banking and similar services. Thus, if the respondents do not use their phones as tokens, naturally they do not need to fear the loss of these tokens. An alternative explanation could be that they are not interested in the tokens, but rather more concerned with their private information and contact list.



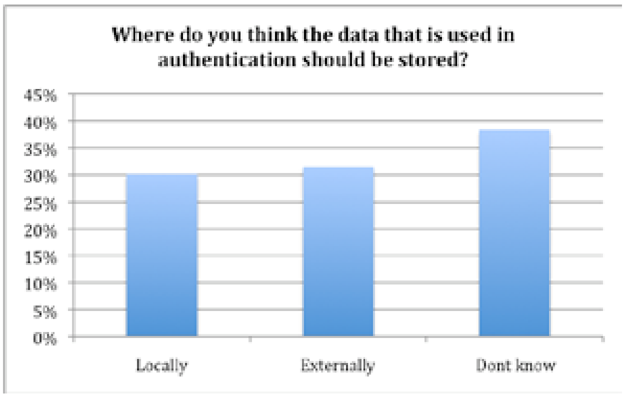
Graph 6. Responses on question "Do you think that there is need for higher security for mobile service?"

The majority of the respondents agree there is a need for higher security for mobile devices (Graph 6). However, we fear the question "Do you think that there is need for higher security for mobile services?" might be a leading question, since improving security would be seen as a good thing. There is also roughly a third (30%) who is unsure.



Graph 7. Responses on question "Which of these authentication types for mobile services would you use in the future?"

Therefore, we found it more interesting to look at what kind of authentication methods on mobile devices the respondents would use in the future (Graph 7). While more than half (58%) are positive to scanning their finger-print, less than half considers any of the other alternatives. Iris scanning takes second place, which 34% would use, followed by keystroke analysis with 32%. We are unsure of the reasons behind this result. It could be that the respondents are not familiar with the solutions and methods such as face recognition, hand recognition and location-based (each with only 22% acceptance). On the other hand, it could be due to privacy issues, since all these methods include revealing a part of you or your location.



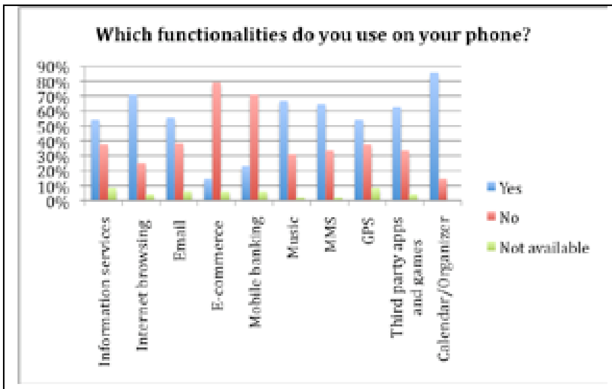
Graph 8. Responses on question "Where do you think the data that is used in authentication should be stored?"

When given the choice between storing the data used in an authentication process locally or externally, most respondents are undecided (Graph 8). For those that have decided, there is a slight preference to externally over locally. One of the main reasons for this question is the privacy issues concerned with storing biometric data. For instance if a finger-print is stored at a central server where everyone has to connect in order to authenticate, all these prints might end up in the wrong hands if the server is compromised. Additionally, some people might object at all to handing over for instance their fingerprint, as they do not know how and to what purposes it will be used beyond the authentication process. When storing such information locally, on the other hand, the individual is much more protected from misuse.

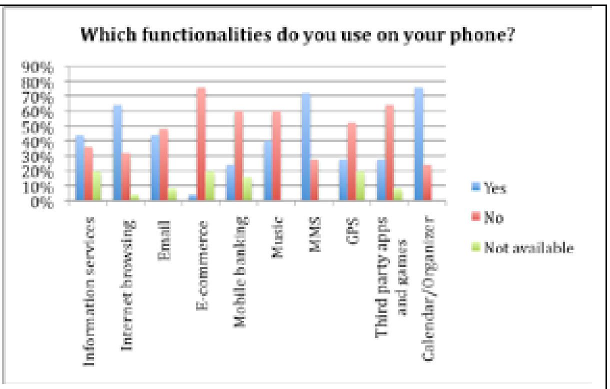
In other cases, such as with passwords, these would perhaps rather be stored externally than locally. As long as the passwords are not stored in clear-text, but hashed for instance, they do not provide a danger if the central server is compromised. What this question perhaps fails to take into consideration is that it might depend on the type of service and the type of data. This might be the reason the majority of the respondents have answered "Don't know", as there is no universal answer.

4.3.2 Results filtered by the gender of the respondents

In this part of the report we will describe some interesting results of questionnaire that vary based on the gender of respondent.



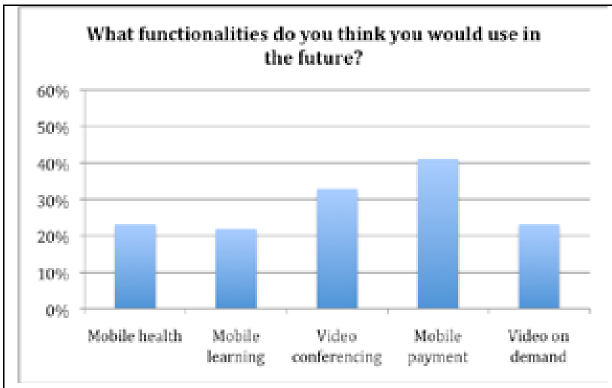
Graph 9. Results - men



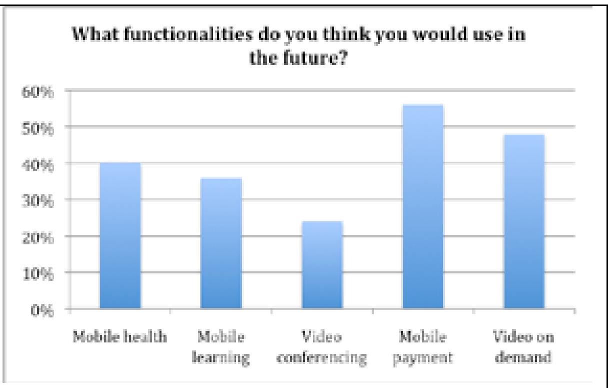
Graph 10. Results - women

Graph 9 and 10. Results on the question "Which functionalities do you use on your phone?" filtered by gender

From the results presented in the Graph 9 and 10 we see that men are using more different functionalities (e.g. Third party applications - 63%, Music - 67%, GPS - 54%) on the mobile phone then women (e.g. Third party applications - 28%, Music - 40% GPS - 28%). These results present just variety of services that are used, not frequency of usage. But we can see that men are more interested in different functionalities, while women are mostly sticking with the basic things.



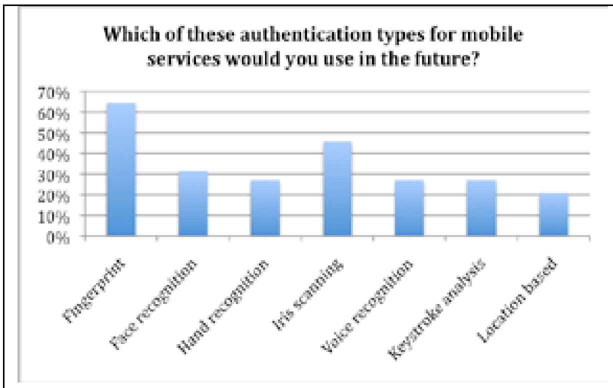
Graph 11Results - men



Graph 12. Results - women

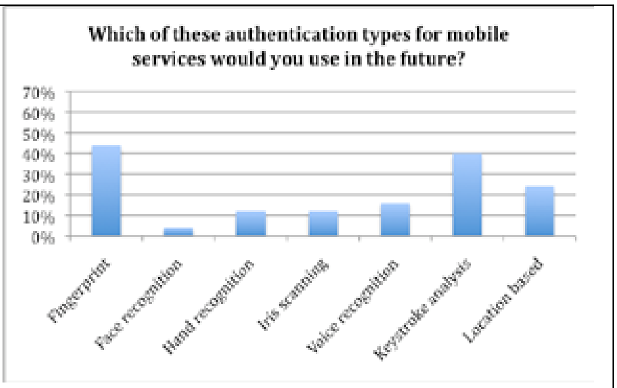
Graph 11 and 12. Results on the question "What functionalities do you think you would use in the future?" filtered by gender

Though on the other hand, in the results of the question "What functionalities do you think you would use in the future?" presented in the Graph 11 and 12 we see that women are actually more interesting in new future services regarding mobile health (men 23%, women 40%) and mobile learning (men 22%, women 36%). Only thing that are men more interested in is video conferencing feature (men 33%, women 24%) that is more related to multimedia functionalities. From this two questions we can see that women are not disinterested in all mobile services, but more attracted to specific services that they find useful and can have some gain from (managing health, learning new things, paying in a store). But men are more interested in trying out more functionalities and using mobile device as entertainment (video conferencing, GPS, third party applications and games).



Graph 13

Results - men

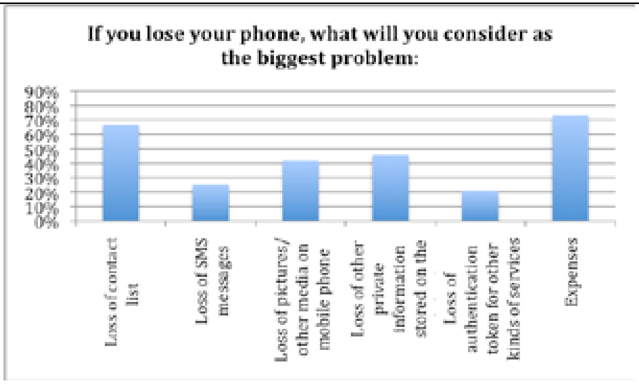


Graph 14

Results - women

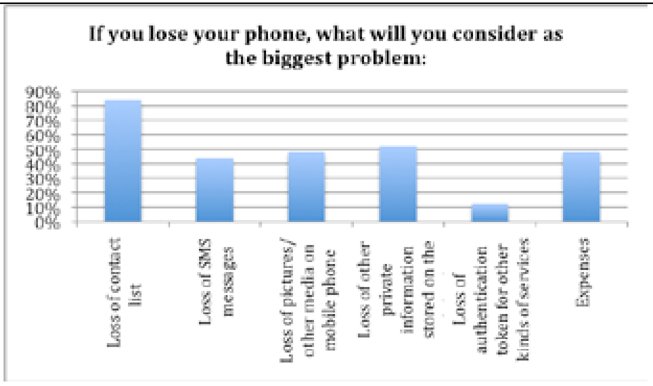
Graph 13 and 14. Results on the question "Which of these authentication types for mobile services would you use in the future?" filtered by gender

One other interesting fact that we noticed is acceptance of advanced authentication services (Graph 13 and 14). While men are much more open to fingerprint (men 65%, women 44%) and iris scanning (men 46%, women 12%), woman prefer more nonintrusive authentication methods as keystroke analysis (men 27%, women 40%) and location based (men 21%, women 24%). From the questionnaire we could not conclude the reason for this, and we think this can be interesting thing for further research.



Graph 15

Results - men



Graph 16

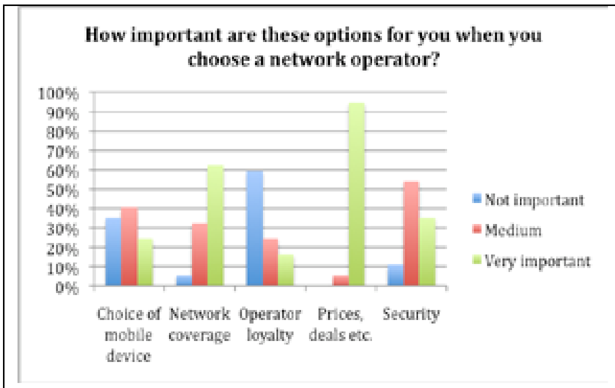
Results - women

Graph 15 and 16. Results on the question "If you lose your phone, what will you consider as the biggest problem?" filtered by gender

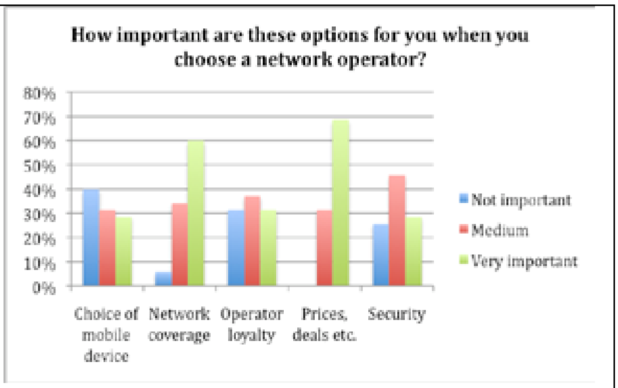
We also noticed the differences in what is considered as most valuable information on the mobile device (Graph 15 and 16). While women sees contact lists, SMS messages and pictures as very important information men are more worried about higher costs due to the misuse of the phone if the phone is lost then disadvantage of losing private information. Through interviews with users we tried to discover the reasons behind some of these differences.

4.3.3 Results filtered by the age of the respondents

Next we wanted to see if there are user's opinions and preferences that vary based on age of participant. Initially we formulated question regarding age to group respondents in four age groups: bellow 18, between 18 and 24, between 25 and 34 and above 34. The main reason for making these specific groups is that in the research□14□the mobile device users are grouped in that manner and each group are given specific characteristics and names ("the cellular generation", "transitionary" and "adult adopters"). But because we did not have any respondents bellow 18 and just one above 34, this filtering is done only on two middle age group that are probably the most frequent users of mobile devices (leaving out respondents not fitting in these two groups).



Graph 17Results – age group 18-24

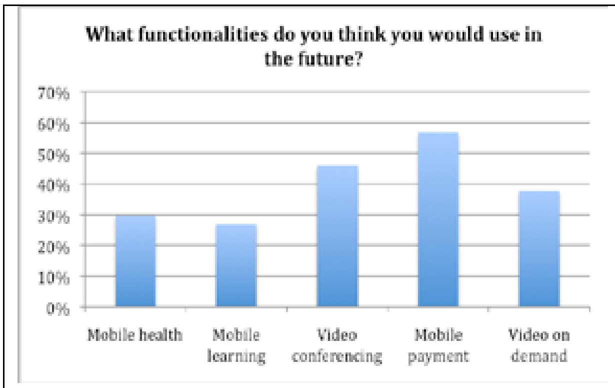


Graph 18

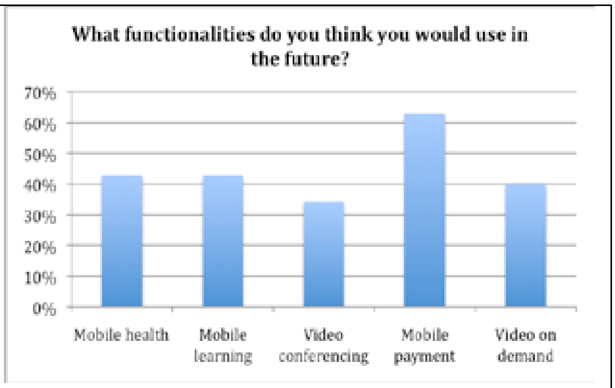
Results – age group 25-34

Graph 17 and 18. Results on the question "How important are these options for you when you choose a network operator?" filtered by age

We noticed differences regarding preferences when choosing network operator (Graph 17 and 18). We see that younger respondents take more care of prices (95% younger respondents answer very important while 69% of older respondents answer very important) and they do not think a lot about loyalty to operator (59% of younger respondents answer not important while 31% of older respondents answer not important). This is very logical, because younger people are usually studying and do not have fixed income. Also they usually use some standard contracts with operators with no extra functionalities so changing operator is not that problematic for them. One other thing that we noticed is that younger respondents are more concerned about security (younger respondent: 54% medium and 35% very important while older respondents: 46% medium and 29% very important). This result is may be influenced by the type of people that responded to our questionnaire (where younger respondents are mostly finishing informatics studies) but we thought it was worth mentioning.



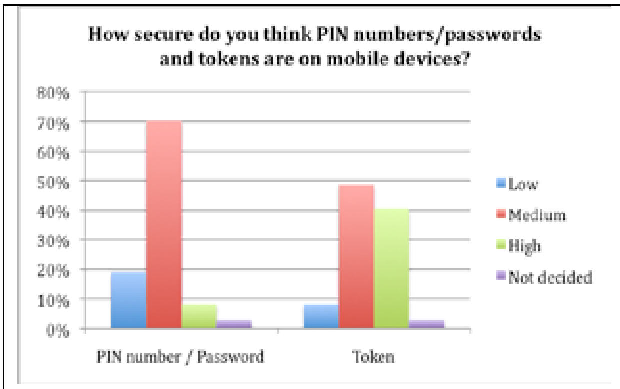
Graph 19Results – age group 18-24



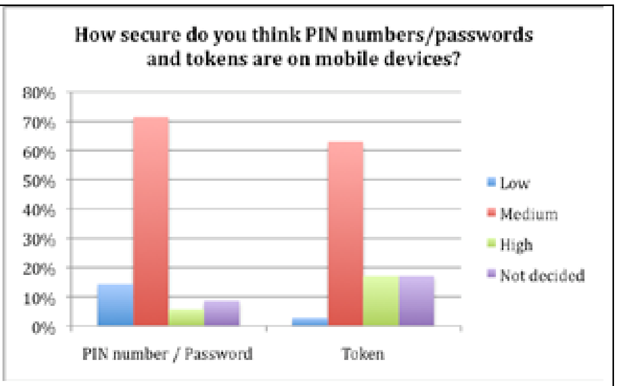
Graph 20Results – age group 25-34

Graph 19 and 20. Results on the question "What functionalities do you think you would use in the future?" filtered by the age

When talking about what respondents from different age group think about future services (Graph 19 and 20), we can notice that respondents from older age group are more interested for majority of future services (Mobile health: younger 30%, older 43%; Mobile learning: younger 27%, older 43%; Mobile payment: younger 57%, older 63%; Video on demand: younger 38%, older 40%), except for video conferencing services (younger 46%, older 34%) which younger respondents prefer more. These results match some general perception of mobile device usage where younger people use mobile phone more for entertainment while older use those more for some advanced functionalities and work.



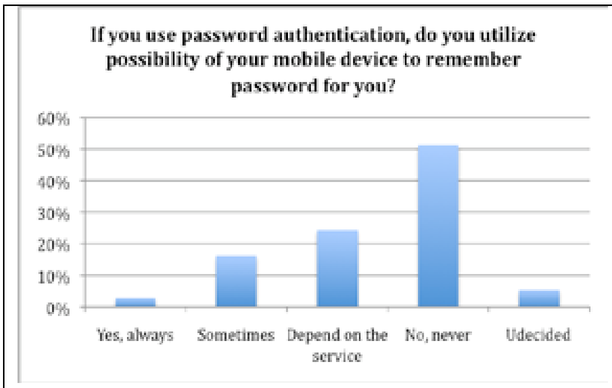
Graph 21Results – age group 18-24



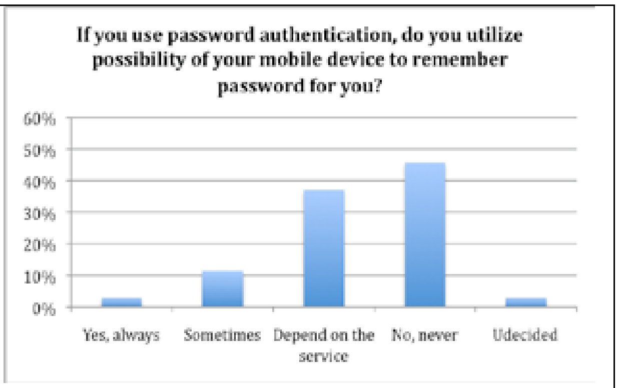
Graph 22Results – age group 25-34

Graph 21 and 22. Results on the question "How secure do you think PIN numbers/passwords and tokens are on mobile devices?" filtered by the age

One other thing we noticed is that security of token-based authentication is perceived little differently by these two groups of respondents (Graph 21 and 22). While passwords and PIN numbers are seen to provide medium level of security by both groups (younger: medium 70%, older: medium 71%), there is some difference with tokens. We saw that younger respondents actually perceive tokens as more secure than respondents from older group (younger: medium 49%, high 41%; older: medium 63%, high 17%). The reason can be that younger people are more acquainted with new technologies and understand security issues in more details.



Graph 23Results – age group 18-24



Graph 24Results – age group 25-34

Graph 23 and 24. Results on the question "If you use password authentication, do you utilize possibility of your mobile device to remember password for you?" filtered by the age

We also saw that these two groups of respondents have slightly different approach regarding storing passwords on the mobile device. From the Graph 23 and 24 we see that respondents from older group more frequently decide to save password on mobile device dependent on the type of the service (younger: 24%; older: 37%). We can say that the probable reason for that is the number of passwords that is accumulated over the time, and then one more likely decide to store password for the services that do not contain highly private information. But still this difference is not that big, and still majority of respondents prefer not to save passwords on the mobile device in both age groups.

From the previous discussion we saw that younger people are using mobile devices more for entertainment and do not think that other more advanced services will be useful. But at the same time they are more concerned about security and they are better acquainted with advanced authentication methods.

5 Interviews

When we were done with the questionnaires, there were some "why" questions and unclarities that we wanted to find out some more about.

We set up a simple prototype (http://folk.uio.no/oyvinbak/auth) where the users could try to interact with a couple authentication methods. We chose password, token, fingerprint and location as options. The prototype was designed so that we could easily make different combinations and test them out on the users. We made various combinations of two and three factor authentication to illustrate the process of authentication to the users.

For the testing purpose we made five different combinations; one with username and password, one with username, password and token and one with fingerprint and password.

5.1 Interview description

1. **Background questions** - General questions regarding demographics
2. **Usefulness of the services on mobile phone -** In the questionnaire people had clear preferences of what they would use and not. What are the main reasons for this and is it related to perceived security? Are there other reasons?
3. **Try out different authentication -** Experiment with using different authentication methods, get familiar with them.
4. **Questions regarding the authentication methods -** Mapping between authentication methods and services. What methods does a user see as appropriate for the different services? Why/why not?
5. **Where do you think the data (password, biometrical data) that is used in authentication should be stored? -** Many participants in the questionnaire had opinions about this, what is their foundation?
6. **If you use passwords, do you store the passwords on devices? (stationary/mobile device)**
7. **Do you use mobile phone as authentication token for services? Do you know what a token is?**

With these goals to be answered, we set out to interview some subjects.

Midway we also added some questions regarding loss of phone and operator loyalty, as there appeared some results we didn't understand from questionnaires.

5.2 Carrying out the interview

In practice it was a bit difficult to keep to the original structure, point 3 and 4 merged sort of naturally together. While reviewing the questionnaire we also added some questions to the interviews underway. In general we picked up semi random people near our workstations, and interviewed them for duration of 20-30 minutes.

5.3 Results

We interviewed five women and three men. Four of the subjects were in the age span between 18 and 24, one was 25, and two were 29. Four of the subjects were students at the university, three working. The subjects experience with mobile devices spanned from novice (uses primary a phone to message and call other people) to experienced (also play around with technical aspects).
Cell phones are by far the most common mobile device in Norway, so we focused on them in the interviews. Three of the users had smart phones, such as iphones and androids, and the rest had "normal" phones.

5.3.1 Usefulness

In general the main limitations on what services the subjects used were based on usability and good overview of the content. Mobile phones have smaller displays than stationary machines, so more sophisticated applications such as banking, altinn/minside and facebook were perceived as less usable.
All the subjects used **social mediums** such as Facebook or similar. Only one used facebook regularly on the phone, one used it if no stationary device was available and the rest didn't use it. Reasons given for not using mobile services were because the same service was available on a stationary device that provides better overview of the content and better usability.

None of the subjects used **mobile banking** regularly. One checked balance by sms, and one used mobile banking in the past, but no longer. Reasons given were that stationary devices were more practical, and gave a better overview for these types of applications. Two subjects also perceived mobile devices as less secure than stationary.
E-commerce was the best received potential service, and three of the subjects saw use of this in their everyday life. Two of the subjects were skeptical, quoting "too many eggs in one basket". They like having important tokens/services spread like they have now (one credit card, one bus ticket, one mobile device). One of the subjects could see herself/himself using this if it was a part of a job or if the availability was good enough.

Mobile learning tools were perceived as somewhat interesting, but the options today are limited. General services such as podcasts of lectures could be interesting, but the subjects saw little use for accessing more sensitive information (such as grades or feedback) through mobile devices. **Government applications** (altinn/minid) were not very interesting because for using it one need good overview of content on a screen and these types of services were usually quite complex to be handled on the mobile device.

5.3.2 Authentication methods

5.3.2.1 Passwords

Passwords are the most popular authentication methods, and all the subjects used them for multiple services. Authentication with this method is very straight forward and people perceived it as "secure enough". Subjects were conscious about the length of their password and security. On the other side looking from the negative point of view this leads to multiple passwords and it gets hard to remember.

The usability perceptions were consistent with the questionnaire results where people think passwords are acceptable method of authentication. When asked if they would consider using weaker passwords on services for mobile devices, which may have limited input capabilities (for instance a small keypad), most of respondents wouldn't sacrifice security for usability by having a shorter password.

5.3.2.2 Tokens

All the subjects used tokens in some form, either through paper tabels (for altinn), key generators (for BankID) or through SMS (altinn, skandiabanken). The subjects perceived tokens as secure and with high usability. Two subjects were skeptical regarding token generators integrated in phones because of grouping too many services into one device.

5.3.2.3 Location

The subjects were positive to the usability aspect, as location tracking happens without user input. However some expressed concerns about privacy issues, and it is perceived a bit too complicated at this stage. Maybe if the subjects were more familiar with this technology we could go more in depth with this discussion.

5.3.2.4 Biometrics

Most of the subjects liked the aspect of quick login, but are conscious about the risk of data loss. Data loss is perceived bad because it contain sensitive information about themselves, not necessarily because of practical issues such as the fact that one is unable to change biometric factors, but a general impression of that loosing private data is bad and should be avoided. Face recognition was also considered as more negative because of giving away too much information about one self.

Fingerprint is still the one most preferred biometrical method, as it was in the questionnaire results. Some users have experience with it, although these ranged from very positive to poor, as result of the methods functionality. All the subjects had some ideas of fingerprint, and other than privacy issues they were generally positive.

5.3.3 Mapping versus services

Most of the subjects had some opinions about the mapping between different services and authentication methods. Here is a summary.

5.3.3.1 Facebook/Social services

Most of the subjects considered facebook as a low value service. Convenience and ease of use were major factors for their continued usage. If facebook applied more (advanced) security measures, many of the subjects would consider stop using it. Trust issues regarding storage biometrical is one argument, others indicated that they didn't see any reason for facebook to use that kind of data for authentication. Tokens are considered too time consuming for this kind of service, as one want easy access everywhere independently of token generators. Password authentication for this service and similar ones were considered as secure enough.

5.3.3.2 Banking and MinId/Altinn

People considered banking services and government services as about equally valued services. Some indicated that banking/bankid were more valuable as one uses it more often. Anyway, the differences between them indicated in the interviews were minor, so we summarize them as one group. The general opinion is that banks and altinn are more serious service providers. One argument was they are bound by Norwegian law, which is quite strict when it comes to personal data. Another is that there is a more formal agreement between the users and banks or government services.

Combination of passwords, tokens or fingerprint were preferred authentication methods for this kind of services.

5.3.4 Data storage

Most of the subjects prefer external saving, of fear of losing their own device.

5.3.5 Network operator security

Not many of the subjects actually used sensitive services such as banking for instance regularly on phones, so they hadn't really thought too deeply about it. Most of the subjects were consciousness about using secure or unsecure wireless networks. Also most of them tried to limit use of banking applications for home networks, either never using it for unknown unsecure networks or only when there were no other options. Some were aware of options such as virtual private networks (vpn), but didn't really use it even though they expressed some desire to.

5.3.6 Password storage

On stationary machines all except one of the subjects store some passwords. Some save all passwords (but only on their home computer), others grouped their passwords according to the importance of the related service and only stored the less important ones. The subjects had from two to five different sets of passwords, with different uses and importance. Two of the subjects tried to avoid storing the password on the device if that was achievable.

5.3.7 Mobile phone as authentication factor

The views were splitted on whether integrating token generators in mobile phones were a good thing or not. Both sides focused on that your phone then will do everything, it takes less space than walking around with several devices, but if you loose it you are out of luck.

5.3.8 Review

While reviewing the questionnaire, we noticed that many women consider loosing sms messages on the phone is worse than the loosing numbers or the related expenses, so we decided to add this to the interviews to see what a reason behind this is. We also added a part about operator loyalty, to find out if there are any other factors than price that makes customers loyal.

5.3.8.1 Loss of phone

Women often considered loss of text messages as a greater loss than number lists or expenses, and we found this a bit interesting. What do they keep in their messages? We therefore added this to the interviews.We found out that those who considered messages more important did so because they use messages as notes to remember events and other things.

5.3.8.2 Operator loyalty

What are the main reasons of why people are loyal to their mobile operator? Is it connected to security and authentication?
Three of the subjects had had their subscription for more than three years. The main reason for keeping the subscription were that it was the cheapest for their use, and some used additional services such as "fri familie" ("free family" - one can call a group of people for free) and similar. Two of the subjects did not think about the security when choosing the operator, the coverage and availability was more important.

5.4 Thought for improvement and further research

Working with user interviews is often a complex task. When creating the questions a lot of different factors plays an important role; how the questions are formulated, will all the interview objects understand what we are actually trying to ask, how do we avoid to asking leading questions. Designing by concept "everything for all" was definitely something we were not struggling after, but we wanted to make the interview consistent and pretty easy to understand for a user that is not familiar with this field. We tried also to explain the terms as far as this was achievable, but not leading them in any direction.

Eight interview objects are somewhat a small number for giving a representative result when it comes to subject we are writing about, but at least we got some thoughts and feedbacks on what do people use and what they do not use. But combining this with our questionnaire we could draw a much more nuanced overall picture about the situation today regarding authentication on mobile and stationary devices.

6 Discussion

In discussion part of report we tried to make conclusions and respond to the research questions set on the beginning of the report based on results described previously.

6.1 What are most common and accepted authentication methods for mobile services?

Our findings show that the most common authentication method for mobile services is passwords and PIN numbers. Since passwords are also the most commonly used method on traditional computer stations, it might explain high acceptance on mobile devices.

The reasons for this method's popularity may be its medium to high usability, familiarity from the users, familiarity for service providers (as a time tested method), technical simplicity and so on. Passwords have been around since before the computer age, and have been used for authentication on computers for quite some time. A question that can be raised is whether the high usability comes from users experience alone. Biometric based authentication methods such as fingerprint for instance should in theory only require a swipe by your finger and should therefore be more user friendly, but these methods doesn't score too high, partly for other reasons. The training the users have received through years of practice may be essential for successful introduction of authentication methods.

Tokens are also a time tested method that has been ported to the digital world. In general this is an authentication method that users associate with services of higher importance, as it primarily is used for banking and government services. Many users perceive it as a less mobile solution, as they have a key code generator device that may be kept home or get lost, but integration of token with cell phones may help for this issue and this is the area in which much of research is done now. Integrating mobile service terminal and security token into one device can provide in the same time higher usability and security level for mobile services, and on that manner utilize advantages of mobile devices over stationary. Our impression is that this kind of authentication has more potential for mobile devices, and it will probably be used more frequent in the future.

In addition to passwords, services like e-banking and public services use some form of a token in their authentication process. This can be a SMS-message sent to your phone, or something like a certificate that is stored on the phone, depending on the service.

Why do other methods fall short? Biometrics and location based authentication are authentication methods that have been around for some time, but haven't been used to a large degree. Our interviews suggested that people are skeptical to these because of the possibility of losing personal data. Also additional hardware and software must be developed and improved and in the same time made widely available on the mobile devices for people to start accepting them as general solution without skepticism.

6.2 How do people accept them and what are their opinions regarding security on mobile device?

Looking from a general point of view users are satisfied with current authentication methods like passwords and tokens, and they trust service provider to ensure enough level of security. The overall impression is that users actually do not pay much attention to security when choosing an operator and/or purchasing a mobile device. Rather they are more worried about their private data, and how it is stored and used by different mobile services. So while they might assume a certain level of security from the operator side by default, they try to use the services and their data in a responsible way. Mobile services in general are not highly accepted and users think that there is need for higher level of security for mobile services.

When looking at the token as an authentication method it is often perceived as "too much" to take care about, but is in general perceived as high level of security and also widely used.

We see that the most wide-spread solutions are very light on battery life and do not require much processing. Given that battery life is such an important issue when a person considers purchasing a mobile phone, this might have helped the methods gain popularity since battery-power is not used too much. Some newer methods such as biometric solutions will require more processing power, and might not be as welcomed compared to low-cost alternatives.

Biometric solutions, such as finger-print scanning are more accepted than face recognition, and most users would use fingerprint method. However at the present moment, it is still not a wide-spread solution, though some phones support finger-print scanning. So while people are generally positive to using this method, few implementations exist. Most other biometric solutions are for the most part confined to research stage at the moment and are not in common use.

Location-based authentication is another solution which is not as wide-spread at the present moment. However, as more and more devices support GPS, the use of this method might increase in the future.

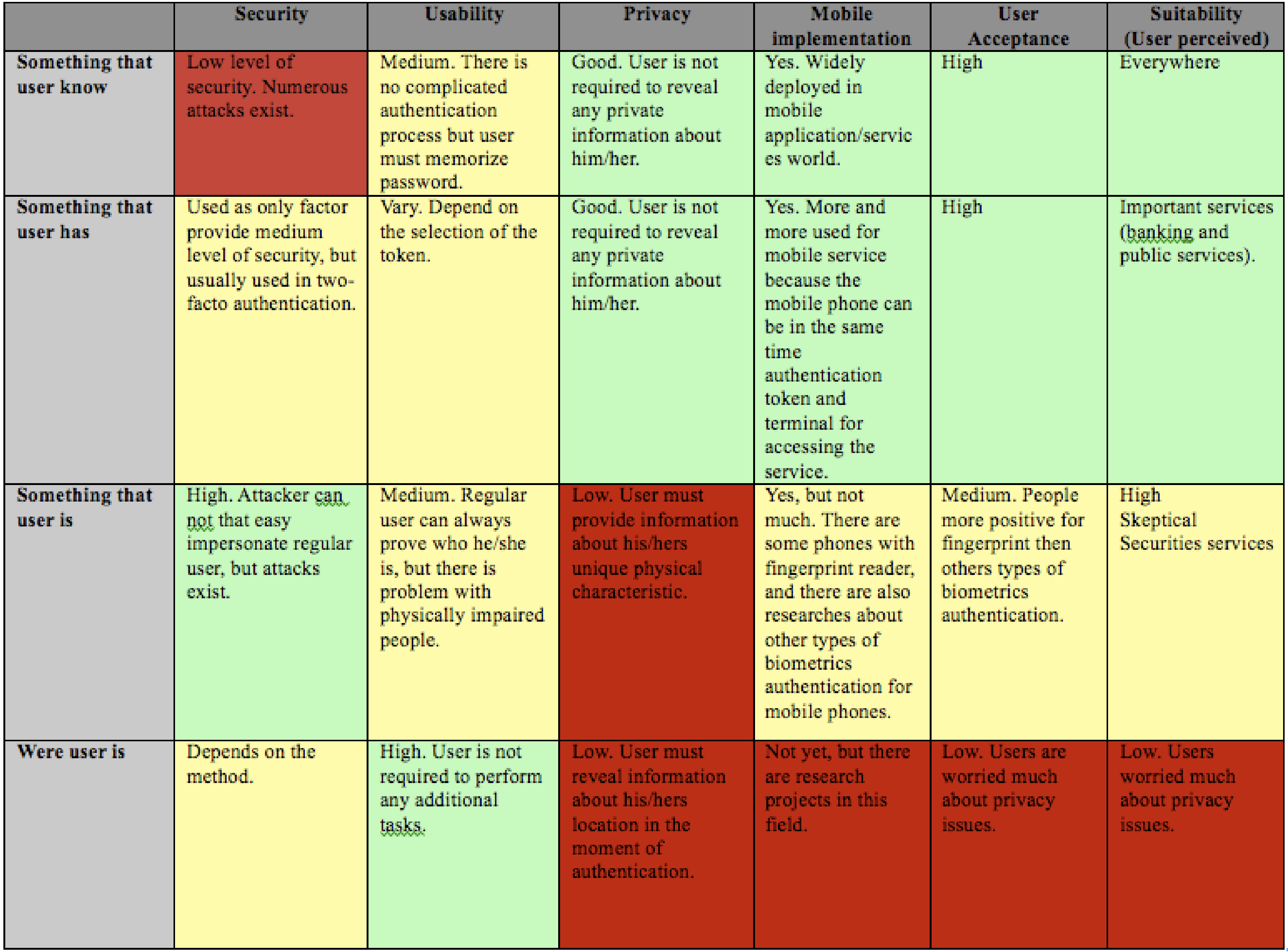
Additional remark that can be seen from the questionnaire is that there are some different opinions and acceptance of authentication methods for different groups of people (we tried to identify differences between age and gender groups). This shows that when talking about user acceptance it is always important to have in mind user group to which mobile service is attended so it can be adjusted to their specific needs and requirements.

6.3 What are differences, opportunities and challenges concerning user authentication for mobile services compared with traditional stationary computers?

The main differences between mobile and stationary devices when it comes to authentication are due to different usage, requirements and limitations. Mobile devices are designed to be very simple and easy to use and available all the time, while stationary devices are more suitable for performing more complicated tasks and usage only on one place. This is a difference that one can say is fading because of platforms that position themselves in the middle, such as tablets, ipads and similar, but in general there is a distinction between this devices and we have seen the different usages in our questionnaire and interviews. Our interviews suggested that people tend to prefer stationary devices for applications that they perceive more complex and require better view of content.

Portability of the mobile devices can open doors for new utilization of services as mobile trading or banking (on the run). Additionally portability characteristics that are not available on the stationary devices can be utilized for implementing authentication methods in more effective manners (e.g. user is almost all the time in the position of the mobile device that can in the same time be the security token, information about user location is available all the time and can be used in authentication process).

The challenges when it comes to mobile services are the limitations of the devices. Even though they may be more powerful than stationary computers were a couple years ago, the requirements from software and users are still very high. Limitations for the mobile platform as computational limitations, display limitations (mostly relevant for mobile phones), storage capability or battery (as mentioned earlier in the discussion) can provide additional problems when implementing certain authentication methods on mobile device.



	Security	Usability	Privacy	Mobile implementation	User Acceptance	Suitability (User perceived)
Something that user know	Low level of security. Numerous attacks exist.	Medium. There is no complicated authentication process but user must memorize password.	Good. User is not required to reveal any private information about him/her.	Yes. Widely deployed in mobile application/servic es world.	High	Everywhere
Something that user has	Used as only factor provide medium level of security, but usually used in two-facto authentication.	Vary. Depend on the selection of the token.	Good. User is not required to reveal any private information about him/her.	Yes. More and more used for mobile service because the mobile phone can be in the same time authentication token and terminal for accessing the service.	High	Important services (banking and public services).
Something that user is	High. Attacker can not that easy impersonate regular user, but attacks exist.	Medium. Regular user can always prove who he/she is, but there is problem with physically impaired people.	Low. User must provide information about his/hers unique physical characteristic.	Yes, but not much. There are some phones with fingerprint reader, and there are also researches about other types of biometrics authentication for mobile phones.	Medium. People more positive for fingerprint then others types of biometrics authentication.	High Skeptical Securities services
Were user is	Depends on the method.	High. User is not required to perform any additional tasks.	Low. User must reveal information about his/hers location in the moment of authentication.	Not yet, but there are research projects in this field.	Low. Users are worried much about privacy issues.	Low. Users worried much about privacy issues.

Table 1 Characteristics of different authentication methods

Also, since you might carry a mobile device with you at all times it might be more in danger of being lost or stolen. In such a case, the data stored on the device would be lost as well. While this threat also affects the stationary platform, mobile devices might be more vulnerable.

6.4 Evaluation of a security / usability / privacy trade offs for different authentication mechanisms

In the table 1 we can see the strongest and the weakest points for each approach. Making this table made us to better understand the general situation and make comparisons between different methods. For content of the table we used results that we discussed previously, so we will not discuss the content of this table in details. Our main conclusion for this more graphical presentation of our results is that each of authentication methods has advantages and disadvantages, and that there is no universal solution that is suitable for every service. The main task when choosing the authentication method is to understand these advantages and disadvantages and find the one method that is most suitable for your specific service.

7 Concluding remarks

When we started this project we saw that there is much potential for mobile services today and in the future and we identified security as main issue that can greatly affect their development and deployment. Because of that in our project we decided to research more in depth different authentication methods and their suitability for mobile services.

During our research we identified main authentication methods that are used today both for mobile and stationary devices and their main characteristics. Beside their general theoretical characteristics that we found in documentation we additionally tried to see what people think about them, how they accept them and do they think they are suitable for current and future services.

Our main conclusion based on previous work is that there are many approaches for user authentication for mobile devices now, but only couple of them are really accepted and in everyday usage. Also we see some potential to other types of authentication (e.g. biometrics), but still the main obstacles are limited capabilities of mobile devices and users perception of the methods.

8 References

1. *Authentication.* 2007 [cited 2010. 02.06]; Available from: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211621,00.html.
2. Council, F.F.I.E., *Authentication in an electronic banking enviroment.* 2005.
3. Bordea, D.d., *Selecting a two-factor authentication system.* Network Security, 2007. **2007**(7): p. 17-20.
4. *Computer security reference book*. ed. K.M. Jackson, J. Hruska, and B.P. Donn. 1992, CRC Press, Inc. 949.
5. *Comparing PhoneFactor to Other SMS Authentication Solutions.* [cited 2010. 04.20]; Available from: http://www.phonefactor.com/sms-authentication.
6. Boudriga, N., *Security Of Mobile Communications*. 2009: Auerbach Publications.
7. Fang, L., M.K.H. Leung, and C.S. Chian, *Making Palm Print Matching Mobile.* International Journal of Computer Science and Information Security (IJCSIS), 2009. **Vol. 6**: p. 001-009.
8. *Cellphones / PDAs / GPS / Portables / Assistants personels / GPS.* [cited 2010. 02.08]; Available from: http://pagesperso-orange.fr/fingerchip/biometrics/types/fingerprint_products_pdaphones.htm.
9. NGT. *CScout Exclusive: Mobile Vein Authentication.* 2009 [cited 2010. 02.16]; Available from: http://www.mobilebehavior.com/tag/authentication/.
10. *BioWallet Signature.* [cited 2010. 02.08]; Available from: http://www.mobbeel.com/en/mobbeel/Products/biowallet.html.
11. Veum, H. and A. Flesland. *Biometri - fordeler og ulempe.* 2007 [cited 2010. 02.24]; Available from: http://www.datatilsynet.no/templates/article____1729.aspx.
12. Leyden, J. *Gummi bears defeat fingerprint sensors.* 2002 [cited 2010. 04.18]; Available from: http://www.theregister.co.uk/2002/05/16/gummi_bears_defeat_fingerprint_sensors/.
13. *The use of biometrics in schools.* [cited 2010. 04.28]; Available from: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/fingerprinting_final_view_v1.11.pdf.
14. Harmel, K. *Walt Disney World: The Government's Tomorrowland?* 2006 [cited 2010. 02.17]; Available from: http://newsinitiative.org/story/2006/09/01/walt_disney_world_the_governments.
15. Vinson, J. *Cracking your Fingers*. Feature Articles 2009 [cited 2010 03.08]; Available from: http://thedailywtf.com/Articles/Cracking-your-Fingers.aspx.
16. Ashfield, J., D. Shroyer, and D. Brown. *Patent Application Publication.* 2008 [cited 2010. 02.07]; Available from: http://www.freepatentsonline.com/20100022254.pdf.
17. *Enterprise Mobile Security Protecting Mobile Data and Increasing Productivity*. 2007 [cited 2010. 02.03]; Available from: http://emea.trendmicro.com/imperia/md/content/us/pdf/products/enterprise/mobilesecurity/wp03_tmms_071212us.pdf.

18. Clarkea, N.L., et al., *Acceptance of Subscriber Authentication Methods For Mobile Telephony Devices.* Computers & Security, 2002. **21**(3): p. 220-228.

19. Furnell, N.L.C.a.S.M., *Authentication on users on mobile telephones – A survey of attitudes and practices.* Computers & Security, 2005. **24**(7): p. 519-527.

20. *Consumers in the 18-to-24 Age Segment View Cell Phones as Multi-Functional Accessories; Crave Advanced Features and Personalization Options.* 2007 [cited 2010. 03.06]; Available from: http://www.comscore.com/Press_Events/Press_Releases/2007/01/Cell_Phones_and_18-24_Year_Olds.

9 Appendix A (Questionnaire)

Questionnaire - Authentication methods for mobile devices

1. Age

   □ Below 18 □ 18-24 □ 25-34 □ Above 34

2. Gender

   □ Male □ Female

3 Highest achieved education level:

□ Grade school

□ High school

□ Bachelor degree/ Diploma

□ Master degree and above

4 How important are these options for you when you choose a network operator?

	Not important	Medium	Very important
Choice of mobile device	□	□	□
Network coverage	□	□	□
Operator loyalty	□	□	□
Prices, deals etc.	□	□	□
Security	□	□	□

5 How important are these options for you when you choose a mobile device?

	Not important	Medium	Very important
Brand	□	□	□
Battery	□	□	□
Accessories	□	□	□
Games	□	□	□

Security	□	□	□
Infrared/Bluetooth	□	□	□

6 Which functionalities do you use on your phone?

	Yes	No	Not available
Information services (e.g. radar control, offers)	□	□	□
Internet browsing	□	□	□
Email	□	□	□
E-commerce	□	□	□
Mobile banking	□	□	□
Music	□	□	□
MMS	□	□	□
GPS	□	□	□
Third party applications and games	□	□	□
Calendar/Organizer	□	□	□

7 What functionalities do you think you would use in the future?

- □ Mobile health (e.g. access to healthcare record, communication with healthcare provider)
- □ Mobile learning (e.g. online learning for mobile phones)
- □ Video conferencing
- □ Mobile payment (e.g. purchasing things in shops, transfer of funds)
- □ Video on demand

8 Which services do you use today on mobile and/or stationary devices?

	Social networks	Subscription	Banking	MinID
	facebook myspace.com LinkedIn	YouTube flickr Spotify last.fm	BankID skandiabanken	MinID minside altinn Skatteetaten Lånekassen
Mobil	□	□	□	□

Stationary	□	□	□	□

9 How secure do you think PIN numbers/passwords and tokens (One Time Password generators, password cards, SMS) are on mobile devices?

	Low	Medium	High
PIN number/Password	□	□	□
Token	□	□	□

10 How do you perceive usability of PIN numbers/passwords and tokens on mobile devices?

	Low	Medium	High
PIN number/Password	□	□	□
Token	□	□	□

11 If you use password authentication, do you utilize possibility of your mobile device to remember password for you?

□ Yes, always □ Sometimes □ Depend on the service □ No, never

12 If you lose your phone, what will you consider as the biggest problem:

□ Loss of contact list

□ Loss of SMS messages

□ Loss of pictures/other media on mobile phone

□ Loss of other private information stored on the mobile phone

□ Loss of authentication token for other kinds of services

□ Expenses (higher bill due to misuse, buying new phone)

13 Do you think that there is need for higher security for mobile services?

□ Yes □ No □ Don’t know

14 Which of these authentication types for mobile services would you use in the future?

□ Fingerprint

□ Face recognition

□ Hand recognition (scanning your hand shape)

□ Iris scanning (scanning iris of your eye)

□ Voice recognition

□ Keystroke analysis (typing pattern)

□ Location based (the service is accessible just from specific locations)

15 Where do you think the data (for example passwords, biometrical data...) that is used in authentication should be stored?

□ Locally (SIM card or phone memory)

□ Externally (Network operator, service provider…)

□ Don’t know

10 Appendix B Questionnaire Results

Question 1: **Age**

	Below 18	18-24	25-34	Above 34
Number	0	37	35	1

Question 2: **Gender**

	Male	Female
Number	48	25

Question 3: **Highest achieved education level**

	Grade school	High school	Bachelor degree	Master degree and above
Number	0	29	27	17

Question 4: **How important are these options for you when you choose a network operator?**

	Not important	Medium	Very important
Choice of mobile device	27	27	19
Network coverage	4	24	45
Operator loyalty	34	22	17
Prices, deals etc.	0	13	60
Security	13	36	24

Question 5: **How important are these options for you when you choose a mobile device?**

	Not important	Medium	Very important
Brand	19	33	21
Battery	3	35	35
Accessories	26	40	7
Games	54	19	0
Security	10	47	16
Infrared/Bluetooth	16	42	15

Question 6: **Which functionalities do you use on your phone?**

	Yes	No	Not available
Information services	37	27	9
Internet browsing	50	20	3
Email	37	30	5
E - commerce	8	57	8
Mobile banking	17	49	7
Music	42	30	1
MMS	49	23	1
GPS	33	31	9
Third party applications and games	37	32	4
Calendar/Organizer	60	13	0

Question 7: **What functionalities do you think you would use in the future?**

	Mobile health	Mobile learning	Video conferencing	Mobile payment	Video on demand
Number	27	25	30	44	29

Question 8: **Which services do you use today on mobile and/or stationary devices?**

	Social network	Subscription services	Banking	MinID
Mobil	38	20	14	8
Stationary	66	62	63	59

Question 9: **How secure do you think PIN numbers/passwords and tokens (One Time Password generators, password cards, SMS) are on mobile devices?**

	Low	Medium	High	Not decided
PIN number / Password	13	51	5	4
Token	4	41	21	7

Question 10: **How do you perceive usability of PIN numbers/passwords and tokens on mobile devices?**

	Low	Medium	High	Not decided
PIN number / Password	7	44	16	6
Token	14	39	11	9

Question 11: **If you use password authentication, do you utilize possibility of your mobile device to remember password for you?**

	Yes, always	Sometimes	Depend on the service	No, never	Udecided
Number	2	10	22	36	3

Question 12: **If you lose your phone, what will you consider as the biggest problem:**

	Loss of contact list	Loss of SMS messages	Loss of pictures/other media on mobile phone	Loss of other private information stored on the mobile phone	Loss of authentication token for other kinds of services	Expenses
Number	53	23	32	35	13	48

Question 13: **Do you think that there is need for higher security for mobile services?**

	Yes	No	Dont know
Number	46	5	22

Question 14: **Which of these authentication types for mobile services would you use in the future?**

	Fingerprint	Face recognition	Hand recognition	Iris scanning	Voice recognition	Keystroke analysis	Location based
Number	42	16	16	25	17	23	16

Question 15: **Where do you think the data (for example passwords, biometrical data...) that is used in authentication should be stored?**

	Locally	Externally	Dont know
Number	22	23	28