Mobile Ticket Control System with RFID Cards for Administering Annual Secret Elections of University Committees

Hans Weghorn
BA-University of Cooperative Education
Rotebühlplatz 41, 70178 Stuttgart, Germany
E-mail: weghorn@ba-stuttgart.de, http://hansweghorn.org

Hans Peter Großmann, Dieter Hellwig, Cahya Kusuma Ratih, Andreas Schmeiser and Heiko Hutschenreiter
University of Ulm, Albert-Einstein-Allee 43, 89081 Ulm, Germany
E-mail: hans-peter.grossmann@uni-ulm.de, http://omi.e-technik.uni-ulm.de

Keywords: ubiquitous computing, RFID, NFC, mobile aplications, wreless JAVA

Received: April 23, 2007

RFID technology often is suspected to provide means of undesired surveillance and observation of people in their roles, e.g., as private persons, customers of any business or employees. Here, an opposite scope of application sample shows how such technology based on intelligent smart cards can help improving secrecy in a sensitive environment. The annual election runs for the representatives of the studentship of Ulm University have to be operated in a way that it cannot be tracked, who is electing how often. On the other hand, it has to be ensured that voting is not abused, hence some entrance check is obligatory. The technical solution presented here is using a prototype mobile phone, which is equipped with a communication module for contact-less information exchange with the student ID. In addition to ensuring confidentiality, with this mobile vote administration system the studentship of Ulm University has the opportunity of enhancing the operation of the election, because the election office is also mobile now and not fixed to any location in the University buildings. This enables that the election assistants go out for the students instead of waiting for them to come, and by that, the poll is likely to be increased.

Povzetek: Razvita je metoda za preverjanje pri volitvah, temelječa na RFID.

1 Introduction

Today, RFID tags are applied in many fields of daily life. For instance, clothes in department stores may be marked with such electronic tags intending different aims: On the one hand side, these tools may simplify purchase and payment, on the other hand stealing of goods may be prevented by electronic supervision of exit doors. The latter aspect leads to the part of RFID technology, which is in general feasible for tracing and observing people. And of course, there exist well-funded concerns of people against such scenarios which remind us of George Orwell's famous novel "1984".

Especially considering the technical weaknesses of radio monitoring systems [1], these concerns appear quite reasonable. Overall, the question arises whether everything which is technically possible should be implemented, and what kind of impacts radio monitoring constructions will have on societies [2].

Despite this all, it also has to be respected that in many environments access control is required and unavoidable. For instance, protecting buildings, offices, or private property against unauthorized access can be performed with electronic systems in a quite convenient and efficient manner. Such a sample system is an electronic ID card of our University students: In Ulm University environment, a smart card is used as student ID. It is a MIFARE® classic card that is distributed by the company Philips [3]; its capabilities are an extension of the RF communication standard ISO 14443A. This communication standard often also is called Near Field Communication (NFC), because the RFID reader and the card have to be in maximum distance of 10 cm. Our specific Mifare® card contains 1 kbyte of E^2PROM memory that is sectorized, and for each data sector there can be different access rights and keys defined, which are independent of the other data sectors.

In its storage system, the card holds the matriculation number of the student, the access number for library services, and other information in terms of read-write byte arrays. Another possibility is using a data block on the card as counter value. The counter can be configured for an access with two distinct secret keys: One key enables setting the counter value, while the other access key is good only for reading and decrementing the counter. With this, electronic payment functions [4] will be realized in near future: The loading of the counter – i.e. booking money onto the card – is done with the "better" key, and this is used only in a specially protected environment. Discharging the account is not as sensitive,

and there is no risk of imposture by leaving the other – weaker – key in electronic cash boxes, or in public terminals for inspecting the account balance and last transactions in this electronic wallet.

Figure 1: Student ID card of Ulm University, and prototype phone equipped with RFID communication hardware.

This specially shielded counter system on the student ID cards was also already used since several years as entry ticket for the elections of the studentship's representatives, because this application is equivalent to money payment scenarios: With each re-matriculation (Fig. 2), the students earn the right to vote for their representatives during the new semester. Since there may be several elections in the same semester, an initial high counter value is decremented with each vote. The start counter value is increased with each studying year by a big stepping count, so there is a clear distinction between the different years (there have to be never more than this count of elections in the same year). The counter is loaded on the student ID in an electronic administration terminal accordingly. Up to now, the counter was read and decremented in the election office with a desktop computer with special RF communication equipment and software.

Overall, this construction represents a closed system, and the students can rely on the fact that it is not traced in any database, how often they vote, or whether they vote at all. Ensuring confidentiality is a very important issue for making the students to contribute their vote. The stationary computers in the election office may feed the suspect that the voting could be traceable, because these are easily connected to the Intranet and by that to the administration database of the University. Therefore, a mobile control system should help diminishing this concern. For this, a prototype cellular phone was supplied in the frame of an industrial cooperation (Fig. 1) [5], which is equipped with an additional RF hardware for communicating with the student ID. The following sections discuss the implementation and operational aspects, which are required for constructing mobile software for the election office.

Another important positive effect of using a mobile system for the vote control is that the students do not have to come any more actively to an office, which is located in one single building of a widely distributed campus. The election office is made movable itself, and it can be placed to efficiently meet many students, e.g., after courses in big lecturing halls. Due to this improvement, the turnout at the election, which is traditionally low for different reasons, is presumed to increase in future.

2 Data representation and data handling on the student ID card

The student ID card contains one kilobyte of EEPROM memory, which is split into 64 blocks [3]. Four blocks are always clustered in one sector, while the last block in each cluster defines the access rights and cryptographic access keys for the entire sector. The data blocks can be used either as flat memory of 16 bytes size, or as 32 bit counter value [6]. In the latter case, the counter value is replicated within its block two times for security reasons and for enabling consistency checking. For controlling access to the elections of the studentship's representatives, one dedicate block on our student ID card was defined as containing a counter value. On base of this data entry, it can be decided whether a student is allowed to apply a vote or not. For better understanding of the functionality and its requirements, it has to be noted that the number of election runs are varying each year, and in general, there will be several elections. This control system was introduced in year y_b, and the counter is reloaded each year with the first re-matriculation of the student, which is obligatory in each semester, with a new value c_r:

$$c_r = (y - y_b + 1) \cdot s$$

y denotes the actual year
y_b denotes the year of the introduction of this system
s denotes a stepping factor that is larger than the maximum number of elections in each year

When the student applies a vote during the election this counter value on his/her ID card is in first approximation decremented by one. After the n-th election the counter will carry the following target value t:

$$t = (y - y_b + 1) \cdot s - n$$

An entry control system for the votes now has to compare the target value t calculated for the current run with the counter value c on the ID card. From this, a decision can be applied:

$c > t \Rightarrow$ Vote is allowed

$c = t \Rightarrow$ Already voted, i.e. vote is not allowed

$c < t \Rightarrow$ Re-matriculation not yet performed – has to be completed first

During each election, the same person may only apply one single vote, even if there was no participation in elections that took place earlier in the same year. Therefore, in the true control system the counter value is not simply decremented during each vote, but it is always set to the target value as defined above (performed by iterative decrementing). This ensures that only one single

vote can be applied in each run. The reloading of the counter is tracked in the administration system, so that a second re-matriculation will not reset the counter. On the other hand, the counter on the card itself is not tracked and also not stored in any central database or administration system of the University. Hence, this construction represents a closed system, and it cannot be observed from outside, how often a student attends the elections, or whether the student votes at all.

Figure 2: One of the public terminals at Ulm University, where students can re-matriculate with their ID and perform other administration tasks, e.g., updating their home address or printing out certificates of exams.

For security reasons, precise values of the above-defined parameters are not documented here. The ID card also contains couple of additional information, like registration number for the studying course and lending code for the University library. These additional data contents are not relevant here, and the different access keys for the different data sectors on the ID card prevents interference between data handling of the different instances of administration that are indeed required for operating a University system. The different access keys shield the different application against each other, and make these all perpendicular.

Up to now, the election entry control was performed with stationary desktop computers that are equipped with NFC readers / writers. This control system shall be miniaturized and made moveable by using mobile terminals instead of desktop computers. For NFC experiments the company Siemens / BenQ Mobile supplied few prototype mobile phones, which are equipped with NFC communication hardware in addition to their normal functionality (Fig. 1). These devices were used for the implementation of the application described in the following sections.

3 System construction and its operational behaviour

3.1 Start up of election control tool

For simplicity and convenience of handling, the election tool was automated as much as possible. After displaying a welcome screen, which disappears automatically after a short delay, the user has to enter a PIN code (Fig. 3).

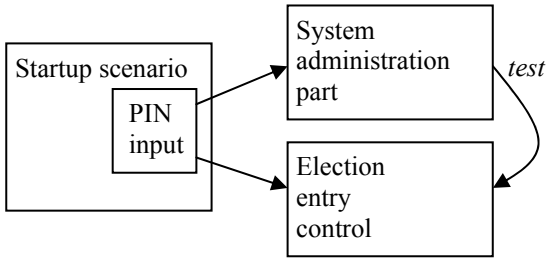

Figure 3: The election tool is structured into three parts, each of which is realized as finite state machine (FSM). Depending on the entered PIN code, the SW branches from the start-up scenario either to the system administrator part, or to the regular operational mode, which is using the system as entry check for the elections.

The system contains two valid PIN codes, one for the system administrator, and another one for the vote assistant. Hence, after entering the PIN code, the application automatically can branch to the required operational scenario and by that, one selection menu is saved. Of course, all error cases – at this stage entering an invalid or no code – are treated also separately. After installation of the vote software on the device, a default PIN for the system administrator is generated internally. The election control, which is considered being the regular use case, cannot be launched until all required system parameters are entered by the system administrator.

3.2 System administration

In the system administration scenario, the administrator of the tool has to enter the following information into the system:

- System administrator PIN
- Vote administrator PIN
- Date period for election run
- Running number for the election in the actual year
- Secret access key for the ID card
- Timeout values for card scans and sensitive menus

For testing purposes, the system administrator can read the election counter on the card. With this, it can be verified that the configured secret key is valid. Also for system testing, the vote assistant software can be launched directly from the system administration menu.

3.3 Vote control

After displaying a timed welcome screen for the vote administrator, the system switches to an input screen, from which a card scan can be launched by one single key press (Fig. 4). After detecting a card, and reading the counter value (and if appropriate decrementing it) one of the possible results is displayed. The student, who wishes to vote, may be granted or rejected, or this student may

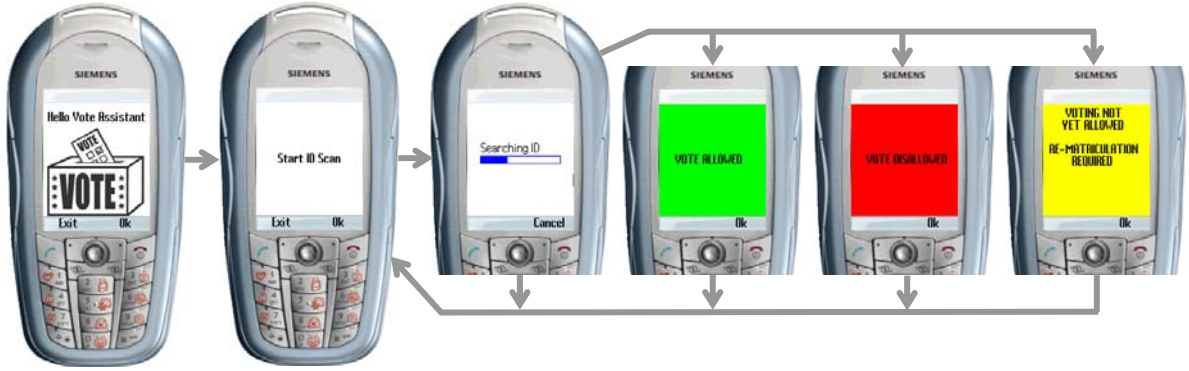

Figure 4: UI chart for the vote control system without the error screens. After scanning the card, the result is displayed with indicative coloured screens.

be required to re-matriculate first. A card scanning problem or time-outs represent the possible irregular cases. The vote administrator has to acknowledge the result screen, and then the system returns to the screen, from where a card scan can be initiated again. In the regular case, the vote administrator has to apply for each ID control two manual button presses – one for starting the scan, and a second one for acknowledging the result. The scanning of the ID card could theoretically be started automatically, but this is not recommendable because the card search consumes high power. Hence, the manual start of the card scanning will help to extend the operational stand-by time of the device.

3.4 Aspects of technical implementation

The software was realized in wireless JAVA [7], which offers convenient and adequate programming functionality for SW that shall be executed on mobile phones. In wireless JAVA, the standard UI provides the possibility to constrain input in text fields with certain properties. In particular, the input field for passwords can be masked automatically, and the char set for input can be limited, e.g., to decimal digits only. With this kind of control, the extend of error checking code for wrong input is reduced considerably. Another special standard UI element is the class DateField, which allows the user to comfortably enter the required information (Fig. 5). Overall, wireless JAVA offers a UI concept that is fully appropriate for small devices [8], which are constraint in terms of screen size and keyboard char set.

On the prototype phone, the internal communication with the NFC hardware is performed through a serial connection, which also can be handled by standard library functions of wireless JAVA. The election tool is structured in two parts: The application layer, which takes care of user inputs and treatment of execution parameters, and a connection library that handles the communication with the ID card. Both layers are active in general simultaneously, and hence multi-threading was used to serve this requirement of parallel processing.

Multi-threading [9] represents one important standard language feature of Java that provides advantage over alternative programming languages like C or C++. For a communication with smart ID cards there exist already a library specification for wireless Java [10], which has the identification JSR-257, and a preliminary library implementation was available for the prototype phone. Unfortunately, this library specification completely disregards the most advantageous features like using cryptographic keys for data exchange or like accessing the card's built-in counter functionality. Instead, JSR-257 treats the ID card as streaming medium, and since this is inappropriate for the given data structures on our student ID card, an own card access library had to be developed.

Figure 5: Wireless Java provides standard UI elements for simplified application programming. The samples here show how password input can be masked automatically, and how comfortable the input of date information can be.

The software metrics of the developed system shall here be described in terms of number of code lines, UI screens, and total count of states of the FSMs. Approximately 20 different UI screens are contained in the complete application, while 20% of them represent error messages and confirmation screens. The display language can be switched by an internal constant between English and German, and hence the string resources had to be implemented for all the screens and messages for both cases. The application layer consists of 1200 lines of code (without comments), and handles 30

different system states. The number of states is higher than the number of UI screens, because the same UI screens can be reused in different states. Two threads are required in the application layer – one for handling UI events, and the second one for cycling through the FSMs –, while the connection library, which consists of 600 lines of code, requires only one background thread that handles the communication via serial interface with the NFC hardware module. Since the latter communication is time-critical, this connection library thread runs with increased priority

For didactic reasons, the above sections show only the relevant core part of the ticket control application, which consists of a few UI screens only. For a complete fault-tolerant tool, which is robust against wrong handling – which is usually unintended – and error cases like mal-functional cards, an extended software construction is required. This can be seen from the numbers of the before discussed software metrics in contradiction to the limited functionality of the inner

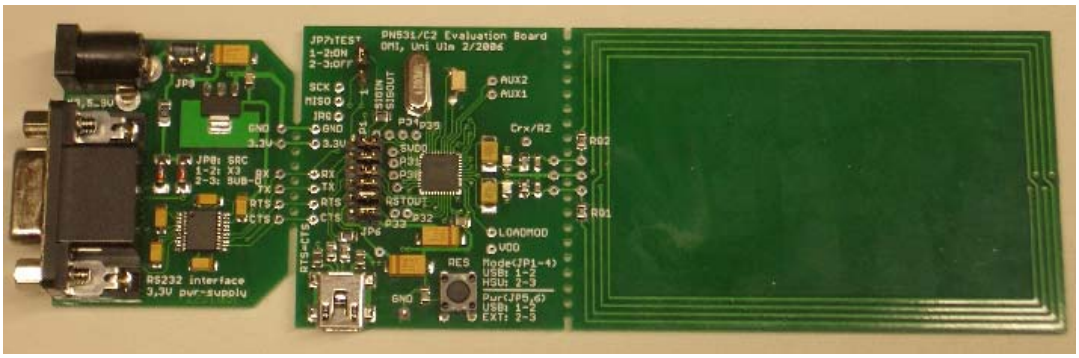

Figure 6: PCB with electronic RF circuit and on-board antenna that was developed at Ulm University. This first prototype design is equipped with USB and RS232 communication interface, so that it can be connected to different host systems (e.g., recent PDAs have today micro USB interfaces). Further designs of this will have to be adapted to dedicate handheld devices in use, and it will also be considerably more miniaturized for this purpose.

4 Data security and protection against abuse of system

For preventing abuse of the system, a variety of security features were built into the software:

❶ After installation, the tool can only be launched with a default PIN, and before the software can be used for scanning an ID card, all parameters defined above have to be entered by the administrator.

❷ One important aspect is that the secret access key for the ID card is crypted in persistent storage area on the device (part of the phone's FLASH memory). The concept is to use the vote assistant PIN as starting value for a binary noise polynomial [11], which is used for ciphering the secret card key.

❸ The PIN value itself is not preserved on the system; instead a hash value [12] derived from the PIN is saved in the FLASH memory, so that the entry to the voting software can be verified, but without entering the correct PIN it is impossible to derive the value of the secret card access even at infinite efforts of HW and SW debugging.

❹ An implicit protection is already available with the construction of the ID card itself, because the used key is only feasible for reading and decrementing the election counter on the card. Hence, even if the secret access key could be extracted, the counter value could not be modified in a way that the ID owner is allowed to vote more than once in each election run.

❺ Another approach of protection is that sensitive menus of the application are equipped with timer "good" branch (Fig .4).

functionality: If the administration software or the vote assistant software is started successfully, but it is not used for certain defined time (this duration can be configured by the administrator), the application exits automatically. This ensures that even if the system is stolen, when an authorized person has logged on already, the tool will terminate after a while.

❻ Furthermore, for preventing any abuse, the vote assistant software works only during the specified date frame of the election run. Before and after these dates, the software cannot be launched with the vote assistant's PIN code at all.

❼ To preserve secrecy, the actual counter value on the ID cannot be displayed in the voting control scenario. Only the system administrator can inspect from his menu the vote counter, but this possibility is required for validation of the cryptographic key and error detection in the voting system itself. During the election runs, the system administrator is not acting as vote administrator, but s/he is only in charge of technical support during this time.

5 Actual and future developments

In parallel to the plain software work with the RFID phone, we have also developed an own communication hardware, which is software-compatible to the NFC interface used in the prototype phone. This hardware (Fig. 6) is more versatile, because it can be connected via either USB or RS232 interface. Hence, this communication device can be attached electrically to standard desktop computers as well as to handheld computers, or smart phones. Several samples of this own

hardware have been manufactured manually, and the design could successfully be verified already.

Comparative software investigations with this new PCB already unveiled a severe firmware bug in the prototype phones. Unfortunately, exactly this firmware bug in the RFID communication module prevents that at the moment, that the outlined security concepts can be used to their full extend.

Future use of this PCB design will be in connection to very simple handheld computers, which do not have any else communication interface like wireless phone network access or WLAN. This shall yield higher confidence in the secrecy of the election entry control. This hardware design will add benefits to the project in different ways: At first, it will allow us becoming manufacturer-independent, and secondly it will enable using cheaper consumer devices for this application. Furthermore, at the moment this RFID circuit is adapted to replace the faulty RFID communication module in the prototype phones. The software written so far is adapted specifically to the properties of the used prototype phone. For using in future alternative devices, the software will have to be extended in terms of dynamically handling screen sizes, and possibilities for persistent data storage.

6 Conclusion

A concept for an appropriate ticket system for the elections of representatives of the studentship in Ulm University was developed. The system provides secrecy for the voting action, and the concept prevents an abuse of voting. With the development and implementation of software for a prototype mobile phone that is equipped with an additional NFC communication module besides its standard hardware, the vote ticket control itself is made mobile. The advantages of this approach are obvious: By enabling easily movable control tools, the election can be operated in decentralized manner, and by that the poll is presumed to be increased.

As outlined, the vote control represents an embedded closed system. Due to RFID communication with the intelligent smart card, the application can run entirely in local mode. It is not required for the application to interact with University's administration system or database, and hence this application shows how RFID technology can help improving privacy and secrecy.

Meanwhile two dozen NFC-enabled phones were provided by our industrial partner for a use in the project. Unfortunately, it turned out that the NFC communication subsystem in these phones contain firmware errors, so these devices cannot be used in the safest mode like described above. Therefore, at the moment we are developing our own communication hardware module for these phones to fix this problem by replacing the faulty hardware. After achieving this, the next election run shall take advantage of this new technology.

Furthermore, with the own hardware the number of devices and the handling in the election scenario can be improved additionally. This NFC technology can be applied for wider purposes during the operation of our studying courses, for instance using the NFC-enabled devices as presence control in examinations, or entering marks and results in laboratory exercises and oral examinations through the handheld scanning device [5].

Acknowledgement

We want to thank the companies Siemens AG, Munich, and BenQ Mobile GmbH, Munich, for their kind hardware and software support, and for providing the set of prototype RFID phones.

References

[1] Molnar, D., and Wagner, D. (2004) Privacy and security in library RFID: issues, practices, and architectures. *Proceedings of the 11th ACM conference on computer and communications security*. Washington DC, USA, pp. 210--219.

[2] Hugl, U. (2005) Employment of upcoming technologies and aspects of privacy. *Proceedings of the IADIS conference on e-Society.* Qwara, Malta, pp. 333--339.

[3] Philips (2006) *MIFARE Classic - contactless Smart Card ICs*, http://www.semiconductors.philips.com/products/identification/mifare/classic, last access: March 2007.

[4] Stokłosa, J. (1998) Cryptography and electronic payment systems, *Informatica. An International Journal of Computing and Informatics*, vol. 22, no. 1, pp. 29--33.

[5] Weghorn, H, Schmeiser, A., Großmann, H. P., Pirker, M., and Haubold, S. (2005) ISA4G - Integrated Student Access ID Card of Fourth Generation, *Proceedings of the IADIS Conference on WWW/Internet*, Isaias, P., and Nunes, M. B. (Eds.), Lisbon, pp. 333--337

[6] Philips, 2001, *MIFARE Standard Card IC MF1 IC S50 Functional Specification*, Revision 5.1, http://www.semiconductors.philips.com/acrobat_download/other/identification/m001051.pdf, last access: March 2007.

[7] Knudsen, J., and Li, S. (2005) *Beginning J2ME: From Novice to Professional.* Apress, Berkeley.

[8] Mahmoud, Q. H. (2002) *Learning Wireless JAVA.* O'Reilly. Sebastopol, 1st edition.

[9] Bell, D., and Parr, M. (2002) *JAVA for Students.* Prentice Hall. Dorchester, 3rd edition.

[10] JCP (Java Community Process) (2005) *JSR-00025 Contactles Communication API*, Version 2.6, http://www.jcp.org/aboutJava/communityprocess/edr/jsr257, last access: March 2006.

[11] Rorabaugh, C. B. (2004) *Simulating Wireless Communication Systems.* Prentice Hall PTR, Indianapolis.

[12] Reeds, J. A., and Weinberger, P. J. (1984) File Security and the UNIX Crypt Command. *AT&T Bell Laboratories Technical Journa*l, Vol. 63, No. 8, pp 1673-1684.