This is the author copy of the paper "Usability Of Mobile Voting with NFC Technology". For the original paper, please go to http://www.actapress.com/Abstract.aspx?paperId=37960.

USABILITY OF MOBILE VOTING WITH NFC TECHNOLOGY

Kerem Ok, Vedat Coskun, Mehmet N. Aydin
ISIK University, Department of Information Technology
34980, Sile, Istanbul, Turkey
{keremok | vedatcoskun | mnaydin}@isikun.edu.tr

ABSTRACT
Voting is a method to select one opinion or a person often following discussion, debate or an election campaign. After centuries of paper based voting ballots, electronic voting is used along with various technologies. One of the promising technologies is Near Field Communication (NFC) which allows data transfer between NFC-enabled devices and smart tags within a short distance. In this paper, we have presented a new type of a secure voting system, namely NFC voting, and evaluated the system's usability in a university council election with an executable prototype. Among other findings, we found that NFC voting satisfies electronic voting requirements and further increases the subjective usability of the proposed system.

KEY WORDS
NFC, Mobile and Wireless Computing, Electronic Voting, Subjective Usability.

1. Introduction

Voting is described as a method for a group such as a meeting or an electorate to make a decision or express an opinion-often following discussions, debates, or election campaigns in [1]. In traditional voting systems, people go to specific voting locations and cast their vote using paper ballots.

After the extensive implementations of traditional voting for many centuries, as the advances in technology promised some help on this issue, electronic voting systems are developed giving the opportunity to people cast their votes using electronic devices. Electronic voting has several benefits and solves many problems of traditional voting [2]. It further enables voters to vote almost anywhere without geographical restrictions [3].

Electronic voting systems are classified as poll-site voting, kiosk voting, and remote electronic voting [2].

Poll-site voting: This is similar to traditional voting systems. A voter goes to a specific place to cast her vote, generally through touch screen voting terminals. The voter identifies himself using her ID card [2].

Kiosk Voting: Voting machines are placed to convenient locations such as libraries and schools. The voting platforms are controlled by election officials to ensure security and privacy [2].

Remote Electronic Voting: A voter may vote from any location and her vote is transmitted over Internet. In this method, the voter can vote using electronic devices such as notebooks, mobile phones, or PDAs. The voter is identified via remote verification mechanisms such as digital signature, biometrics, and PIN codes [2].

While it is clear that electronic voting systems must still satisfy the requirements of traditional voting systems, it demands some additional requirements. The additional requirements mentioned in various study are accuracy [3, 4, 5], democracy [3, 4, 5], privacy [3, 4, 5], verifiability[3, 4, 5], mobility[3, 4], convenience[4], flexibility[4], simplicity[3], uncoercibility[3], and no unauthorized proxy[5]. Clearly, Some of these requirements overlap, and some are very much related to each other.

After analyzing requirements of classical voting systems and the requirements set by the referenced works, we summarize the requirements for an electronic voting as follows:

1. *Accuracy*: (i) A vote should not be altered. (ii) An invalid vote should not be counted in the final tally. (iii) It should not be possible to eliminate a validated vote from the final tally.
2. *Democracy*: (i) Only eligible voters should be able to vote. (ii) All eligible voters may vote only once.
3. *Anonymity* (*Privacy*): A ballot should not be linked back to the voter who casted it.
4. *Verifiability*: Each voter may verify that her vote is counted.
5. *Mobility*: A voter may vote anywhere without any geographical restrictions.
6. *Usability*: A system may be used by intended users to achieve specific goals.

In this paper, we investigate the use of NFC-enabled devices in voting, namely NFC voting, which extends electronic voting process. We analyze the requirements of NFC voting, by taking into account the requirements of traditional and electronic voting as well. While exploring

the requirements of electronic voting system using Near Field Communication (NFC) technology, we specifically consider the usability of NFC based voting. Usability of electronic voting systems can be measured by three metrics; *effectiveness*, *efficiency*, and *satisfaction*[6]. The first two metrics are objective, whereas the last one is a subjective metric. Effectiveness is about an extent to which the goals of using the system are achieved in terms of its accuracy and completeness. Effectiveness can be measured by completion rates, errors, and assists. Efficiency is the relationship between the level of effectiveness achieved, and the amount of resources expanded. It can be measured by the time spent to achieve the task. Satisfaction can be defined as the user's pleasure whilst using the system. In the context of voting, it can be measured by subjective responses of voters. Satisfaction is assured when a voter is pleased with her voting experience, confident with her vote to be counted, and she thinks that her anonymity is preserved [6, 7].

The NIST reports standardized instruments to test user satisfaction in "Common Industry Format for Usability Test Reports" in [6]. One of these instruments is the SUS (System Usability Scale). It is a simple, ten-item scale giving a global view of subjective assessments of usability. It investigates various aspects of usability and should be used immediately after giving the opportunity to evaluate the system to the participants. In the SUS assessment model, ten five-point items are asked to the participants. The ratings for the items are calculated in a particular manner and a score between 0-100 is produced. A higher score indicates higher usability and lower score indicates the opposite [8].

In this work, we study the viability of the emerging technology, NFC, in the context of electronic voting to improve its usability. To evaluate the usability of NFC in mobile voting, we create a test bed by applying an experimental student council voting in our university. Furthermore, we compare the usability of our model with web-based voting, which is the current method of casting votes at our university. Moreover we investigate if the requirements can be satisfied in the proposed system.

The remainder of this paper is organized as follows. In Section 2, background information of NFC technology is given. In Section 3, the proposed system, its requirements, and the proposed voting scenarios are described. In Section 4, we present the details of the experiment. Section 5 includes the results of our survey together with the discussion of our survey and requirements satisfaction. Finally, we conclude with implications of the findings in Section 6.

2. Background

Voting technology and the usability of these technologies in the context of voting actually can influence the voters' response to the system and directly influence the election results [9]. The usability of electronic voting systems is not deeply studied, and it still preserves its obscurity. Remote electronic voting is the only option to eliminate geographical constraints in the context of voting. So, current and promising technologies which can be used in remote electronic voting have the potential to increase voters' satisfaction.

NFC is one of these promising technologies. It is a short range radio communication technology based on Radio Frequency Identification (RFID). It enables communication between two NFC-compatible devices when they are brought together within less than four centimeters apart, or even by touching themselves. Short range communication within short distance is the major feature of this technology, because it brings ease of use and inherent security. It operates at 13.56 MHz and can transfer data up to 424 Kbits per second [10].

In NFC model, Radio Frequency (RF) communication is performed between two NFC-enabled devices: an *initiator*, and a *target*. Initiator starts the communication, where the target responses to the request made by the initiator. An initiator is an active device which has embedded energy component, where a target may be either an active or a passive device such as an RFID tag. An RFID tag, also called as an NFC tag, is a passive device, since it does not include any energy source. It holds data that can be read only by an active NFC device [11].

One of the important aspects of NFC technology is its inherent security, because communication is started by bringing two devices very close to each other. Separating devices over a limit terminates the communication. The range is so short that, if any hacker device comes close, it will be clearly noticed [12].

One of the most important advantages of this technology is that NFC enabled devices are easy to use, since its technical process is already integrated to the NFC enabled phones during manufacturing. The required software can also be downloaded and installed easily by the technique named as over the air (OTA) transfer. Mobile phones are today's easy to use and comfortable communication equipments, and it is expected that the NFC-compatible mobile phones will reach to 500 million by 2011 [12]. This encourages NFC to be one of our daily life technologies in the near future.

Innovation of NFC technology and NFC built-in mobile phones offer new possibilities for many real-life applications. In [13] a meal service system based on NFC is studied. An application that allows making daily meal orders by touching NFC-enabled mobile phones to an NFC-enhanced menu is tested. In [14] an Electronic Data Capture system for patients is developed. Patient's blood pressure, heart rate, stroke volume and other related data are read by patients' NFC-enabled mobile phone and

transferred to the hospital's server system over Internet. In [15] mobile coupons are used to promote products and services. In this way, users can download mobile coupons to their mobile devices, using the NFC tag attached to a poster or a newspaper. After the download, the coupons can be used at the cashier. In [16] several NFC scenarios are studied and tested. First, a person sees a poster on the street and downloads the information about a movie to her NFC-enabled mobile phone by scanning the NFC tag which is embedded into the poster. She buys a ticket for the movie with her mobile phone, so that cost will be paid through the phone bill later. Then she enters to the theatre by waving her mobile phone to turnstile. After the show, she may also scan a taxi company's poster by the theater entrance to call a taxi. In [17] a prototype system using NFC to support and encourage the outdoor physical activities is presented.

3. Proposed Model

We propose an electronic voting model which uses NFC-enabled devices. We have selected our university's student council election for verification and evaluation of our model. Our university currently uses an in-house developed web-based system for this purpose. After testing the model, it became possible to request comparison of our model with the current model from the student voters.

In our model, three applications will be used: *voting midlet* running on the mobile phone to enable secure voting, *validator servlet* running on the validator server to authenticate the votes, and the *tallier servlet* running on the tallier server to count the legitimate votes. Voting midlet will be installed to the NFC-enabled mobile phone, whereas the servlets will be installed on two separate servers. In order to satisfy some requirements mentioned in the earlier sections, the votes will be encrypted by the midlet, and will be decrypted by the servlets. The midlet as well as the required encryption keys will initially be loaded to the mobile phones. A voter student further can touch her mobile phone to an NFC tag of her favorite candidate in order to start voting process. The student must then enter the pin code to enable the midlet retrieve the encryption keys to be used in encrypting the vote. To send the vote to the validator server, mobile phone should have internet access through Wi-Fi, WiMax, or another mobile data service such as GPRS, EDGE, or HSDPA. After the mobile phone sends the encrypted vote to the validator server, the decryption process is executed and the valid votes are further counted by the tallier server. The details of the process occurred in backend servers are explained further in the following section. After performing this process, midlet displays a confirmation message on the screen giving information about the result of the voting process. Some screen shots of the execution of the midlet are given at Figure 1.

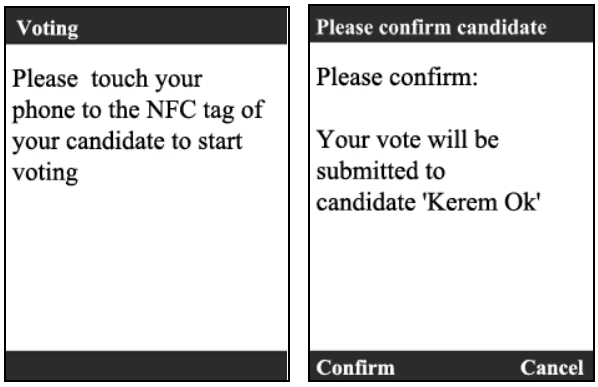

Figure 1. Mobile phone displays

3.1 Details of the Model

Important phases of electronic voting are validating each vote to enable only authorized users vote, and then counting already validated votes. In order to validate and count the votes appropriately we have used two servers; *Validator Server* to validate the received votes, and *Tallier Server* to count validated votes. Validator server must ensure that only and all eligible voters can vote, and they can vote at most once; it keeps the list of the eligible students for this purpose. During the registration of the eligible voters, validator server is also responsible for generating public & private key pair of students, and keeping the students' public keys at its database. For counting the votes we need another server, namely Tallier Server. This server is responsible for counting the validated votes, by using appropriate methods so that anonymity is also satisfied at the same time.

$$\text{Vote} = D(K_{Rt}, D(K_{Uv}, E(K_{Rv}, E(K_{Ut}, \text{Vote}_{user})))) \quad (1)$$

Technical details of the voting are depicted in Figure 2, whereas the model architecture is depicted in Figure 3. We used public-key algorithms for secure data transfer between the mobile phone and the servers, as shown in Equation 1. During the voting process, voting midlet encrypts the vote twice; first using tallier server's public key (K_{Ut}) and then using voter's own private key (K_{Rv}). After the encryption process, voting midlet creates a packet which includes the encrypted vote together with the voter's id, and later sends the packet to the validator server. Validator server extracts the voter identification number from the packet's header. It first searches the list of registered voters from its database. If it finds the student's identification number within the list, it further searches the voted users list until then. If a student's identification number doesn't exist in the voted users list, it decrypts the data using student's public key. If it can't find the student's identification number in the registered voters list or if it finds the identification number in the voted users list, it returns error message to midlet. Otherwise the vote needs to be added to the used vote list,

and hence validator server sends the decrypted data to Tallier server. Tallier server decrypts the data using its own private key (K_{Rt}) and increments the related candidate's vote count. After a successful final, tallier server notifies the validator server, and the validator server notifies the mobile about the successful final.

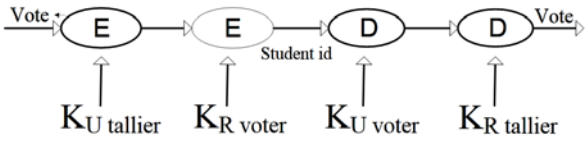

Figure 2. Vote Authentication and Counting Process

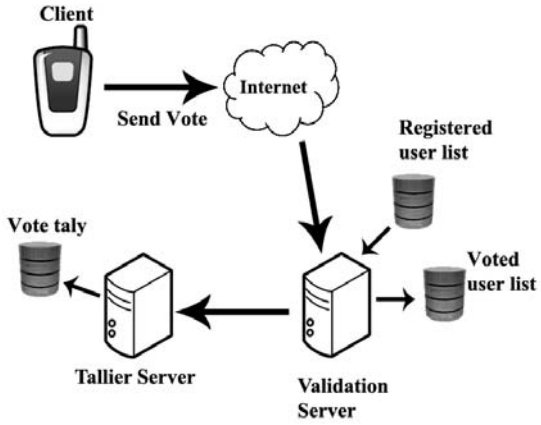

Figure 3. Model architecture

Students need to complete the registration process prior to voting. Registration process includes registering voters and installing the midlet together with the keys to the mobile phone. It involves face-to-face meeting of the voter with the registrar to determine eligible voters. For this purpose the eligible voter goes to voting registrar's office and shows her student identity card to registrar. Registrar verifies the identity of the student and generates a public-private key pair (K_{Uv}, K_{Rv}) which is unique for that specific voter. After the key pairs are generated, the registrar installs the private key of the voter together with public key of tallier server (that is only created once and stored by the registrar) to the student's mobile phone by conveniently using NFC. Public key of the voter (K_{Uv}) is saved on the validator server at this time. Validator server adds student's identification number to its list of registered user list during this process. Note that Registered User List will be used in voting process, as shown in Figure 3.

3.2 Voting Scenarios

NFC tags are to be prepared for each candidate. During this process, candidate's election id is to be integrated into the NFC tag, which possibly will be attached to a form that contains human readable candidate information. We propose three scenarios for student council voting. Each scenario provides different features and usage opportunities to voters. Each student can vote using any one of the scenarios in our model.

Voting Room Scenario (#1): In this scenario, voter should cast her vote inside the voting room. The room should be prepared accordingly prior to the voting. In the room stands may be used to include replaceable candidate information, papers, and candidate NFC tags. NFC tags are prepared by the registrar to include candidate information prior to the Election Day as described above. When a voter enters to the voting room, he approaches to the plastic stand and touches her phone to the tag of her favorite candidate. Then the processes described in the section 3.1 will occur.

Promotional Product Scenario (#2): In this scenario, the candidates may prepare promotional products (e.g. pencil, keychain) with their NFC tags attached. Within the election week, the candidates may reserve some period at the conference room to meet with the students. A 30 to 60 minutes period may be appropriate for this purpose. At the meeting candidate can talk about her plans about the next academic year to convince the voters. After this meeting, candidate distributes her promotional product to students. Students can vote by using this promotional product whenever and wherever they want, since NFC tags are already embedded into them. For example; when voter arrives home, he touches her phone to the NFC tag on the promotional product. And then the processes described in section 3.1 will occur.

Poster Scenario (#3): In this scenario each candidate prepares her poster together with the tags attached on it. During the election period candidates hang their posters to different places in university (e.g. cafeteria, gym). When a student sees a poster, she can vote making her phone close to the tag on the poster. As she touches the phone to the tag, the processes described in section 3.1 will occur.

4. Experiment

For the experimental purpose, a real-time environment is prepared for each of the three scenarios. To use as the test area for voting room scenario (#1), we prepared plastic stands (Figure 4) and candidate fliers. Stands included advertorial documents those contain candidate descriptive information. These stands are further placed into the voting room. Papers on the stands include the data such as candidate's photo, name and surname, student number, e-mail address, faculty, department, and class information. On the paper, a space is allocated for the NFC tag. For the promotional product scenario (#2), we prepared promotional pens with NFC tags attached. For the poster scenario (#3), we obtained posters, and onto the posters we have attached the NFC tags.

50 students (31 boys and 19 girls) have attended to the prototype testing. All attendees were university students who actually have voted in the previous web-based

student council election. Attendees were 19-26 years old. Since NFC is a rather new technology and most people did not know much about this technology, brief explanation of the NFC technology and how to vote using our model required 2 to 3 minutes. After the scenarios are explained, all students were requested to choose one of the three available scenarios and vote using that chosen scenario. After the voting is completed, the attendees were asked to fill out a survey to test the system's usability. This survey includes SUS survey of NFC-voting and web based voting to test the satisfaction, a subjective usability metric. SUS is formed by 10 questions, each of which is rated between 1 and 5, which contributes with its score value to the overall system usability. Items 1, 3, 5, 7, 9 are positive items and the score contribution of these items is scale position minus 1. Items 2, 4, 6, 8 and 10 are negative items and, score contribution of these items is 5 minus scale position. Then to calculate the overall value of SUS, total value of score contribution is multiplied by 2.5. Obtained SUS score ranges from 0 to 100. Higher score indicates higher usability.

Figure 4. Plastic stands

In addition to SUS, some additional questions are asked in the survey to receive information about participants and scenarios.

5. Results and Discussion

5.1 Results

Our survey consisted of two parts. The first part is about attendees and scenario selections. In [10], NFC technology's major intentions are listed as *simplicity* and *ease of use*. On the other hand a voting system must definitely preserve user's *anonymity*. Thus privacy and ease of use are considered as two primary factors in choosing a scenario. So we asked participants whether the criteria to choose their scenario were privacy or ease of use. After first part, the ease of use term is tested with SUS usability survey.

In the first part, *technology usage of attendees* is asked to students to learn the familiarity with technology. In Table 1 the distribution of the answers is presented. The distribution of chosen scenarios is presented in Table 2.

Table 1. Frequency of technology usage of attendees

Technology Usage	**Count**	**Percentage**
I try to use new technologies	33	66
I use new technologies when I need	11	22
I use new technologies when I have to	6	12

Table 2. Frequency of chosen scenario

Chosen Scenario	**Count**	**Percentage**
Voting Room	20	40
Promotional Product	11	22
Poster	19	38

60% of students those have chosen *Voting Room Scenario* stated their reason of scenario selection as *privacy*. All of the students those have chosen *Poster Scenario* and 73% of students those have chosen *Promotional Product Scenario* stated their reason of scenario selection as *ease of use*. The distribution of scenario selection reason is presented in Table 3.

We asked the planned place for voting to the students who have chosen promotional product scenario. Five students stated that they would vote anywhere; three students stated that he will vote at home, and three students stated that she will vote immediately after she gets the promotional product.

Table 3. Frequency of Scenario Selection

Scenario Selection Reason	**Privacy**		**Ease of Use**		**Other**	
	#	**%**	**#**	**%**	**#**	**%**
Voting Room	12	60	7	35	1	5
Promotional Product	3	27	8	73	0	0
Poster	0	0	19	100	0	0
Total	15	30	34	68	1	2

Table 4 shows the scores of the SUS survey. Figure 5 shows the overall SUS score of *web-based voting* and NFC-voting which is calculated by SUS survey's score. Overall SUS score of web-based voting is 78.50, and overall SUS score of NFC voting is 82.75.

5.2 Discussion

5.2.1 Survey Discussion

Figure 5 shows that NFC voting gained a higher usability than web based voting. We argue that the main reason for high usability of NFC voting may depend on the population who performed voting. These 50 students are university students and have high technology adaption as shown in Table 1. Also the sample size needs to be considered as an important factor to generalize the findings. It should be performed on a larger and homogeneous group of people to get more detailed findings.

Table 4. Scores of SUS Survey

Ratings and Scores of (*Web-based Voting* / NFC Voting)							
	5	**4**	**3**	**2**	**1**	**Average Score**	**Average Score Contribution**
Q1: System use	*28* / 35	*13* / 12	*2* / 1	*1* / 0	*6* / 2	*4.12* / 4.56	*3.12* / 3.56
Q2: Complexity	*5* / 1	*4* / 2	*2* / 3	*8* / 12	*31* / 32	*1.88* / 1.56	*3.12* / 3.44
Q3: Ease of use	*31* / 38	*10* / 6	*4* / 3	*3* / 0	*2* / 3	*4.30* / 4.52	*3.30* / 3.52
Q4: Need for support	*2* / 6	*7* / 3	*6* / 11	*8* / 7	*27* / 23	*1.98* / 2.24	*3.02* / 2.76
Q5: Integrity	*28* / 35	*10* / 10	*3* / 3	*4* / 1	*5* / 1	*4.04* / 4.54	*3.04* / 3.54
Q6: Inconsistency	*7* / 1	*4* / 4	*2* / 3	*8* / 4	*29* / 38	*2.04* / 1.52	*2.96* / 3.48
Q7: Ease of learning to use	*27* / 31	*11* / 5	*6* / 10	*3* / 2	*3* / 2	*4.12* / 4.22	*3.12* / 3.22
Q8: Cumbersome to use	*4* / 3	*1* / 1	*4* / 1	*6* / 6	*35* / 39	*1.66* / 1.46	*3.34* / 3.54
Q9: Confidence	*28* / 25	*15* / 15	*4* / 7	*0* / 0	*3* / 3	*4.30* / 4.18	*3.30* / 3.18
Q10 :Learning a lot of things to get going with system	*2* / 7	*5* / 2	*7* / 6	*9* / 11	*27* / 24	*1.92* / 2.14	*3.08* / 2.86
SUS Score:(Total Score Contribution * 2.5)							*78.50* / 82.75

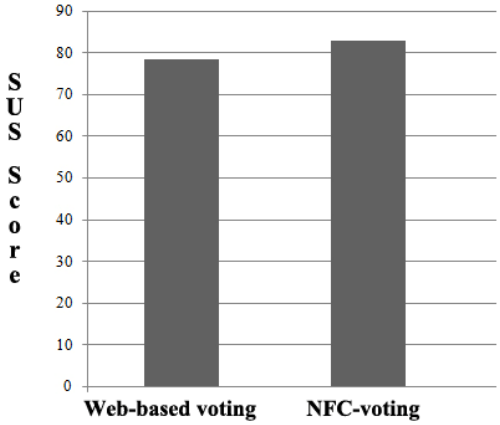

Figure 5. Overall SUS score

The three proposed scenarios differ in terms of ease of use and privacy. In this regard, the voting room scenario (#1) satisfies privacy better, but it definitely requires extra time for the voters to arrive a specific voting place, hence satisfying worse ease of use. So it is expected that voting room scenario would be mostly preferred when privacy is the main concern, and it should be less preferred in terms of ease of use. On the contrary, poster scenario satisfies ease of use better, however it does not satisfy privacy property, since anyone can see a voter's selection easily. Promotional product usage may satisfy privacy in various degree based on where and how the voting is performed using the product. If a voter votes in a private place such as home, it satisfies privacy; but if she votes in a public place, it may not satisfy. So if a participant has selected the poster scenario, she is not expected to have concerns about the privacy issue, rather she is expected to care about ease of use.

All participants those have chosen poster scenario stated their reason as ease of use. On the other hand, 60% of the participants who have chosen voting room scenario stated their reason as privacy. 73% of participants who have chosen promotional product scenario stated their reason as ease of use, 27% percent stated their reason as privacy. These findings suggest that people who go for ease of use may not consider privacy with high priority. On the other hand, those people who care about their privacy, ease of use may not be so much important for their selection.

For the usability testing, NFC-voting's SUS score gave a total value of 82.75, whereas web-based voting gave a score of 78.50. At the outset, NFC-voting has generally good usability than web-based voting. The fact that NFC-voting has a higher usability is not much surprising. It is developed to provide ease of use, but in the context of voting, NFC's usability is measured, and its high usability is attractive.

Analyzing some of the scores shows important results. The answer to the 2nd question shows that NFC-voting is less complex than web-based voting. The contribution of 3rd question shows that NFC-voting is easier to use. The result of the 6th question shows that people see less inconsistency in NFC-voting.

Questions 4, 7, and 9 can be analyzed as a group. The score of the 7th question meant that NFC model is easier to learn, 4th question meant that NFC model needs more support, and 9th question meant that voters feel less confident with NFC model. After a preliminary analysis, the results may be seen as conflicting, but it is not so. Although the people tend to apply NFC model easily, they are still suspicious about the potential problems that may occur because of immature new technologies, hence they assume that more support is required with NFC than web based known model. They also have less confidence to NFC for the same reason. But we may also comment on this, since as time passes and NFC technology becomes more recognized, and with the rise of NFC usage in daily

life, the usability score of NFC may grow up in the very close future.

From our findings we contend that the usability of NFC at the context of voting is high enough, and it will increase when NFC is used more frequently in our daily life. Overall we can evaluate that, NFC-voting satisfies the student voters in university environment.

5.2.2 Voting Requirements Discussion

Notice that we have listed six voting system requirements; namely accuracy, democracy, anonymity, verifiability, mobility, and usability in section 1. In this section, we will investigate whether these requirements are actually satisfied or not.

As also explained in section 3, a voter encrypts her vote first using the tallier server's public key, and then using her private key and further sends the encrypted data to the validator server. The validator server checks the incoming data to make sure that the voter is registered and haven't voted before. Then it forwards data to the tallier server. The tallier server decrypts the data with its own private key and records the vote, which is depicted in Figure 2. These processes prevent unauthorized users to vote and authorized users to vote more than once. So democracy requirements, namely *only eligible voters to vote* and *all eligible voters to vote only one time* are satisfied. This process also satisfies the *anonymity/privacy* requirement; a *ballot cannot be linked back to the voter who cast it.*

Also the *mobility* criterion is satisfied by enabling voting via mobile phones. Although there are some geographical constraints in voting room scenario and poster scenarios, promotional product scenario doesn't have any geographical constraints. A student can vote using the promotional product at her dormitory, home or wherever he wants.

In the contrary, *accuracy* and *verifiability* requirements couldn't be satisfied in our proposed system. In the future we will try to satisfy these properties and assess this systems objective usability.

5.2.3 Discussion on Related Work

In the context of voting, some usability studies are performed earlier. In [7] subjective usability together with objective usability of arrow ballot, bubble ballot, punch card, and lever machine are investigated, and it is found that bubble ballot provides higher subjective usability than the other three. In [9] the usability of DRE systems are investigated and it is found that only %10 of the voters have significant concerns. These studies investigated the usability of electronic voting systems but not remote electronic voting. On the other hand remote electronic voting is the only voting system that satisfies mobility requirement. It has the potential to increase users' satisfaction, but the usability of such systems isn't investigated. So our efforts to investigate the usability of remote electronic voting are a progress toward the goal, but there is still much work to done.

6. Conclusion

In this research we have presented a new type of a voting system, namely NFC voting, and evaluated its usability in a university environment. Our experience and the results of the usability test showed that NFC technology has a great potential to increase the usability of systems. With the rise of NFC-compatible mobile phones, it will bring new opportunities to easiness our lives. In the context of voting, NFC provided a practical and easy to use environment. But the privacy needs of elections should be considered, if it requires high privacy such as government elections or if a more easy-to-use environment is preferable such as a student council election.

Our study indicated that the requirements of electronic voting can be satisfied in NFC voting. Currently we satisfied democracy, anonymity, mobility, and usability criterion in our implementation. In the future extension of this research, we will try to satisfy the remaining accuracy and verifiability requirements of a secure electronic voting. We will also investigate NFC voting's objective usability tests in addition to subjective usability test on a more homogeneous group of people.

Acknowledgements

This study is supported by a grant from the ISIK University with the project number ISIKBAP 09A103. We also appreciate the help the students those have attended to the voting prototype.

References

[1] http://en.wikipedia.org, October 2009.

[2] A.E. Keshk, H.M. Abdul-Kader, Development of remotely secure E-voting system, *Proc. ITI 5th International Conf. on Information and Communications Technology*, Cairo, EGYPT, 2007, 235-243.

[3] L. Chun-Ta; H. Min-Shiang; L. Yan-Chi, A Verifiable Electronic Voting Scheme Over the Internet, *Proc. 6th International Conf. on Information Technology: New Generations*, Washington DC, USA, 2009, 449- 454.

[4] L.F. Cranor, R.K. Cytron, Sensus: A security-conscious electronic polling system for the Internet, *Proc. 30th Hawaii International Conf. on System Sciences*, Wailea, HI, USA, 1997, 561-570.

[5] I. Ray, I. Ray, N. Narasimhamurthi, An Anonymous Electronic Voting Protocol for Voting Over The Internet, *Proc. 3rd International Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems*, San Jose, CA, USA, 2001, 188-190.

[6] Industry Usability Reporting Project. (2001). Common industry format for usability test reports (ANSI/INCITS 354-2001).
[7] M.D. Byrne, K.K. Greene, S.P. Everett, Usability of Voting Systems: Baseline Data for Paper, Punch Cards, and Lever Machines, *Proc. Conf. on Human Factors in Computing Systems*, San Jose, CA, USA, 2007, 171-180.
[8] J. Brooke, SUS: A "quick and dirty" usability scale. In P. W. Jordan, B. Thomas, B. A. Weerdmeester & A. L. McClelland (Eds.), Usability Evaluation in Industry, 1996, 189-194.
[9] B.B. Bederson, B. Lee, R.M. Sherman, P.S. Herrnson, R.G. Niemi, Electronic voting system usability issues, *Proc. SIGCHI Conf. on Human factors in computing systems*, Florida, USA, 2003, 145 - 152
[10] http://www.nfc-forum.org/, October 2009.
[11] Ecma International, Near Field Communication - White Paper, 2005, Ecma/TC32-TG19/2005/012, http://www.ecma-international.org/
[12] M. Csapodi, A. Nagy, New applications for NFC devices, *Proc. 16th IST Mobile and Wireless Communications*, Budapest, HUNGARY, 2007, 245-249.
[13] E. Siira, J. Haikio, Experiences from near-field communication (NFC) in a meal service system, *Proc. 1st RFID Eurasia Conf.*, Istanbul, TURKEY, 2007, 273-278.
[14] J. Morak, V. Schwetz, D. Hayn, F. Fruhwald, G. Schreier, Electronic Data Capture Platform for Clinical Research based on Mobile Phones and Near Field Communication Technology, *Proc. 30th Annual International Conf. of the IEEE Engineering in Medicine and Biology Society*, Vancouver, CANADA, 2008, 5334-5337.
[15] S. Dominikus, M. Aigner, mCoupons: An Application for Near Field Communication (NFC), *Proc. 21st International Conf. on Advanced Networking and Applications Workshops/Symposia*, Niagara Falls, CANADA, 2007, 421-428.
[16] O. Falke, E. Rukzio, U. Dietz, P. Holleis, A. Schmidt, Mobile Services for Near Field Communication, *Technical Report LMU-MI-2007-1*, 2007, ISSN: 1862-5207.
[17] O. Rashid, P. Coulton, W. Bird, Using NFC to Support and Encourage Green Exercise, *Proc. 2nd International Conf. on Pervasive Computing Technologies for Healthcare*, Tampere, FINLAND, 2008, 203-206.