Smart Cards in Electronic Voting: Lessons Learned from Applications in Legally-Binding Elections and Approaches Proposed in Scientific Papers

Jurlind Budurushi, Stephan Neumann and Melanie Volkamer

Fachbereich Informatik – „SecUSo“
CASED / Technische Universität Darmstadt
Hochschulstraße 10
64289 Darmstadt, Germany
{name.surname}@cased.de

Abstract: Recently, the interest in electronic voting has increased as more and more states have started to implement such systems. At the same time, classical national ID cards are often being replaced by national electronic ID cards which enable citizens to securely identify and authenticate themselves over the Internet. Despite their popularity, the possibility of using eID cards for e-voting has not been adequately studied. This work surveys e-voting systems in which smart cards were used or were proposed to be used to support the voting process. We consider all types of smart cards, including those only for use in e-voting as well as existing and future national eID cards. In a two-step process, we will analyze the most interesting, real-world applications and proposals from a security, usability, and cost perspective, allowing us to derive our lessons learned. Upon these lessons, we show that the restricted-ID mechanism as implemented in the German eID card serves as an interesting basis for the integration of eID cards in e-voting. We outline that the risk of a “forced-abstention” attack can be mitigated by using the restricted-ID.

1 Introduction

Recently, the interest in electronic voting (e-voting) has increased, and many states are pushing for their use in legally binding elections. At the same time, states are adopting national eID cards, which provide a very secure way to identify and authenticate users over the Internet and thus allow citizens to interact with public authorities or private companies from their homes, even if they live abroad.

In e-voting, voter identification and authentication plays an important role in ensuring that only eligible voters may cast a vote, that those voters only cast a vote once, and that eligible voters are not prevented from voting. Therefore, using eIDs for voter identification and authentication in e-voting has a promising future in the field.
As smart cards like eIDs are no longer only used for the purpose of identification and authentication but also for storing sensitive information and securely processing some

parts of cryptographic protocols including signing and encrypting, these functionalities can also be used (and have also been used and proposed to be used) to increase the security of e-voting systems.

Since there are already real-world e-voting systems and approaches proposed in scientific papers which rely on or propose the usage of smart cards in different ways, the goal of this paper is to evaluate these systems and approaches in order to produce a list of lessons learned for future applications of existing eIDs as well as for future eIDs to better support existing and future electronic voting schemes.

Therefore, we will analyse the use of smart cards in the university elections in Austria, the national elections in Finland and Estonia, and the D21 election in Germany. Furthermore, we will evaluate scientific proposals including the application of the European Citizen Card, the German eID, and two scientific papers proposing additional functionalities for smart cards used in e-voting, namely the Votescript+ and Votinbox e-voting schemes.

Our lessons learned are manifold: Generally, legally binding elections should not use arbitrary smart cards but rather eID cards with which voters are familiar and which mitigate the risk of vote-selling significantly. In addition, we learned that there are no more secure alternatives to integrate current eIDs with very limited functionality (like the eID used in Austria and Estonia) as implemented in the corresponding systems. We concluded from the e-voting schemes Votescript+ and Votinbox that it is very important to find an adequate trade-off between necessary functionality, which increases the security of the overall e-voting system, and too much functionality, which increases the risk of vulnerabilities to the eID itself. We were able to point out that the idea presented in [BKG11] has the potential to improve the security of electronic voting in regards to coercion resistance. The Restricted-ID mechanism mitigates the risk of “forced-abstention” attacks against “less powerful” attackers, i.e., attackers who observe public channels and the Bulletin Board but are not able to break the used cryptographic protocols.

The remainder of the paper is structured as follows: section 2 gives a general overview of smart cards and a short list of smart card types we take into consideration. Section 3 describes real-world e-voting systems, defines appropriate evaluation criteria, and analyses these systems with respect to the proposed criteria. In section 4, we describe and analyse different scientific approaches that use smart cards that offer more functionality than the national eID cards, which have been used in current real-world e-voting systems. Section 5 summarizes the lessons learned and concludes with our contribution.

2 Smart Cards

According to [ISO7816] smart cards are plastic cards with embedded, integrated circuits and similar in size to today's payment cards. They can be used as an access-control device, making personal and business data available only to the appropriate users. Smart cards provide data portability and are designed from the ground up to be a secure system component [Ab02]. There are three different categories of smart cards according to [RE03]: integrated circuit (IC) memory cards, IC optical memory cards, and IC microprocessor cards. An IC memory card simply stores data in a secure manner. IC optical memory cards are the same as IC memory cards but have more memory capacity. An IC microprocessor card, on the other hand, can process, i.e., add, delete, or manipulate, information in the memory of the card, allowing for a variety of applications and dynamic read/write capabilities.

Smart cards are used in e-voting schemes to securely identify and authenticate voters as well as to secure the actual e-voting scheme including, signing and encrypting messages and/or votes. Usually e-voting schemes use IC microprocessor cards because they are based on cryptographic protocols and primitives. Thus, when we refer to smart cards in this paper, we are referring to IC microprocessor cards.

We consider different types of smart cards such as the one designed exclusively for e-voting, digital signature cards, the Java Card [1], the European Citizen Card (ECC), and several national eID cards, namely the Austrian, Estonian, and German eID card.

3 Systems in Use

In this section we first describe and then analyze four real-world e-voting systems using smart cards. Afterwards we define evaluation criteria, which we then use to analyse the described e-voting systems. We take both e-voting systems conducted at polling stations as well as remote e-voting into consideration. In focusing on the provided functionalities and usage of the smart cards, we chose not to focus on the parts of the system that are irrelevant to our investigation.

3.1 Remote E-voting in Austria

In 2003, remote e-voting was introduced in Austria by the research group E-Voting.at [Pr03] as a test election in conjunction with the Austrian Student Union elections at Vienna University of Economics and Business (WU Vienna). In 2004, they carried out a test election for the students at the WU Vienna during the Federal Presidential elections [Pr04] and in 2006 for Austrians abroad [PS06]. In 2009, remote e-voting was used for legally binding elections of the Austrian Student Union [Kr10]. This time a system

[1] http://www.oracle.com/technetwork/java/javame/javacard/overview/getstarted/index.html (15.02.2012)

provided by Scytl [2] was used. Remote e-voting was offered as an additional channel. Each eligible voter in possession of an Austrian citizen card [3] was able to vote over the Internet.

In accordance with §63 of [HSWO05], the Austrian citizen card has to be used to identify and authenticate voters over the Internet. The voter needs to know two PIN codes associated with his or her citizen card: PIN1 for secure electronic identification and authentication and PIN2 for using a qualified electronic signature. On an abstract level, the remote e-voting scheme works in the following way: in the first step, the voter selects the university where he or she wants to cast a vote. The voter then enters PIN1 for identification and authentication. He is then required to enter PIN2 and digitally sign his electoral registration data, thus authenticating and confirming his or her identity. The voting server checks the voter's right to vote based on the signature and the corresponding certificate and displays the corresponding ballot to the voter. Once a selection is made, the vote is encrypted by the client-side voting software. In order to cast the vote, the voter enters PIN2 again, thus signing the hash value of the encrypted vote. Afterwards, the encrypted vote and the signature are sent to the voting server.

3.2 Remote E-voting in Estonia

In Estonia, remote e-voting was first introduced for legally binding elections during the 2005 local elections and carried out again in the parliamentary elections in 2007, the 2009 European Parliament and local elections, and the parliamentary elections in 2011 [TV11, ODIHR11]. Remote e-voting was offered as an additional voting channel. Each eligible voter in possession of an ID card [4] was able to vote using remote e-voting: vote updating was enabled.

The Estonian ID card is used to identify and authenticate voters over the Internet. The voter needs to know two PIN codes associated with his ID card: PIN1 for secure electronic identification and authentication and PIN2 for using a qualified electronic signature [ODIHR11]. On an abstract level, the remote e-voting scheme works in the following way: the voter identifies and authenticates him- or herself by entering PIN1. The e-voting system checks the voter's identity and the voter’s right to vote. The voter is then provided with the corresponding ballot upon successful authentication. After having made a choice, the vote is encrypted. In order to cast the vote, the voter enters PIN2, which enables the ID to digitally sign the hash value of the encrypted vote. Once signed, the encrypted vote is sent to the voting server.

[2] http://www.scytl.com/ (15.02.2012)

[3] http://www.buergerkarte.at/ (15.02.2012)

[4] Statistics of issuing the ID card: http://www.id.ee/pages.php/03020504 (15.02.2012)

3.3 Remote E-voting for the Initiative D21 Elections

In 2003, Initiative D21 [5] was the first registered association in Germany to carry out a legally binding board election using remote e-voting. The remote e-voting system used was POLYAS [6]. Every D21 member received a PIN-protected digital signature card using a qualified electronic signature and was able to vote using remote e-voting.

In order to activate their digital signature card the voters filled out a form and sent this via fax, along with a copy of their identity card. Once voters received a confirmation email, they were able to start the voting process. On an abstract level, the remote e-voting scheme works in the following way: the voter identifies and authenticates by entering his PIN, in order to digitally sign a challenge. The e-voting system verifies the voter's identity and his right to vote by matching the voter's advanced electronic signature and email address with the one stored on the registration server. The voter then gets a random voting token, which is used to proceed with the vote casting process anonymously. Once marked, the vote is sent to the ballot box server together with the random voting token, while the transmission is secured by server side SSL.

3.4 E-voting at Polling Stations in Finland

For the 2008 municipal elections in Finland, Finnish authorities were able to arrange e-voting in three municipalities. The e-voting system in use was provided by the TietoEnator [7] company [TE08]. E-voting was offered as an additional channel and took place at polling stations. Each eligible voter who had an election-specific smart card was able to vote electronically.

After manually confirming the voter's eligibility to vote (just the same as the traditional system), the election official configures an election-specific smart card and hands the card to the voter. The voter enables the e-voting system by inserting the smart card into the card reader. The e-voting system verifies the voter's right to vote and displays the corresponding ballot to the voter. Once the ballot is marked, the vote is encrypted by the e-voting system. The e-voting system also signs a hash value, which is derived from the encrypted vote, a random number, the voter login ID, and the election ID. The encrypted vote and the signed hash value are sent to the voting server. The voter returns the smart card to the election official, which is not used anymore in the election [KM08].

[5] D21 is a non-profit organization established in Berlin. It is Germany's largest partnership of government and industry in the information age For more information see http://www.initiatived21.de/ (15.02.2012)

[6] http://www.polyas.de/ (15.02.2012)

[7] http://www.tieto.com/ (15.02.2012)

3.5 Evaluation Criteria

In this section, we define several criteria upon which we analyze the e-voting systems described above with respect to the functionalities and usage of the smart cards [8]. The criteria are divided into three different groups: security, usability, and costs. The list of criteria used in this paper is not exhaustive, but we have chosen the same criteria used in [Vo09]:

1. Secrecy: Our definition of secrecy comprises vote-selling, secrecy of the vote, and long-term secrecy.
2. Usability: We define usability as ease of use and user-friendliness.
3. Costs: The cost factor is very important for e-voting systems, as the number of participants tends to be very high. We define costs as the total of costs for smart card readers and for smart cards.

However, before implementing e-voting systems that use smart cards, other criteria need to be taken into account as well, like robustness, time required for vote-tallying, performance, and other security requirements. Note that these criteria were defined with respect to smart cards used only for identification and authentication purposes.

3.6 System Analysis

In this section, we analyze the e-voting systems described in the previous sections by the criteria defined in section 3.5. The result of this evaluation is summarized in Table 1.

System in Use	**Secrecy**	**Usability**	**Costs**
Austria	+ Vote selling: the card will not be lightly passed on to a vote buyer, since this automatically means that all the other applications of this card are passed on as well	+ User-friendliness: use of the card for identification/authentication is known from other areas	+ Cost for smart cards: no extra costs, as voter already owns a card
	- Long-term secrecy: *Sig*[Hash*(*Enc(Vote))], even if the authorities are honest, the problem of long-term secrecy still remains	- Ease of use: the voter has to enter the PINs multiple times—–PIN1 once and PIN2 twice.	- Costs for smart card readers: the costs of a card reader remains, if the voter does not yet possess such a device

[8] We refrain from considering integrity in this analysis as this is not addressed by smart cards.

Estonia	+ Vote selling: for the same reasons as in Austria’s case - Long-term secrecy: for the same reasons as in Austria’s case	+ User-friendliness: for the same reasons as in Austria’s case - Ease of use: the voter has to enter two PINs	+ Cost for smart cards: for the same reasons as in Austria’s case - Costs for smart card readers: for the same reasons as in Austria’s case
D21	- Vote selling: in contrast to Austria/Estonia, the voter can easily sell the voting card or just the random voting token.	- User-friendliness: the voter must first learn how to use a smart card and a card reader if he or she hasn't used one before - Ease of use: the identification/authentication process of voters takes a long period of time	- Cost for smart cards: extra cost for the digital signature cards - Costs for smart card readers: extra costs for the card readers
Finland	- Vote selling: for the same reasons as in the case of D21, but not as easily, as the voting takes place in a polling station - Long-term secrecy: *Sig*[Hash(Enc(Vote), voter login ID...)] even if the authorities are honest, the problem of long-term secrecy still remains	- User-friendliness: for the same reasons as in the case of D21 + Ease of use: the identification/authentication process is fast and the e-voting system performs encrypting/signing	- Cost for smart cards: extra cost for the special voting cards - Costs for smart card readers: extra costs for the card readers

Table 1: Analysis of systems in use

The result shows that the studied systems relying on smart cards with limited functionality (electronic authentication and signing), are vulnerable to long-term secrecy. The result also shows that e-voting systems that use national eID cards (e.g. Austria, Estonia), even though these smart cards are of limited functionality, fulfil most of the criteria defined in section 3.5. The use of smart cards, which are also used in other privacy-sensitive applications (e.g. online public services, secure online banking, etc.), increases the level of security (with respect to vote selling [9]), the level of usability, and do not impose any further costs. Therefore in section 3.7, we analyze the possibility of using national eID cards with limited functionality. We investigate thereby if the problem of long-term secrecy can be eliminated without introducing new vulnerabilities.

[9] Note that there are other attacks that are not mitigated by the usage of a standard national eID. The usage of the smart card in other areas could also increase the number of possible attacks on the smart card. An attack could be started during an online-banking session, where an attacker tries to make the voter vote while the card is in “heavy” usage.

3.7 Discussion of Alternatives

The analysis of the systems under consideration revealed weaknesses regarding the integration of smart cards into remote e-voting. Based on the results of section 3.6, we investigate whether it is possible to better integrate the Austrian and Estonian national eID cards, which offer limited functionality (namely electronic authentication and signing, into remote e-voting [10]. We first describe possible scenarios to apply these cards and analyze them afterwards. To avoid attacks, like man-in-the-middle and session hijacking, only scenarios in which all communications between the client-side voting software and voting server are secured by TLS/SSL and where the server authenticates itself using its SSL certificate are considered. In case votes are explicitly encrypted, we assume that they are encrypted with the public key of the election authority and for security reasons the decryption key is shared (e.g. as described in [Ge07]). It is further assumed that some anonymization mechanisms (e.g. re-encryption mix-net [BG12]) are in place to break the link between the voter and his or her encrypted vote before decrypting votes.

We distinguish between the following three cases:

1. Two-side authenticated channel with two different voting servers (we distinguish between sending the vote as plaintext or encrypted)
   a. A registration server first checks the voter's voting eligibility based on the voter’s HTTPS certificate and then provides a random voting token to the voter. The voter sends this token along with the cast vote to the ballot box server. The ballot box server checks the authenticity of the voting token and ensures that the token has not been used before. This approach is similar to the one used for the D21 elections.
   b. This case is similar to a) with the difference that the vote is sent explicitly encrypted.

2. Two-side authenticated channel with one voting server: (we distinguish between sending the vote as plaintext or encrypted)
   a. The voting server first checks the voter’s voting eligibility based on the voter’s HTTPS certificate and then sends him or her the ballot. The voter sends the cast vote back to the voting server secured by two-side HTTPS.
   b. This case is similar to a) with the difference that the vote is sent explicitly encrypted.

3. Digitally signing the encrypted vote:
   The voter sends the encrypted vote and a signed message to the voting server. The signed message is the hash value of the encrypted vote. The server checks the eligibility of the voter by verifying the signature. This approach is similar to the one applied in Austria and Estonia.

[10] Note that due to the limited functionality of the considered smart cards, they cannot be used to solve the problem of secure platform.

The first approach 1a is vulnerable to vote selling and coercion as the voter can forward the voting token received from the registration server. The receiver of this token can use it to contact the ballot box server and cast a vote. In addition, in scenario 1a the voter has to trust that the registration server and the ballot box server do not cooperate. The cooperation between the registration server and the ballot box server can break the election secrecy, as the voter sends his vote in plaintext. In 1b, election secrecy is ensured, even if the registration server and the ballot box server cooperate, as the vote is explicitly encrypted and due to the assumption of an anonymization mechanism; however vote-selling still remains a problem.

In 2a, the voter puts his or her complete trust in the one voting server that can break the election secrecy easily, while 2b mitigates the risk of this attack because the vote is explicitly encrypted and, due to the assumption of an anonymization mechanism, the encrypted vote is still clearly associated with the voter which causes problems with respect to long-term secrecy. However, vote-selling is not possible.

The third case is similar to the scenarios 1b and 2b: The voter has to trust the mixing process, which breaks the link between the encrypted vote and the voter's identity (his digital signature). However, signing encrypted data always recalls the problem of long-term secrecy. In addition, the voter does not see what is actually signed.

The above analysis shows that there is no better way to use smart cards, in particular national eIDs, with only limited functionality. Therefore, in section 4 we direct our attention to approaches in scientific papers using smart cards that provide more functionality.

4 Scientific Papers Based on Smart Cards with More Functionalities

In this section, we describe the different approaches of scientific papers that explore the use of smart cards that provide more functionality than only electronic authentication and signing. As many European countries have already started introducing national eID cards, we mainly focus on papers that suggest the usage of those cards. Afterwards, these approaches are analyzed. The aim of this analysis is to identify any practical, feasible functionality that might be implemented in future national eID cards with respect to e-voting. We consider both remote e-voting and e-voting in polling stations.

4.1 Remote E-voting using the European Citizen Card

The voting scheme in [Me08] is based on the design presented in [JCJ05] and its variants in [Sm05, WAB07, Sc06, AFT08]. The authors propose using the European citizen card (ECC) for the identification and authentication of voters as well as for the secure storage of voting credentials and electronic ballots. The original voting scheme is slightly modified because the ECC-standard does not support the generation of zero-knowledge proofs or the ElGamal encryption scheme. The authors make use of the restricted identification mechanism [BSI-TR-03110] to create an anonymous election-specific identifier, and the ECC contains an additional data field as defined in [CEN1540], where an election-specific template is loaded in the registration phase. The authors argue that by using the ECC, the proposed voting scheme, which only requires linear work in the tallying phase unlike [JCJ05] (quadratic with respect to the number of votes), is receipt-free compared to [Sm05, WAB07], does not require complex zero-knowledge proofs like [AFT08], and offers an important advantage regarding usability and economic aspects.

4.2 Remote E-voting Using the German eID Card

In [BKG11], the authors propose the use of the German eID card (nPA, "neuer Personalausweis") to identify and authenticate voters making use of the restricted identification (Restricted-ID) mechanism [BSI-TR-03110] in order to create a pseudonymous election-specific identifier. At the end of the election, all of the encrypted votes and the corresponding eID server-signed restricted IDs are published on the bulletin board (BB). This information allows the public to verify the correctness of the election process, as the eID server signs only authentic restricted IDs. In [Br11], the authors argue that in [BKG11], the secrecy of the election can be broken if the eID server and the certification authority of the German eID cooperate. Therefore, the authors modified the original voting scheme, by using both the restricted-ID mechanism and a randomly generated number, the so-called votingID and blind signatures. At the end of the election, all of the encrypted votes and the corresponding anonymous votingIDs, which are blindly signed, are published on the BB. As the votingIDs are randomly generated and assigned, this ensures the secrecy of the election in contrast to the original scheme. In this case, even if the eID server and the certification authority of the German eID cooperate, they cannot break the secrecy of the election.

4.3 Votescript+

Votescript+ was first introduced in [CB09] and was developed based on the e-voting scheme presented in [Go05]. Both were designed for distributed polling stations and are based on [FOO93] and [CC96], with some improvement upon these designs. In addition, both rely on a special powerful smart card called the Java Card. The main motivation behind using Java Cards is to have smart cards with cryptographic capabilities that have been specially designed for the e-voting scheme. The authors propose using the Java Card to store and execute the vote-casting software and other data related to the voting process, including a receipt-enabling individual verification. The main difference between Votescript and Votescript+ is that Votescript+ uses two different smart cards: any national eID card for secure identification and authentication and a Java Card to run the main vote-casting application on it. The motivation behind using two different smart cards is to achieve a strong separation between the identification and authentication phase and the vote casting phase.

4.4 Votinbox

Votinbox [CS06] is an e-voting scheme designed for polling station elections. Its security relies on a smart card capable of executing cryptographic operations designed specifically for e-voting. The Votinbox e-voting scheme uses cryptographic primitives that provide anonymous services introduced in [CT04].

These cryptographic primitives are programmed into the smart card. One of the most important primitives is the list signature. This anonymous mechanism is especially suitable for e-voting, as it also provides multiple-vote detection. The cryptographic algorithms include the following: RSA encryption/decryption and signature, a secret key generator, a list signature algorithm, and a pseudo random number generator, which reproduces the same output for the same input (required by the list signature scheme).

The procedures implemented within the card help perform many functions: create a ballot, create attendance, check voting eligibility, and validate voting, which completes the participation in an election. The smart card is also able to send various data (e.g., ballot) to the voting machines. The authors argue that a key advantage of this solution is that all of the security is based on the smart card. There is also no need for an additional "Trusted Authority". This is due to the fact that by using list signatures, the participation of a signing authority during the ballot creation process is no longer required.

4.5 Analysis

In this section we analyze the scientific approaches described above according to the criteria defined in section 3.5 with respect to voter identification and authentication, storing sensitive information, securely processing parts of the e-voting scheme, and vote encryption and signing.

The work presented in [Me08] is dedicated to the integration of the European citizen card (ECC) specification with a well-studied remote voting scheme, namely [JCJ05]. Due to the restricted cryptographic capabilities of the ECC, the scheme had to be modified in order to eliminate homomorphic encryption and zero-knowledge proofs, which impose a revision of correctness and security proofs. This scheme also shares the same problem as recognized in [Br11], namely that the cooperation between the eID server and the certification authority of the ECC can break the secrecy of the election.

In the approach presented in [BKG11], the authors use the German eID card as a foundation and integrate it with a generic e-voting scheme. Their first proposal shows weaknesses due to the fact that the eID server and certification authority might break the election secrecy. While this might be acceptable for elections with low coercion risk, it is unconstitutional when it comes to legally binding elections. In a revised version of their proposal in [Br11], the authors developed the VotingID accompanied by blind signatures to ensure the secrecy of the election. While the risks of unwanted anonymity breaches can be mitigated by these measures, the voter could sell his VotingID. However, the recognized security problems in [Br11] and [BKG11] aside, another challenge to both of these approaches is how to exclude people that are not allowed to vote (e.g. people suffering dementia or that lost their right to vote for other reasons), while still letting them use their eIDs in other areas. At this point, we recognize that the first approach has the potential to increase the level of security with respect to coercion resistance. By publishing the restricted ID associated with the corresponding vote on the bulletin board, the risk of mounting "forced-abstention" attacks can be mitigated against "less powerful" attackers, i.e., attackers that observe public channels and the bulletin board but are not able to break the used cryptographic protocols.

The concept introduced in [CB09] relies on the use of an even more powerful card than the German ID, the so-called Java Cards. From a practical point of view, this is a promising approach aimed at overcoming the drawbacks of national eID cards currently in use. However, [MP08] has shown that the flexible structure of these cards can be exploited to mount successful attacks, during which malicious code could be injected.

The concept introduced in [CS06] seems to provide some interesting functionalities that could be implemented by a smart card. However, the voting scheme is very complex, making it infeasible for real-world e-voting schemes. As an intermediate result, we commit to our prior conclusion—to rely on established smart cards for the purpose of usability and infrastructural questions.

5 Conclusion

In this paper, we examined the lessons learned for using eIDs in the context of e-voting from both existing real-world applications and scientific proposals. We first reviewed e-voting schemes in which smart cards were used to identify and authenticate voters as well as to sign votes. The sample of smart cards included both national eID cards and special purpose smart cards. The evaluation, based on the metric introduced in [Vo09], led to the conclusion that e-voting should rely on established smart cards that voters are familiar with, that do not impose additional costs, and that voters will not easily give away, thus preventing vote-selling. We further showed, that current schemes based on national eID cards, i.e., those implemented in Estonia and Austria, have weaknesses regarding long-term secrecy and require the voter to sign something that cannot read, as the message, which is signed, is encrypted. However, we showed that due to the limited functionality provided by those cards, there is no possibility to improve upon security.

Thereafter, in the second half of the paper we directed our attention to scientific proposals that focus on both, the use of national eID cards and special purpose smart cards that offer further functionalities, such as storing sensitive information (e.g. ballot, vote) and securely processing parts of the voting scheme (e.g. generate restricted ID). We discovered that national eID cards providing more functionality, like the restricted ID (pseudonym) or the German eID, have the potential to improve the security in remote electronic voting. We showed that the usage of the restricted ID can mitigate the risk of "forced-abstention" attacks.

As an overall conclusion to these lessons learned, we recommend that states that do not (yet) plan to introduce electronic voting take our considerations into account for their eID design because the proper functionality of an eID can dramatically improve the security of any e-voting system. For future work we plan to investigate the integration of the German eID into an end-to-end verifiable and coercion-resistant e-voting scheme, while also mitigating recognized problems like secrecy of the election, long-term secrecy, and excluding “specific ineligible” voters from the election (e.g. people suffering dementia but possessing an eID). Furthermore, we direct future attention to the question of needed and offered functionality of smart cards, specifically in the field of e-voting.

Bibliography

[Ab02] Abbott, J.: Smart Cards: How Secure Are They?. SANS Institute Reading Room, 2002. http://www.sans.org/reading_room/whitepapers/authentication/smart-cards-secure-they_131 (15.02.2012)

[AFT08] Araujo, R.; Foulle, S.; Traore, J.: A practical and secure coercion-resistant scheme for remote elections. In Frontiers of Electronic Voting, number 07311 in Dagstuhl Seminar Proceedings, Germany, 2008.

[BG12] Bayer, S.; Groth, J.: Efficient Zero-Knwoledge Argument for Correctness of a Shuffle. In Advances in Cryptology – EUROCRYPT 2012 (to appear). http://www.cs.ucl.ac.uk/staff/J.Groth/MinimalShuffle.pdf (10.04.2012)

[BKG11] Bräunlich, K.; Kasten, A.; Grimm, R.: Der neue Personalausweis zur Authentifizierung bei elektronischen Wahlen. In Sicher in die digitale Welt von morgen; pp. 211-225.

[Br11] Bräunlich, K. et. al.: Der neue Personalausweis zur Authentifizierung von Wählern bei Onlinewahlen. Institut für Wirtschafts- und Verwaltungsinformatik, Universität Koblenz-Landau. Nr. 11/2011. Arbeitsberichte aus dem Fachbereich Informatik.

[BSI-TR-03110] Bundesamt für Sicherheit in der Informationstechnik. Advanced Security Mechanism for Machine Readable Travel Documents - Extended Access Control (EAC). Technical Directive (BSI-TR-03110), Version 2.0 - Release Candidate, 2008.

[CB09] Carracedo Gallardo, J.; Belleboni, P. E.: Use of the New Smart Identity Card to Reinforce Electronic Voting Guarantees. In Internet Technology and Secured Transactions, 2009; pp.1-6

[CC96] Cranor, Lorrie F.; Cytron, Ronald K.: Design and Implementation of a Practical Security-Conscious Electronic Polling System, WUCS-96-02, Informatic Department of the University of Washington, St. Louis, USA.

[CEN15480] Comite Europeen de Normalisation. Identification card systems - European Citizen Card - Part 1/2/3/4, 2007.

[CS06] Canard, S.; Sibert, H.: Votinbox – a voting system based on smart cards. Workshop on e-Voting and e-Government in the UK, 2006.

[CT04] Canard, S.; Traore, J.: Anonymous Services using Smart Card and Cryptography. In Smart Card Research and Advanced Applications VI – Cardis 2004, Kulwer, 2004; pp.83-98

[FOO93] Fujioka, A.; Okamoto, T.; Otha, K.: A Practical Secret Voting Scheme for Large Scale Elections, Advances in Cryptology, AUSCRYPT´92, Lecture Notes in Computer Science 718. Springer Verlag, Berlin; pp.244-251

[Ge07] Gennaro, R. et. al.; Secure Distributed Key Generation for Discrete-Log Based Cryptosystems. In Journal of Cryptology 2007. Springer Verlag, New York; pp.51-83

[Go05] Gomez Olivia, A. et. al.: VOTESCRIPT: telematic voting system designed to enable final count verification. http://vototelematico.diatel.upm.es/articulos/Voto_telematico_Collecter_2005.pdf (15. 02. 2012)

[HSWO05] Austrian Government (Election Regulations): Hochschülerinnen- und Hochschülerschaftswahlordnung 2005. http://www.bmwf.gv.at/uploads/tx_contentbox/HSWO_2005.pdf (15.02.2012)

[ISO7816] ISO7816 Smart Card Standard: http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816.aspx (15. 02. 2012)

[JCJ05] Juels, A.; Catalano D.; Jakobsson, M.: Coercion-resistant electronic elections. In WPES '05: Proceedings of the 2005 ACM workshop on Privacy in the electronic society; pp. 61–70

[KM08] Karhumäki, J.; Meskanen, T.: Audit report on pilot electronic voting in municipal elections, Turku, 2008. http://vaalit.fi/uploads/5bq7gb9t01z.pdf (15.02.2012)

[Kr10] Krimmer, R.: Evaluierungsbericht: E-Voting bei den Hochschülerinnen- und Hochschülerschaftswahlen 2009. Bundesministerium für Wissenschaft und Forschung, Wien, 2010.

[Me08] Meister, G. et. al.: eVoting with the European Citizen Card. In A. Brömme & al. (Hrsg.), Tagungsband „BIOSIG 2008: Biometrics and Electronic Signatures", GI-Edition Lecture Notes in Informatics (LNI) 137, 2008, pp. 67-78

[MP08] Mostowski W.; Poll E.: Malicious Code on Java Card Smart cards: Attacks and Countermeasures. In "CARDIS '08": Proceedings of the 8th IFIP WG 8.8/11.2 international conference on Smart Card Research and Advanced Applications, 2008, pp. 1-16

[ODIHR11] Estonia Parliamentary Elections 6 March 2011. OSCE/ODIHR Election Assessment Mission Report, Warsaw, 2011.

[Pr03] Prosser, A., Kofler, R., Krimmer, R., Unger, M.: The first Internet-Election in Austria. Institut für Informationsverarbeitung und Informationswirtschaft Wirtschaftsuniversität Wien, Wien, 2003.

[Pr04] Prosser, A., Kofler, R., Krimmer, R., Unger, M.: Bundespräsidentschaftswahl 2004. Institut für Informationsverarbeitung und Informationswirtschaft Wirtschaftsuniversität Wien, Wien, 2004.

[PS06] Prosser, A.; Steininger, R.: An Electronic Voting Test Among Austrians Abroad. ePubWU Institutional Repository, 2006.

[RE03] Rankl W.; Effing W.: Smart Card Handbook. John Wiley & Sons, 2003.

[Sc06] Schweisgut, J.: Coercion-Resistant Electronic Elections with Observer. In (Krimmer, R. Eds.): Electronic Voting, volume 86 of LNI, pp. 171–177

[Sm05] Smith, D. W.: New cryptographic voting schemes with best-known theoretical properties. In Workshop on Frontiers in Electronic Elections 2005.

[TE08] TietoEnator Corporation: Electronic Voting Pilot 2008: Technical Implementation and Security, Version 1.1. 2008.

[TV11] Trechsel, H., A.; Vassil K.: Internet Voting in Estonia: A Comparative Analysis of Five Elections since 2005. European University Institute and European Union Democracy Observatory, 2011. http://www.vvk.ee/public/dok/Internet_Voting_Report_20052011_Final.pdf (15.02.2012)

[Vo09] Volkamer, M.: Evaluation of Electronic Voting. Springer-Verlag, Berlin, 2009.

[WAB07] Weber, S.; Araujo, R.; Buchmann, J.: On Coercion-Resistant Electronic Elections with Linear Work. In 2nd Workshop on Dependability and Security in e-Government (DeSeGov 2007), pp. 908–916