UNIVERSITY OF OSLO
Department of Informatics

Authentication methods for mobile services

INF 5261

Report: Main factors affecting user acceptance of authentication methods for mobile services in Norway

Jelena Mirkovic

Spring 2010

UNIVERSITAS OSLOENSIS
MDCCCXI

Table of Content:

1. Introduction

The main goal that we set for our research project for the course “Development of mobile information systems and services” was to identify different authentication methods for mobile services and try to familiarize with them and comprehend them from different points of view (differences between stationary and mobile implementation, security, usability, user perceptiveness, usefulness). We see that security issue is becoming more and more important for mobile world, and we think that overcoming this issue will become major obstacle for development and deployment of future mobile services.

For this report I found interesting to compare results that we gathered through our research project in the context of one specific country, in this case Norway. I wanted to identify main authentication methods that are supported today in Norway, their main characteristics and acceptance from the users. I also want to see what is the main reason for their good/poor acceptance. Is that security, usability, privacy issues or something else?

2. Authentication for mobile services – what is supported for services in Norway

In this chapter I will try to identify and shortly describe types of authentication that are offered to people here in Norway. In our group report we saw that mostly used authentication methods for mobile services are based on something the user knows and something the user has. Implementation of these two types of authentication will be presented also here.

2.1. Authentication based on something the user knows

Authentication based on something the user knows is mostly used authentication for mobile services. When accessing most popular mobile services (Internet browsing, mail) the user is usually prompted just for username and password. The user is generally allowed to choose his/hers passwords so he/she can greatly influence security of his/hers private information. Also, most of services offer to the user possibility to save password locally on the device and on that manner adjust security or usability of the service according to his/hers needs.

2.2. Authentication based on something the user has

For this kind of user authentication user is required be in possession of the specific physical object, authentication token [1]. There are different types of tokens and they can vary from cards with printed passwords that require user to retype password, to the specific devices can be connected to user’s terminal so the user can be authenticated. When tokens are used with mobile device one very good approach is to store private information on the mobile device and then use mobile device in the same time as token and terminal. This is example how specific characteristic of a mobile device can be utilized to enhance usability of authentication method. Using this approach there is three different manners how this specific information can be actually stored on device: on hardware of the mobile device, on specific file on the memory of the device or on the operator side. In Norway there is couple of companies that are providing solutions with a token integrated with mobile device. Here I will very shortly describe some of them.

2.2.1. BankID

BankID is personal and simple electronic identity for secure identification and signing on the Internet [2]. It is used by most of the banks in Norway as a possible approach to log into their online banking service. Authentication of the user is based on the Public Key Infrastructure and it is registered at security level 4 with Post- og teletilsynet [3]. Currently this type of authentication is used just for access to services through stationary devices, but they also developed BankID for mobile that is adjusted for usage on mobile phones.

2.2.2. BankID for Mobile

BankID for mobile is electronic identity and signing solutions, where users private information is stored on the SIM card of the mobile phone [4]. The advantage of this solution is that private data cannot be tampered with, and it can be used just for this specific service. On this manner it is provided higher security, but on the other hand user is more dependent on his/hers network provider which produced SIM card. One more disadvantage of this approach is that BankID for Mobile in Norway is supported only by Telenor and none of the other network operators.

2.2.3. SMS

In this approach mobile phone is used by user to get one time password (OTP) through SMS message [5]. Some banks use this approach as part of multi factor authentication of the user before permitting access to on line banking service. Here the main communication channel between the user and the bank is still Internet connection to bank's online site, and SMS message is used as additional communication channel that provide more secure authentication.

2.2.4. Encap One Time Password generator application

Encap One Time Password generator application is patent two-factor user authentication software [6]. This software is used as substitution of the OTP generator, where OTP is generated using some specific information of the mobile device and information received through the network. Advantage of this approach is that it can be used on any phone and do not depend on a network operator.

2.2.5. Buypass Mobil

Buypass company developed mobile phone application that can be used for payment and as identification services [7]. The solution is independent of the network provider and works on all mobile phone that supports Java. First company that used this solution was Norwegian National Lottery.

2.3. Conclusion

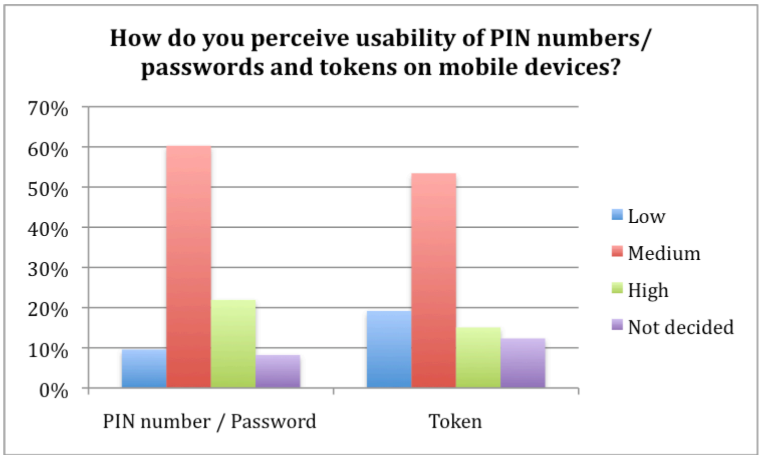
As seen from previous part there is a number of solutions for user authentication available in Norway. This can be proof of great potential of mobile services that is identified by many companies and service providers. But also it can be the evidence that security regulations and requirements for successful deployment of services handling private information are not yet completely formulated and set. Norway can be seen as country that takes care of security of private information of their citizens, and the proof is National Strategy on IT-Security which is adopted in July 2003 [8]. It has an aim at reducing vulnerabilities related to information system and networks, promoting a culture of IT-security and facilitating electronic commerce. So before development and wide deployment of mobile services that are dealing with people's private information security solution that provide good protection of users needs must be in place and accepted as secure enough.

3. User perception of different authentication methods

In previous section I described different authentication methods for user authentication provided in Norway. As we seen passwords are very standard way of authentication but there is more and more approaches for authentication based on tokens that are integrated with the mobile phone and that have different level of usability and security. But the most important thing that determines if some technology will be successful is user's acceptance. To identify user's perception regarding described authentication methods I will use results from the questionnaire and interviews that we conducted in our group project, and try to process results more in the concept of these two authentications methods.

3.1.Usability

In the question from our questionnaire where we asked respondent how they perceive usability of this two authentication methods passwords and PIN numbers are seen as mostly medium usable (10% of respondents reply with Low, 60% with Medium, 22% with High) [Graph 1]. On the other hand tokens in general are seen as also medium usable but with more answers for low usability (19% of respondents reply with Low, 53% with Medium, 15% with High). From this I can see that even on the mobile devices passwords are still perceived as more usable, even beside limited input characteristics of the input methods. Also when processing this results I must take in consideration that when asked about token it is meant of token in general, not integrated with mobile devices.

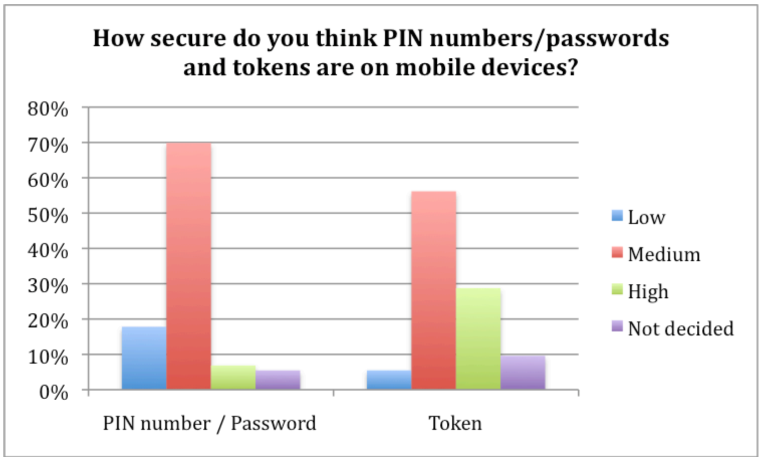


Graph 1. Responses on question "How do you perceive usability of PIN numbers/passwords and tokens on mobile devices?"

From this I can see that both passwords and tokens are on medium level of usability (even thought that passwords are more to high and token to low, but the difference is not that high). Also I can conclude that users do not have any major usability issues with any of the two methods.

3.2.Security

When asked about security majority of respondents both tokens and passwords rated as medium secure (Passwords: 70%, 56% Tokens) [Graph 2]. But passwords have higher number of Low security answers (18%) compared to tokens (5%), and tokens have higher number of High security answers (29%) then passwords (7%). From this I can see that tokens are actually perceived as more secure but the difference in not very high.



Graph 2. Responses on question "How secure do you think PIN numbers/passwords and tokens are on mobile devices?"

As evidence that people are concerned about security of private information on mobile devices is a fact that just 3% people store their passwords on the phone. The rest of them do not use this option as default (at least not for all passwords). From this I can see that they are prioritizing security over usability.

As a conclusion I can say that neither of the methods are rated as high secure, which mean that there is still requirement for higher security authentication method for services that works (or will work) with more sensitive user's information. That also confirmed 63% of respondents that said they think there is need for higher security for mobile services.

Here I would also like to mention the general impression that we had form the performed interviews with users, which are mostly not concerned about security of the mobile services and they are trusting service provider to provide high enough level of protection. They especially have confidence for banks and government because they see them as serious entities that are concerned about security of the service they provide. What are they mostly concerned when talked about security for mobile devices are their personal information that is stored on the device.

3.3. Usefulness

I also wanted to see what is acceptance of these methods in user's everyday life. I will use the responses on the question about services people use today on mobile devices to illustrate this. I saw that very few use services that require higher level of authentication (Social networks – 52%, Subscription services – 27%, Banking - 19%, MinID - 11%). I can see that services that require authentication with passwords are more often used on a mobile device. There is now logical question of why are tokens so much less used? There can be three reasons for this: first is that this kind of authentication is hard to perform (usability issue), second is that this kind of authentication do not provide high level of security, and the last is that this kind of applications is not appropriate for mobile phones regardless what authentication method is used (usefulness of service). From the previous parts I saw that usability is not a problem because both methods are graded very similar and services that uses passwords are still more used. Also security do not seem to be a problem because the most of the people that we interviewed said they trust banks and government as service providers. So the only problem that is left is usefulness of this kind of services. That is also confirmed in the interviews where people said that they do not use these services because of their lack of usability and overview of the content on the screen.

The fact that just 18% of respondents said that they will be worried about loosing authentication token for different kind of services when loosing phone shows that not so much users use mobile phone as identification token. Also when we talked with people during interviews they said that they do not use this option in general because they do not like too much private information to be stored on one place.

3.4. Conclusion

From the previous parts I can see that there are neither major usability nor security problems for both authentication methods. The main reasons why passwords are still used more frequently are lack of usability and usefulness of mobile services that require higher level of security. When more advanced services appear and become more popular, according to this results people will not have problem using tokens for authentication. Also one interesting conclusion is that people actually do not see mobile phone as secure device and they are more worried about security of their private data on the device than accessing mobile services that are working with their private data.

4. Summary

As a conclusion of this report I can see that in Norway exists different authentication methods for mobile services that provide different level of usability and security. Also Norwegian Government and laws are on the side of the people and they are trying to protect their private information. But I can see that the problem with wide deployment of mobile services is more because of users´ perception of their usefulness, then because security issues. I think that in Norway there are authentication methods that provide good level of security to users, but there is still need for development of mobile services that are more adjusted to user requirements and needs and for which higher security authentication methods are needed.

5. References

[1] Computer security reference book. ed. K.M. Jackson, J. Hruska, and B.P. Donn. 1992, CRC Press, Inc. 949.

[2] BankID COI, White Paper. Bankenes Betalingssentral AS. 06.09.2005. Available from: http://www.eurim.org.uk/activities/pi/BankIDWhitePaper.pdf

[3] BankID godkjent i høyeste sikkerhetsklasse. [cited 07.05.2010.]; Available from: https://www.bankid.no/Presse-og-nyheter/Nyhetsarkiv/2008/BankID-godkjent-i-hoyeste-sikkerhetsklasse/

[4] BankID på mobil. [cited 07.05.2010.]; Available from: https://www.bankid.no/Dette-er-BankID/BankID-pa-mobil/

[5] Comparing PhoneFactor to Other SMS Authentication Solutions. [cited 20.04.2010.]; Available from: http://www.phonefactor.com/sms-authentication.

[6] Using the mobile phone in two-factor authentication. Anders Moen Hagalisletto, Arne Riiber. 2007. Available from: http://www.encap.no/admin/userfiles/file/iwssi2007-05.pdf

[7] Buypass Mobil. [cited 07.05.2010]; Available from: http://www.buypass.no/Brukersted/Mobil

[8] Organization for economic cooperation and development (OECD), "OECD studies in risk management, Norway Informaiton Security", 2006. Available from: http://www.oecd.org/dataoecd/36/16/36100106.pdf