

On Online Banking Authentication for all: A Comparison of BankID Login Efficiency using Smartphones versus Code Generators

Ellen Opsahl Vinbæk¹, Frida Margrethe Borge Pettersen¹, Jonas Ege Carlsen¹, Karl Fremstad¹, Nikolai Edvinsen¹ and Frode Eika Sandnes^{1,2[0000-0001-7781-748X]}

¹Department of Computer Science, Faculty of Technology, Art and Design, Oslo Metropolitan University, P.O. Box 4 St. Olavs plass, 0130 Oslo, Norway

²Institutt for Technology, Kristiania University College, Prinsens gate 7-9, Postboks 1190 Sentrum, 0107 Oslo, Norway
frodese@oslomet.no

Abstract. Authentication is an essential component of any digital service. In Norway, such authentication is often relying on BankID using either mobile BankID or a code generator. This study set out to explore the efficiency of these authentication user interfaces. A mixed experiment involving 20 users was conducted. The results show that the code generator is faster, but for individuals with a preference for mobile BankID the difference is insignificant. Individuals with a preference for code generators take significantly longer time to use BankID.

Keywords: accessibility, authentication, security, usability, user diversity, online banking, BankID

1 Introduction

The banks in Norway offers the authentication platform BankID for online banking. BankID is also used for accessing governmental services such as revenue and tax return, digital health services and digital mail services. To use BankID, the customers first need to identify themselves with their 11-digit personal ID-number following a Norwegian standard [1]. The next step is performed using either a smartphone or a code generator. The code generator is a simple small device with a single button and a 6-digit LCD display (see Fig. 1). To use the code generator the user simply presses the button and the code generator displays a disposable 6-digit code that the user inputs in the login form followed by a personal password. To use mobile BankID with a smartphone, the user is asked to enter the mobile phone number during the login procedure. Next, a dialogue is displayed on the phone where the user inputs a personal PIN code comprising 4-8 digits (see Fig. 2).

Both procedures are simple, but they are different. The code generator involves the copying of 6 arbitrary digits, while mobile BankID involves the input of at least 8 familiar digits making up the phone number, followed by a fixed pin of 4 to 8 digits.



Fig. 1. bankID code generator

The code generator requires fewer actual keystrokes, yet the task of copying an arbitrary sequence of digits is cognitively and visually more demanding than recalling 8 to 16 digits from memory. Opinions vary about which of the two is the best. This study therefore set out to determine which of the two methods is the fastest to use, and what method users prefer.

2 Background

There has been much research into the relationship between security and usability [2, 3], also in terms of online banking [4, 5, 6]. As citizens are expected to use digital services the need for accessibility and usability are more demanding. Internet banking is one such service and online banking has received quite some attention among researchers [7, 8, 9]. Olsen [10] documented a case in Norway where the bank automatically appended zeros to incorrectly inputted account numbers. This malpractice led to economic consequences for customers. The Norwegian invoice system requires many digits to be input [11], and better use of mnemonic aids have thus been proposed as one possible remedy [12].

The login procedure is particularly critical. It must be both secure and easy to use. The Norwegian BankID system has received some attention in the research literature [13] and several studies have addressed security issues [14, 15]. BankID has also received some criticism for not being accessible by blind individuals [16]. This questionnaire-based study looked at electronic banking in a wide sense, including Automatic Teller Machines (ATMs), and found that many of the target users have practical IT-skills including that of installing and updating software [16]. This was particularly relevant in the early years of BankID as it required a Java browser plugin capable of running Java applets. The Java-applet oriented solutions have since been replaced with more generic javascript solutions that run in the browser and does not require any browser plugins. Moreover, according to the study [16] many of the services were considered inaccessible yet the level of inaccessibility varied among the services. Most participants reported using several passwords, while the older participants were more likely to always use the same password for different services.

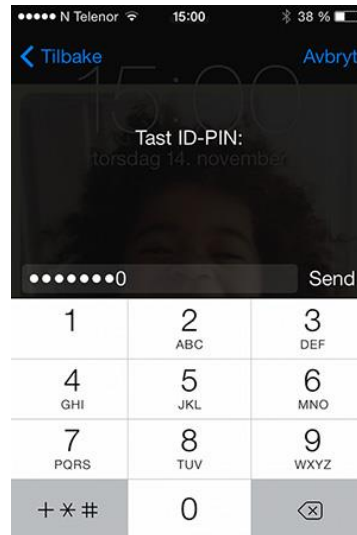


Fig. 2. Smarthpone BankID (Landkreditt Bank AS)

It is especially the BankID web solutions that has been criticized for not been compatible with screen-readers. A screen-reader is a device that allows blind computer users access computer output via synthetic speech or Braille [17]. Screen readers are also used by some dyslexic computer users [18]. Moreover, many banks do not offer code generators with synthetic speech [19] for its visually impaired and dyslexic customers. Recent Norwegian legislature [20] has been introduced to ensure that digital services aimed at the general public are universally accessible to all including individuals with variations in sensory, cognitive or motor functions.

There is a vast body of research that has addressed the general phenomenon involved in man-machine interaction such as output and reduced senses, cognition and memory [21, 22] and input [23]. Several HCI researchers have also addressed banking specifically. For instance, Kaye et al. [24] collected data about monetary and financial patterns of 14 individuals in the San Fransisco Bay Area at both personal and family levels. Vines, Dunphy and Mond [25] studied how technology plays a part in the finances of low-income families and issues related to trust was found to be of importance. A study of users' decision making related to security found that users tended to base their assessment on their perceptions and relationships with the various companies and not the actual privacy characteristics of a service or app [26]. The subjective measurement of trust has also been addressed by the means of Likert scales and semantic differentials [27].

Password credential sharing has been found to be a common practice although it is not allowed by banks [28]. For families, and couples, the sharing of accounts is often practical. A study in Australia [28] showed that especially in low-income communities credential sharing was sometimes the only way to transfer money. The researchers conclude that banking security mechanisms must be flexible enough to facilitate peoples'

need to share accounts. Similarly, a study of culture connected password credential sharing showed that users in the Kingdom of Saudi Arabia shared their credentials within families as a token of trust and against the advice of banks [29] leading to certain problems related to accountability and abuse.

Nilsson, Adams and Herd [30] studied how various authentication mechanisms affect trust. Their questionnaire and interview-based approach revealed that users found login procedures involving random passwords generated with a password box more trustworthy than traditional fixed passwords. If these results generalize it could also be that BankID gives user an increased sense of trustworthiness. Security issues such as phishing has received much attention and a literature on counter measure can be found in Purkait [31].

Kim and Moon [32] studied how interfaces can be designed to evoke certain emotions thereby affecting the users trust where online banking was used as a case. Research studying other aspects of banking interaction includes Medhi, Gautama and Toyama [33] who conducted an ethnographic study of the usability of mobile banking solution for urban areas of India with a larger sample of non- and semi-literate users. Their results showed that prototypes of non-textual interfaces, that is, interfacing relying on images or speech were preferred over a text-based interface prototype. Rich multimedia designs led to higher completion rates while speech-based designs led to faster completion times and less need for assistance. Kumar, Martin and O'Neill studied the general deployment of mobile banking in India [34].

Ravendran, MacColl and Docherty [35] found that the usability in terms of SUS-scales where improved when banking interfaces were tag-based, that is, that various elements could be tagged with user-selected names. Vines and colleagues [36] reported on a prototype of a digital cheque book designed for older users that were accustomed to paper-based cheque books. The concept was as follows: the digital cheque book was visually similar to a traditional paper-based cheque book where the user fills in the cheques with a pen. The authors reported on how they worked with the mass media through press releases to get the local banking industry interested in the project.

One approach that avoids the difficulties associated with technological payment systems is UbiPay which goal is to allow payments to be done implicitly using contextual information as part of everyday interactions [37]. Inspired by wallet phones, that is, the use of a phone to make small purchases by placing a smartphone next to a reader payments may for instance be made automatically for single fare tickets when a passenger enters a metro station. Near field communication (NFC) technology is now widely used for simple transactions. Participatory methods with focus groups involving older people has also been used to bring new insight to the design of banking services [38].

To the best of our knowledge there are no existing empirical studies comparing the usability of mobile BankID and BandID code generators.

3 Method

3.1 Experimental design

A mixed experimental design was chosen with task-completion-time as dependent variable, and authentication device and preferred device as independent variables. Authentication device was a within-groups factor with the two levels smartphone and code generator. Device preference was a between-groups factor with the same two levels, namely smartphone and code-generator.

3.2 Participants

All the 20 participants recruited ranged in age from 15 to 75 years. They were all regular users of BankID. Of these, 6 participants preferred the code generator and 14 participants preferred the smartphone version of BankID.

The participants were asked to use their personal bank-account for the experiment which raises obvious ethical dilemmas. The participants were thus recruited among friends and family to ensure that the participants trusted the experimenters and that no sensitive information would be recorded. Moreover, it would be challenging to recruit arbitrary people in the street as people usually do not carry their code generators around. No personal information, or information that could be used to detect the participants, was recorded. The participation in the experiment was therefore fully anonymous.

3.3 Task

Each participant was asked to log into their Internet bank portal by using both a mobile BankID and by using a code generator. The experiment was balanced to prevent learning effects by randomizing the order of the two authentication devices.

3.4 Procedure

Prior to the observation session the experimenters ensured that the participants had access to their code generator and had activated Mobile BankID. First, each participant was briefed about the experiment. The participants were then asked to sign a consent form which clearly indicated that participation was voluntary, the results are anonymous and that they could withdraw from the experiment at any time. The consent form also asked the participants about their preferred authentication device.

The experiments were conducted in a quiet room with only two of the authors present in addition to the participants to facilitate the experiment, observe and record the time. The experimenters positioned themselves in such a way as not to pry on the participants sensitive banking details. Each session was run with just a single participant.

After the experiment the participants were asked if they had changed their preferences. None of the participants had changed their BankID preference after the experiment. Each session lasted between 5 to 10 minutes including briefing.

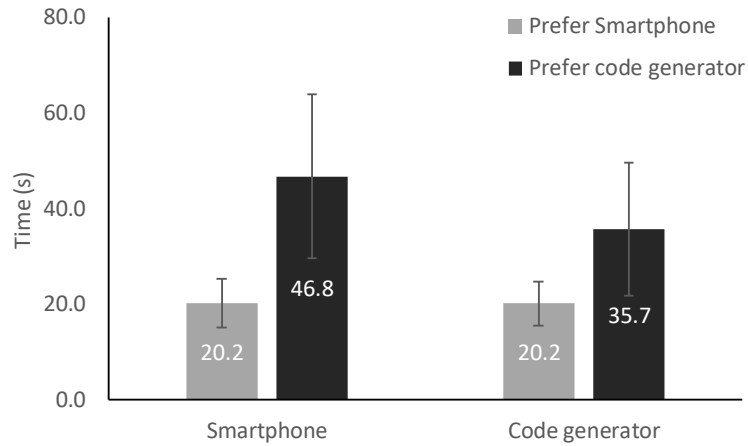


Fig. 3. Results of the authentication experiment. Error bars show standard deviation.

3.5 Measurements and analysis

A stopwatch was used for recording the task completion times. The time from after the participants had inputted their personal ID-number until they had successfully logged into the Internet bank was recorded manually using pen and paper. None of the participants personal information were recorded. The data were analyzed using the open source statistical software package JASP 0.8.6.0 [39]. The experiments were conducted during the autumn of 2017 before the introduction of the General Data Protection Regulation (GDPR).

4 Results

The results (see Fig. 3) reveal that the code generator was faster to use in seconds ($M = 24.8$, $SD = 10.9$) than the smartphone ($M = 28.2$, $SD = 15.8$) although a majority (70%) of the participants preferred the smartphone. The spread of the measurements using the code generator was also smaller than the measurements observed with the smartphone. Fig. 3 shows the results of the experiment also according to the participants preferences. These results reveal that the variation in the observations are related to the participants preferences, as participants who preferred the code generator generally took longer than the participants who preferred the smartphone. The participants who preferred the code generator also performed the task faster with the code generator in seconds ($M = 35.7$, $SD = 13.9$) compared to the smartphone ($M = 46.8$, $SD = 17.1$). This difference between the two authentication devices is significantly different ($F(1, 18) = 13.0$, $p < .002$).

The results obtained for the participants who preferred the smartphone are significantly different from those who preferred the code generator ($F(1, 18) = 24.9$, $p < .001$). There is also an interaction effect between authentication device, and the preference

($F(1, 18) = 12.9, p = .002$). The participants who preferred the smartphone performed the task slightly faster using the code generator ($M = 20.15, SD = 4.61$) compared to the smartphone ($M = 20.21, SD = 5.09$). However, a paired t-test revealed that this difference is not statistically significant ($t(13) = 0.039, p = .97$). Moreover, the spread in the observations of participants who preferred the smartphone is much smaller than for those who preferred code-generators. These small spread signals a more consistent usage pattern and indicates that these participants have more developed technology skills.

5 Discussion

The results show that the code generator is faster to use than the smartphone. This is not surprising as the code generator is a special-purpose device while the smartphone is a general-purpose device. Generally, users prefer familiar environments and if a user regularly uses a smartphone, the smartphone may be more positively perceived than the code generator. By operating in an environment perceived positively, the user may not actually notice that the task may take longer. However, although all the users solved the tasks faster with the code generator this difference was not significant for those preferring the smartphone.

Participants who preferred the code generator generally took longer time and exhibited a larger variation in performance. This is a sign that this group is less experienced with technology. One may speculate that a preference for the smartphone is related to the technological skills of the users, while less skilled users prefer the simplicity of the code generator with its single button and simple interaction steps.

There may also be situations where technologically savvy users prefer the code generator, such as privacy and security. A smartphone that is constantly connected to the Internet and used for many of the user's daily tasks is vulnerable. The code generator on the other hand may be perceived as safer as it is not connected to the Internet.

5.1 Limitations and future work

Conducting observational studies of users conducting sensitive computer operations is challenging as one needs to ensure the privacy of the participants while also ensuring their trust. Consequently, the current study is based on a relatively small sample ($N = 20$) and only one simple dependent variable was observed (completion time). With a larger sample of users from distinct user groups more concrete patterns may be found. For instance, distinct age groups could perhaps be used as a between-groups independent variable to assess the effect of age which has been found to have effects on banking patterns [16].

Moreover, given more elaborate measurements achievable by employing keyboard loggers and screen capturers one may be able to perform more sophisticated analysis of the interaction between users and the banking system. However, detailed logging requires especially stringent steps to ensure privacy and careful ethical considerations.

The study of online banking habits from 2013 [16] did not include smartphone-based BankID. It would thus also be relevant to run a similar study on blind and visually impaired users in context of smartphone-based authentication. Smartphones hold the potential of providing accessibility support when the smartphone apps are implemented to support the built in accessibility facilities such as built-in screen readers such as TalkBack on Android or VoiceOver on IOS.

6 Conclusions

This study explored the difference between BankID authentication using code generators and smartphone solutions from a usability perspective. The results show that the majority prefer the smartphone over the code generator. The code generator is faster to use than the smartphone, but this difference is insignificant for the technology confident participants. Yet, it is expected that all citizens are to use these authentication systems to perform key duties as citizens. Since a large fraction of the population are not interested in or confident using technology, or even wants to use smartphones, it seems sensible to continue with both mobile BankID and the code generator although the smartphone version is both more popular and probably a cheaper alternative for the banks.

References

1. Selmer, E. S.: Personnummerering i Norge: Litt anvendt tallteori og psykologi. Nordisk matematisk tidsskrift 12, 36–44 (1964)
2. Gunson, N., Marshall, D., Morton, H., Jack, M.: User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security* 30, 208-220 (2011)
3. Braz, C., Robert, J. M.: Security and usability: the case of the user authentication methods. In: *Proceedings of the 18th Conference on l'Interaction Homme-Machine*, pp. 199-203. ACM (2006)
4. Casalo, L. V., Flavián, C., Guinalú, M.: The role of security, privacy, usability and reputation in the development of online banking. *Online Information Review* 31, 583-603 (2007)
5. Pikkariainen, T., Pikkariainen, K., Karjaluo, H., Pahnla, S.: Consumer acceptance of online banking: an extension of the technology acceptance model. *Internet research* 14, 224-235 (2004)
6. Smith, A. D.: Exploring security and comfort issues associated with online banking. *International Journal of Electronic Finance* 1, 18-48 (2006)
7. Yeow, P. H., Yuen, Y. Y., Tong, D. Y. K., Lim, N.: User acceptance of online banking service in Australia. *Communications of the IBIMA* 1, 191-197 (2008)
8. Sohail, M. S., Shanmugham, B.: E-banking and customer preferences in Malaysia: An empirical investigation. *Information sciences* 150, 207-217 (2003)
9. Laforet, S., Li, X.: Consumers' attitudes towards online and mobile banking in China. *International journal of bank marketing* 23, 362-380 (2005)
10. Olsen, K. A.: Customer Errors in Internet Banking. In: *Proceedings of Norsk Informatikkonferanse, Tapir Academic Publishers* (2008)

11. Sandnes, F. E.: Effects of common keyboard layouts on physical effort: Implications for kiosks and Internet banking. In: Sandnes, F.E., Lunde, M. Tollefsen, M., Hauge, A.M., Øverby, E., Brynn, R. (eds.) The proceedings of Unitech2010: International Conference on Universal Technologies, pp. 91-100. Tapir Academic Publishers (2010)
12. Sandnes, F. E.: A memory aid for reduced cognitive load in manually entered online bank transactions. In: Proceedings of Norsk informatikkonferanse, pp. 273-276. Tapir Academic Publishers (2012)
13. Wangensteen, A., Lunde, L., Jorstad, J., Thanh, D.: A generic authentication system based on SIM. In: International Conference on Internet Surveillance and Protection 2006 (ICISP'06), pp. 24-24. IEEE (2006)
14. Gjølsteen, K.: Weaknesses in BankID, a PKI-substitute deployed by Norwegian banks. In: European Public Key Infrastructure Workshop, pp. 196-206. Springer, Berlin, Heidelberg (2008)
15. Espelid, Y., Netland, L. H., Klingsheim, A. N., Hole, K. J.: A proof of concept attack against norwegian internet banking systems. In: International Conference on Financial Cryptography and Data Security, pp. 197-201. Springer, Berlin, Heidelberg (2008)
16. Tjøstheim, F. I.: Undersøkelse om autentisering, innlogging og tilgjengelighet blant medlemmer i Norges Blindeforbund. Technical report DART/12/2013, The Norwegian Computing Center (2013)
17. Lazar, J., Allen, A., Kleinman, J., Malarkey, C.: What frustrates screen reader users on the web: A study of 100 blind users. *International Journal of human-computer interaction* 22, 247-269 (2007)
18. Evett, L., Brown, D.: Text formats and web design for visually impaired and dyslexic readers—clear text for all. *Interacting with computers* 17, 453-472 (2005)
19. Subashini, K., Sumithra, G.: Secure multimodal mobile authentication using one time password. In Proceedings of the 2nd International Conference on Current Trends in Engineering and Technology (ICCTET), pp. 151-155. IEEE (2014)
20. Whitney, G., Keith, S., Bühler, C., Hewer, S., Lhotska, L., Miesenberger, K., Sandnes, F.E., Stephanidis, C., Velasco, C.A.: Twenty five years of training and education in ICT Design for All and Assistive Technology. *Technology and Disability* 3, 163-170 (2011)
21. Berget, G., Sandnes, F.E.: Do autocomplete functions reduce the impact of dyslexia on information searching behaviour? A case of Google. *J. Am. Soc. Inf. Sci. Technol.* 67, 2320–2328 (2016)
22. Sandnes, F.E., Jian, H.L., Pair-wise variability index: Evaluating the cognitive difficulty of using mobile text entry systems. In: International Conference on Mobile Human-Computer Interaction. LNCS, vol. 3160, pp. 347-350. Springer Berlin Heidelberg (2004)
23. Sandnes, F. E.: Evaluating mobile text entry strategies with finite state automata. In: Proceedings of the 7th international conference on Human computer interaction with mobile devices & services, pp. 115-121. ACM (2005)]
24. Kaye, J. J., McCuiston, M., Gulotta, R., Shamma, D. A.: Money talks: tracking personal finances. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 521-530. ACM (2014)
25. Vines, J., Dunphy, P., Monk, A.: Pay or delay: the role of technology when managing a low income. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 501-510. ACM (2014)
26. Binns, R., Zhao, J., Van Kleek, M., Shadbolt, N., Liccardi, I., Weitzner, D.: My Bank Already Gets this Data: Exposure Minimisation and Company Relationships in Privacy Decision-Making. In: Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems, pp. 2403-2409. ACM (2017)

27. Rieser, D. C., Bernhard, O.: Measuring Trust: The Simpler the Better?. In: Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems, pp. 2940-2946. ACM (2016).
28. Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G., Furlong, M.: Password sharing: implications for security design based on social practice. In: Proceedings of the SIGCHI conference on Human factors in computing systems, pp. 895-904. ACM (2007)
29. Flechais, I., Jirotko, M., Alghamdi, D.: In the balance in Saudi Arabia: security, privacy and trust. In: CHI'13 Extended Abstracts on Human Factors in Computing Systems, pp. 823-828. ACM (2013)
30. Nilsson, M., Adams, A., Herd, S.: Building security and trust in online banking. In: CHI'05 Extended Abstracts on Human Factors in Computing Systems, pp. 1701-1704. ACM (2005)
31. Purkait, S.: Phishing counter measures and their effectiveness—literature review. *Information Management & Computer Security* 20, 382-420 (2012)
32. Kim, J., Moon, J. Y.: Emotional usability of customer interfaces: focusing on cyber banking system interfaces. In: CHI'97 Extended Abstracts on Human Factors in Computing Systems, pp. 283-284. ACM (1997)
33. Medhi, I., Gautama, S. N., Toyama, K.: A comparison of mobile money-transfer UIs for non-literate and semi-literate users. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems pp. 1741-1750. ACM (2009)
34. Kumar, D., Martin, D., O'Neill, J.: The times they are a-changin': mobile payments in India. In: Proceedings of the SIGCHI conference on human factors in computing systems, pp. 1413-1422. ACM (2011)
35. Ravendran, R., MacColl, I., & Docherty, M.: Tag-based interaction in online and mobile banking: A preliminary study of the effect on usability. In: Proceedings of the 10th Asia pacific conference on Computer human interaction, pp. 35-40. ACM (2012)
36. Vines, J., Thieme, A., Comber, R., Blythe, M., Wright, P. C., Olivier, P.: HCI in the press: online public reactions to mass media portrayals of HCI research. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 1873-1882. ACM (2013)
37. Lehdonvirta, V., Soma, H., Ito, H., Kimura, H., Nakajima, T.: Ubipay: conducting everyday payments with minimum user involvement. In: CHI'08 Extended Abstracts on Human Factors in Computing Systems, pp. 3537-3542. ACM (2008)
38. Vines, J., Blythe, M., Lindsay, S., Dunphy, P., Monk, A., Olivier, P.: Questionable concepts: critique as resource for designing with eighty somethings. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 1169-1178. ACM (2012)
39. JASP Team: JASP (Version 0.9)[Computer software]. <https://jasp-stats.org/> (2018).