Compliance of RIES to the proposed e-Voting Protection Profile

Abstract. The RIES-KOA evoting system was used in the Netherlands as an additional system for the elections by expatriates for the *Tweede Kamer* (roughly: the Dutch House of Commons) elections in 2006. Although the system has been used in other elections in the Netherlands as well, there have been few independent evaluations of the system. In this paper, we apply the recently proposed Protection Profile for e-voting systems to the RIES-KOA system. This serves a two-fold purpose: it is an independent analyses of RIES-KOA and it is the first application of the Protection Profile. We indicate several issues with RIES-KOA and the Protection Profile, respectively, as learned during the analysis.

1 Introduction

Electronic voting is asserting itself as an addition to the election process. One of the prime examples of this is RIES – the Rijnland Internet Election System. RIES has been developed for regional water management board elections in the Netherlands in order to stimulate voter participation and cut down election costs. RIES was specifically developed to facilitate integration with the existing vote-by-mail system, to allow the voter to choose how she wishes to cast her vote.

After successful use for one election, use of RIES has spread. First to other water management board elections (which are regional organs with regional elections), which piqued the interest of the Dutch government. The government has initiated a project to use RIES to enable expatriates to cast their votes for national elections via the Internet. Previously, expatriates could only cast votes via mail. Past experiences indicated several problems with this medium, mainly that mail is unreliable and slow. Hence, voting officials were interested in providing an alternative which would address these issues, while not deviating too much from the established practice. As RIES was developed to be integrated with a vote-by-mail system, it was the perfect candidate. However, several adoptions were needed to fit to the law. Unlike water management board elections, national elections are governed by Dutch election law which allows for small-scale Internet Election experiments for national voting, if governed (in duration and in reach) by an additional, temporary law. Eg, water management board elections are for persons, while in national elections the candidates are affiliated with parties. The effort to adapt RIES, was dubbed "RIES-KOA ", where *KOA* stands for *Kiezen Op Afstand* (electing at distance). The resulting RIES-KOA system was used in the November 2006 national elections for expatriate voting, integrated with the mail-voting system used previously for this purpose. 19.815 votes were cast over the Internet.

This paper focuses on the RIES-KOA system. Its main features are, that it

- requires no special equipment on the voters side, just secrets sent to the voter via ordinary mail (unlike in the Estonian electronic elections, where advanced national ID-cards are available with digital signature capability),
- is simple to use via a web page with all cryptographic functionality hidden in embedded Java script,
- requires no retention of (personal) data by voters to cast their votes,
- provides some kind of verifiability of the outcome, both at an individual and universal level.

Although RIES is based on academic work and despite several researchers (see [8]) and international observers (from the OSCE [10]) actively monitoring RIES, to date there has been no scientific security evaluation of RIES, and specifically not of the RIES-KOA system. The Dutch e-voting interest group *Wij Vertrouwen Stemcomputers Niet* investigated RIES on a more practical level [9]. This paper provides elements of a scientific valuation, concentrating on security aspects, together with some recommendations for improvement. The security analysis is based on the Common Criteria Protection Profile for basic requirements to remote electronic voting systems [13]. Even the Protection Profile has been developed in Germany, it can be used internationally whenever a country accepted the Common Criteria Methodology.

The remaining sections are structured as follows: First, the paper continues with a detailed description of the RIES-KOA system. Then, the analysis approach based on a Common Criteria Protection Profile is proposed. The security requirements from this Protection Profile and the defined assumptions are named in Section 4. The security analysis of RIES-KOA is described in Section 5. where for each of the security requirements it is argued whether RIES-KOA passes the evaluation or not. The paper closes with a discussion of the evaluation results, identifying serious security problems of RIES-KOA as well as flaws in the Protection Profile.

2 Analysis approach

In the past, election officials have invited security experts to analyse e-voting systems for vulnerabilities. Usually, each group of experts used their own set of requirements and evaluation methods. Additionally, the depth of evaluation varied much.

This lack of a generic approach leads to conclusions about the security of e-voting systems which are hardly comprehensible by third parties. To mitigate this, standardized requirements, testing mechanisms, evaluation procedures, and observation techniques are essential. In [13], the authors presents a Protection Profile (PP) for remote electronic voting following the methodology of the Common Criteria (CC, [2]). The PP was written within the context of the German Federal Office for Information Security (BSI), in cooperation with the e-voting expert round of the German scientific association of informatics (GI). The PP

has been evaluated successfully by the testing authority Security Research & Consulting (SRC) in the first quarter of 2007 but it still needs to be certified by the BSI. Now, it serves as a contribution to the international community and can be used for certification of remote electronic voting systems in any country around the world that has adopted the Common Criteria. Further information about the background is available in [6].

The application of the CC has three advantages compared to existing approaches: First of all the methodology is word-wide known and accepted. Secondly, the evaluation depth is clearly defined and the third advantages is the possibility to compare different systems based on their evaluation report. Moreover, we do not provide just another list of requirement but the Protection Profile combines all the requirements from other catalogues (like [4, 7, 1, 5, 12, 3]).

The developed Protection Profile for remote electronic voting defines only a basic set of required security requirements (called security objectives in this context) which base on a couple of assumptions. We do not want to discuss here, whether the chosen assumptions are realistic ones or even met the Dutch situation but to evaluate the RIES-KOA systems against the security objectives in the Protection Profile to see whether it is in general in compliance to the Protection Profile. In our later discussion, we will also talk about those assumptions not given within the Dutch context.

3 The RIES system

RIES-KOA operates in three phases: the pre-election phase, the election phase and the post election phase. Because of the structure and the alignment of the Protection Profile, only the functionality used in the election and post election phase are analysed. However, here will explain all three phases.

The main parties in the RIES-KOA system are: V_i (the i^{th} voter), the voting server, the counting component, and the election authority.

In the **pre-election phase** the election authority generates for each voter V_i anonymous secret values:

- an identifier unique to V_i: $sk_i(0)$
- unique values $sk_i(j)$ for each of the N candidates, where $sk_i(j)$ is derived in a deterministic way from the election authority's master key K and the identifier $sk_i(0)$

They end up with a table where each column represents the secret values for one voter, but the columns are not link to a particular voter, meaning his name or any other identification token. The anonymous secret values from each column are printed on official election paper and sealed. This sheet is put into an envelope together with an instruction booklet (which beside others directs voters to the RIES-KOA web-site on the voting server). These sealed envelopes are then addressed using the election register and sent to the voters. Thus if the process is implemented correctly no one knows which column is sent to which voter.

Before the vote casting phases starts, the election authority commits to the keys $sk_i(j)$ by publishing a list of corresponding public keys on the voting server, consisting of $N+1$ elements $pk_i(j)$, $0 \leq j \leq N$, for each V_i, where $pk_i(j) = hash(sk_i(j))$. Notice that nevertheless the table with the secrets is kept and stored at a secret place.

This table carries per voter an ordered list of hashes of all possible votes (= encrypted secret values) the voter can choose. Based on this table, the voter can verify that the received secret values are correct, by hashing her/his $sk_i(j)$ to get her/his own values $pk_i(j)$, $0 \leq j \leq N$ and comparing these to the values posted on the voting server.

In the **election phase** the voter visits the election web page and the browser shows her/him the ballot. She/he makes her/his choice and enters her/his secret: $sk_i(0)$ and $sk_i(j)$ denoting the secret key linked to the chosen candidate j. The pair $(sk_i(0), sk_i(j))$ is transmitted to the voting server using SSL.

A vote will only be accepted if the pair $(sk_i(0), sk_i(j))$ indeed corresponds with public keys previously published on voting server and no vote for $sk_i(0)$ has been cast before (note that actually $pk_i(0)$ is the public identity of the voter). After casting the vote, she/he receives a confirmation message.

In the **post-election phase**, the counting component computes and publishes the results. The votes cast, represented by the pairs $(sk_i(0), sk_i(j))$, are published on the voting server, in the post-election phase. Each voter can check that his vote has been counted, that is, appears on the voting server in the list of votes as well as whether the tally is correctly by using the first table to link and $sk_i(j)$ to candidate j and start counting.

4 Security objectives

The security requirements are described in the Protection Profile [13]. The generic Protection Profile takes only the voting period into account (including the counting process). The Protection Profile itself is focused mainly on the interface provided by the voting system and the communication. As such, compliance to the profile does not imply that the evaluated voting system is secure in all manners. It does imply that the interface of the ToE is correct and devoid of errors (both security errors and less grave errors, such as usability errors).

The security objectives defined in the Protection Profile are restated below. They are labeled for cross-referencing in the analysis.

- *UnauthorisedVoter* Only voters eligible to vote who are unmistakeably identified and authenticated by RIES-KOA may cast a vote.
- *NoProof* No data that RIES-KOA makes available to the voter can be used by the voter to prove her vote to any third party.
- *IntegrityMessage* RIES-KOA must verify that the content of the authentication message, identification data, ballot data, vote records and the confirmation cannot covertly be deleted, inserted, replayed or amended during transmission (between the client-side and server-side RIES-KOA).

- *ElectionSecrecy* RIES-KOA must guarantee the election secrecy during transmission; in other words it is not possible to link the voter to her clear-text ballot. In particular, no conclusions about whether the vote is valid or invalid can be drawn from the number or size of the exchanged messages.
- *SecretMessage* RIES-KOA must guarantee the secrecy of identification data, of the contents of the authentication message and of the vote during transmission. This is necessary to ensure that an intruder observing the network cannot calculate intermediate results.
- *after-Integrity* RIES-KOA must guarantee that the polling period data and the result are stored securely within RIES-KOA once the vote count has taken place. Any changes to these data using any interface provided by RIES-KOA must be recognisable as such.
- *after-ElectionSecrecy* The system must prevent the possibility to determine how any specific voter voted after votes have been counted using the interfaces provided by RIES-KOA – even when supplementary data such as decryption keys are available. A link between voter and vote cannot be inferred from the order and/or time of storage of votes in the ballot box.
- *Cancel* The client-side of RIES-KOA must offer the voter the possibility to interrupt the voting process and to retain her right to vote when doing so.
- *EndElection* RIES-KOA must guarantee that the election committee does not accidentally stop the elections before the official election end time. Following an explicit confirmation, the election committee is able to end the elections prematurely.
- *after-BallotBox* RIES-KOA must guarantee that the interface does not accept votes after the elections are closed.
- *SecretElectionCommittee* RIES-KOA must guarantee election secrecy for all interfaces it provides on the election server during the polling period including the vote count. The election committee is not able to link voters to their plain text votes using any interface provided by the RIES-KOA system.
- *IntegrityElectionCommittee* RIES-KOA must not provide any interface to the election committee to insert votes into, delete votes from, or amend votes in the ballot box. In particular, there is no interface of RIES-KOA that allows the election authorityto reset RIES-KOA to its original state once an election has started. The RIES-KOA interfaces must guarantee that the election committee cannot allow any voter to cast more than one vote and that the election committee cannot change the authentication data in the list of eligible voters nor change the ballot data. RIES-KOA must guarantee that a restart is not possible once the election is closed.
- *SecretElectionCommittee* The election committee interface of RIES-KOA must not provide any knowledge of the content of authentication messages. RIES-KOA must not provide any interface to calculate intermediate results on the voting server.
- *OverhasteProtection* RIES-KOA is only allowed to accept a vote if the voter has explicitly double-checked and confirmed her vote. To this end, the vote is shown to the voter once again for final verification before the casting is final.

- *Correction* RIES-KOA must place no limit on the number of corrections a voter can make to her vote before she definitely casts it. The voter can correct the vote after the vote has been displayed for final verification.
- *Confirmation* RIES-KOA must allow the voter to check whether her vote has been stored in the ballot box. This means that the voter is presented with an on-screen confirmation once the vote has successfully been stored in the ballot box. Further, if a voter logs in again, the successful storage of her vote is confirmed onscreen.
- *Malfunction* The election committee must be able to recognise any malfunction on the server-side RIES-KOA by application of a self-test. After a break-down or other problems, the election committee must have the possibility to start a secure rerun of the system.
- *Log* RIES-KOA logs the events
  - Storage of the election data at the start of the election,
  - System errors as well as other reductions in the operability of the server-side RIES-KOA ,
  - Interruptions of communication,
  - Start and rerun of the election on the server-side RIES-KOA ,
  - Closing of the election,
  - Start of the vote count,
  - Determination of the vote count result.

  and allows the election committee to view them.
- *OneVoterOneVote* RIES-KOA must guarantee that nobody can cast more than one vote and that nobody loses their right to vote without having cast a vote. RIES-KOA must guarantee the right to vote especially in the case of an abort. This can be caused by a voter on the client-side, the client-side itself or the IT environment of the client-side. RIES-KOA also must guarantee that where malfunctions to the server-side occur, as well as to any subsequent restart and the execution of such restart, no data are lost and nobody loses their voting right or is allowed to cast more than one vote. Election secrecy must be preserved in all these cases.
- *AuthElectionCommittee* RIES-KOA must possess an authentication function that supports separation of duty between a minimum of two members of the election committee. Starting or ending the online election as well as initiating a restart must require two or more members of the election committee to be logged on. Initiating the vote count must also be conditional upon the same requirement being fulfilled.
- *StartVoteCount* RIES-KOA must guarantee that the election committee is only able to initiate the vote count once the elections are closed.
- *VoteCount* RIES-KOA must guarantee that all vote records, that are stored in the ballot box after the elections are closed, are correctly evaluated (and, where necessary, correctly decrypted) and contribute to the result of the vote count.

Additional expected security objectives that are not address in this Protection Profile are covered by the following assumptions:

– Election data is properly and correctly installed on RIES-KOA before the start of a polling period; the ballot box is empty; the election preparation phase has been carried out correctly; and RIES-KOA is correctly initialised.
– The voter ensures that nobody is watching her while she votes.
– The election committee accesses no data other than that on RIES-KOA ; i.e., it uses only the functions made available by the RIES-KOA system.
– The voter handles her voting credentials with care and is consistent in doing so; in particular, she ensures these remain private (solely accessibly by herself)
– The voter acts responsibly in securing the client device. Each voter installs or uses the RIES-KOA does so in such a way that the client device can neither observe nor influence the vote casting process. This includes the assumption that the voter does not manipulate her client device.
– The election server is protected against network attacks.
– The election server and the network are assumed to be robust, to be available and to provide a sufficient quality of service.
– No one outside the election committee, as appointed by the election organiser, has access to the server room, nor to the election server for the duration of the polling period, until the vote count.
– The data storage hardware is functioning correctly.
– The correct time is made available by the server's IT environment.

5 Security Analysis

The analysis validates the compliance of RIES-KOA to the proposed protection profile [13]. In a full-blown Common Criteria evaluation, adherence to the security functional requirements would be checked. However, as these requirements are derived from the security objectives, the below analysis employs the security objectives, which are more readable.

5.1 Used sources

The analysis below is based on the official RIES-KOA documentation [11], augmented by additional insights from personal experience[1] The official documentation is geared towards describing the operational aspects of the system, such as used file formats. Unfortunately, there is a lack of other publicly available sources of information on the RIES-KOA system, apart from the description of the original RIES system [8].

The analysis is of the conceptual RIES-KOA system, because the number of sources are limited, and the analysis was undertaken *a posteriori*. Nevertheless, as the official RIES-KOA documentation is used, we believe that the below analysis carries over well to the system used in the November 2006 elections.

[1] most notably a meeting with ms. Beneder from the Election Board on 22 February 2007, and a workshop on the security of RIES organised by SURFnet on 15 May 2007.

5.2 Compliance to security objectives

Below, the security objectives are listed once more by name, and for each security objective, the compliance of RIES-KOA is analysed. *FAIL* indicates lack of compliance, while *PASS* indicates RIES-KOA meets a particular security objective. *INCONCLUSIVE* means that the used sources did not provide enough information to determine a PASS/FAIL verdict.

- *UnauthorisedVoter*
  FAIL. The RIES-KOA system prescribes that the voter credentials are delivered via post. This is an insecure, unauthenticated channel, and thus the voting credentials must be considered exposed.
- *NoProof*
  FAIL. The RIES-KOA system is specifically designed to have these proofs.
- *IntegrityMessage*
  FAIL. The RIES-KOA system relies on SSL to secure the connection between RIES-KOA and the voter. However, the RIES-KOA documentation does not mention how to configure SSL. An incorrect setup can lead to exposure (as SSL specifically allows the option to use no encryption).
  Note that with a correct SSL setup, the verdict will become PASS.
- *ElectionSecrecy*
  FAIL. This is again ensured by using SSL.
  Note that with a correct SSL setup, the verdict will become PASS.
- *SecretMessage*
  FAIL. This is again ensured by using SSL.
  Note that with a correct SSL setup, the verdict will become PASS.
- *after-Integrity*
  PASS. The RIES-KOA system calculates a hash over the file containing the collected votes, after the closing of the elections. This hash is published.
- *Cancel*
  PASS. The voting process can be interrupted without foregoing the right to vote, until final confirmation. The final confirmation concludes the voting process.
- *EndElection*
  INCONCLUSIVE. The RIES-KOA system documentation mentions that a current election can be closed, but does not describe what preconditions must be met for this status change to occur.
- *after-BallotBox*
  PASS. The RIES-KOA server no longer accepts votes after closing.
- *SecretElectionCommittee*
  PASS. Note that this information **is** available on the server and thus to anyone with administrator access to the server.
- *IntegrityElectionCommittee*
  This requirement breaks down as follows:
  - changing ballot box: PASS.
    There is no interface to change the ballot box.

  - reset RIES-KOA : PASS.
    Again, there is no interface to reset the system.
  - no double voters: FAIL.
    The RIES-KOA system allows additional voter credentials to be handed out. Only access to the specific computer handling this functionality is required; in particular the system never knows to whom the credentials were handed.
  - change authentication data: PASS.
    The authentication data is inmutable by the system and used as a given.
  - change ballot data: PASS.
    RIES-KOA provides no interface to change ballot data.
- *SecretElectionCommittee*
  This requirement breaks down as follows:
  - knowledge of content of authentication messages: PASS.
    RIES-KOA provides no interfaces that provide knowledge of the content of authentication messages.
  - calculate intermediate results: INCONCLUSIVE.
    The documentation describes the tally process as taking the set of collected votes as an input. There is no mention of any provision to prevent a partial set being used to calculate an intermediate result; neither is it mentioned when or how the voting server provides this set of collected votes.
- *OverhasteProtection*
  PASS. Confirmation is required, before the vote is finalised.
- *Correction*
  PASS. This works equivalently to cancelation of a vote.
- *Confirmation*
  PASS. The voting is confirmed on-screen after reception of the vote, and the voter can choose to receives a confirmation from the election server.
- *Malfunction*
  INCONCLUSIVE. The documentation available provides no information on self-tests.
- *Log*
  This requirement breaks down as follows:
  - Storage at start: PASS.
    This is published.
  - System errors: INCONCLUSIVE.
  - Communication interruptions: INCONCLUSIVE.
  - Start and rerun: INCONCLUSIVE.
  - Closing: INCONCLUSIVE.
  - Begin vote count: INCONCLUSIVE.
  - Vote count result: PASS.
    RIES-KOA creates an official *procesverbaal* of this.

  The documentation mentions several logs, amongst which a `sysstatlog` and an `eventlog`, but fails to mention what these logs contain.

– *OneVoterOneVote*
PASS. Using $pk_i(0)$ RIES checks if a vote as already been cast by the corresponding voter before it stores the vote.
Note that this assumes that no voters has access to two different sets of voter credentials (this assumption is covered partially by *IntegrityElectionCommittee*).
– *AuthElectionCommittee*
FAIL. Starting or stopping an election requires access to a specific terminal per server used in the election. The available documentation in no way distinguishes users for this purpose.
– *StartVoteCount*
INCONCLUSIVE. The documentation fails to mention when access to the vote count becomes available.
– *VoteCount*
PASS. Everyone with access to the pre-election table and the post-election list can execute the counting procedure and thus verify the correctness of the counting procedure of the TOE.

5.3 Conclusions on RIES-KOA

Note that the protection profile is targeted on the interface provided by the TOE. This is not a weakness in itself, however care should be taken not to mistake PASS verdicts for a secure system. The results from the analysis are thus also valid for the interface.

The available documentation of RIES-KOA is lacking in some places. With better documentation, or access to more documentation, the analysis would probably be more positive in some points (more specifically, a description of SSL setup would mitigate *IntegrityMessage*, *ElectionSecrecy* and *SecretMessage*). Additionally, RIES-KOA was specifically designed to have proofs, and thus its failing the *NoProof* objective is inherent to the design goals of the system. That these specific security objectives are not achieved by RIES-KOA , thus seems reasonable.

More serious is the lack of documentation on self-tests, on access to the ballot box, on logging and on preconditions for starting or halting elections. The documentation fails to mention self-tests, which would greatly facilitate detection of malfunctions in the system (*Malfunction*). Neither does the provided documentation specify when the ballot box becomes accessible for counting. Hence, intermediate results (*SecretElectionCommittee*) and premature start of vote count (*StartVoteCount*) cannot be ruled out. The lack of documentation on loggin means that it is impossible to determine whether sytem errors, communication errors, and even status changes such as starting or halting elections can later be traced (*Log*). And finally, there is no mention in the documentation of support for multiple users in the system. This means that RIES-KOA lacks the support to ensure elections can only be halted by more than one person (*AuthElectionCommittee*). There are design decisions underlying each of these

security objectives, and the provided documentation strongly indicates (without being conclusive) that the wrong decisions can have been taken.

6 Conclusions

We analysed the Dutch RIES-KOA system used in November 2006 national elections for expatriate voting according to the Common Criteria Protection Profile describing basic requirements for remote electronic voting. In the analysis above we did not discuss the large list of assumptions on the environment in which the system analysed needs to ensure the defined basic requirements to become certified according to the Protection Profile. The evaluation was done assuming these assumptions hold. Surprisingly, even given these lax assumptions on our part (not verifying that the system's environment indeed satisfies the assumptions), RIES-KOA cannot succesfully meet the requirements of the Protection Profile. RIES-KOA fails to meet several security objectives outright, and might fail several more where we had to conclude "inconclusive".

This analysis not only showcases some weaknesses of RIES-KOA but also some of the Protection Profile. In the assumptions of the Protection Profile, two main weak points can be identified:

> The election committee [..] uses only the functions made available by the RIES-KOA system.

This is a very strong assumptions with the consequence that on the voting server side only security objectives to the RIES-KOA interfaces are defined in the Protection Profile. As a counterexample, within RIES-KOA there is a database on the voting server, that usually has its own user interface and security. If this interface can be used, election secrecy is easily broken. Even worse, the election results can be easily changed by deleting corresponding database entries. This is a potential large weakness of RIES-KOA which is not at all addressed by the Protection Profile

> Election [..] preparation phase has been carried out correctly [..].

This assumptions includes the generation and distribution of the authentication data to the voter. The intention was that all but only eligible voters receives the authentication data and the authentication data cannot be read through the envelope using a bright light source. But within RIES-KOA this phase is essential for the election secrecy because the election commission must not know the content of the election material because otherwise they can break the election secrecy and easily cast votes in behalf of the voter.

Summing it up it is good to have the Protection Profile but it needs to be seen as the first step describing really basic requirements which are not enough for most elections. Nevertheless, the analysis shows that the RIES-KOA system needs to be improved in order to get certified against the basic Protection Profile.

Notice that even if it would pass, the certificates only generates a secure election if the assumptions to the environment holed. If only one fails, no statements about the security of the system are made.

In general passing, this evaluation does not say whether the voter can detect any fraud and if she/he cannot detect it, she/he should know how many people of the election commission she/he needs to trust not to work together.

References

1. Voting standards: Project 1583 - voting equipment standard, project 1622 - electronic data interchange, 2005.
2. Common Criteria for Information Technology Security Evaluation, Version 3.1 2006.
3. Bundesministerium des Inneren BMI. Verordnung ber den Einsatz von Wahlgerten bei Wahlen zum Deutschen Bundestag und der Abgeordneten des Europischen Paralments aus der Bundesrepublik Deutschland. *Bundeswahlgerteverordnung (BWahlGV)*, (Vom 03.09.1975 (BGBl S. 2459) zuletzt gendert am 20.04.1999 (BGBl I S. 749)), 20.04.1999.
4. Council of Europe. Legal, operational and technical standards for e-voting. Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe and explanatory memorandum. *Council of Europe, Straburg*, 2004.
5. Gesellschaft fr Informatik e.V. Anforderungen an internetbasierte vereinswahlen. *Informatik Spektrum*, 28, Nr. 5:432–435.
6. Rüdiger Grimm, Robert Krimmer, Nils Meißner, Kai Reinhard, Melanie Volkamer, and Marcel Weinand. Security requirements for non-political internet voting. In *Proceedings of the 2nd International Workshop on Electronic Voting*, number LNI 86, pages pp. 203–212, 2006.
7. Volker Hertmann, Nils Meissner, and Dieter Richter. Online Voting Systems for Nonparliamentary Elections - Catalogue of Requirements. Technical report, Physikalisch-Technische Bundesanstalt Braunscheig/Berlin, 8.5.2004.
8. Engelbert Hubbers, Bart Jacobs, and Wolter Pieters. RIES - internet voting in action. In *COMPSAC (1)*, pages 417–424, 2005.
9. Lucas Kruijswijk. i-voting with RIES analyzed, November 17 2006.
10. OSCE. The netherlands parliamentary elections 22 november 2006, March 12 2007.
11. Piet Maclaine Pont, Arnout Hannink, Jacques Hoeienbos, Marco Rijkschroeff, and Jacques Schuurman. RIES-KOA – functioneel ontwerp, November 13 2006.
12. Melanie Volkamer and Margaret McGaley. Requirements and Evaluation Procedures for eVoting. In *Dependability and Security in e-Government*, 2007.
13. Melanie Volkamer and Roland Vogt. Protection Profile - Central Requirements for Online Voting Systems. Technical report, German Research Center for Artificial Intelligence, 2007.