Compliance of RIES to the proposed e-voting protection profile

Compliance of RIES to the Proposed e-Voting Protection Profile

Hugo Jonker[1,2] and Melanie Volkamer[3]

[1] Eindhoven University of Technology
[2] University of Luxembourg
[3] Institute of IT-Security and Security Law (University of Passau)
hugo.jonker@uni.lu, melanie.volkamer@uni-passau.de

Abstract. The RIES-KOA e-voting 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 analysis 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.

Keywords: e-voting, RIES, Protection Profile.

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 reduce 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 adaptions to RIES were needed to comply with election law. This had not been an issue before, as water management board elections are not governed by the Dutch election law (as opposed to national elections). Additional changes were prompted by the

A. Alkassar and M. Volkamer (Eds.): VOTE-ID 2007, LNCS 4896, pp. 50–61, 2007.

differences between water management board elections and national elections, for example: In water management board elections, voters choose one person, 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* (choosing 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 voter's side, just secrets sent to the voter via ordinary mail (unlike 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.

RIES is based on academic work and several researchers (see [7]) and international observers (from the OSCE [11]) actively monitor RIES. Despite all that, 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 *We Do Not Trust Voting Computers* investigated RIES on a more practical level [9]. This paper provides elements of a scientific evaluation, concentrating on security aspects, together with some recommendations for improvement. The security analysis is based on the Common Criteria Protection Profile (PP) for basic requirements to remote electronic voting systems [14]. Although the PP has been developed in Germany, it is not specific to Germany and hence it is usable for evaluations according to the Common Criteria methodology anywhere.

The remainder of this document is structured as follows: First, the approach used, is described in Section 2. Then, the paper provides a detailed description of the RIES-KOA system in Section 3. The security requirements and assumptions of the PP and are described in Section 4. A synopsis of the security analysis of RIES-KOA is described in Section 5, where RIES-KOA is tested on each security requirement. The paper closes with a discussion of the evaluation results, identifying serious security problems of RIES-KOA as well as suggestions for improvements of the PP.

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 has led to conclusions about the security of e-voting systems which are difficult to understand by third parties. To address

this problem, standardized requirements, testing mechanisms, evaluation procedures, and observation techniques are essential. In [14], the authors present a Protection Profile (PP) describing a set of minimum requirements for remote electronic voting, in line with the Common Criteria (CC, [2]) methodology. The PP was written within the context of the BSI (the German Federal Office for Information Security) in cooperation with the e-voting expert group of the German scientific association of Informatics. The PP has been evaluated successfully by the testing authority Security Research & Consulting in the first quarter of 2007, and certification by the BSI is pending. For now, the PP 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 [5].

The application of the CC has three advantages compared to existing approaches: First of all, the methodology is known and accepted world-wide. Secondly, the evaluation depth is clearly defined. The third advantage is the possibility to compare different systems based on their evaluation report. Moreover, the PP does not just provide another list of requirements but it combines requirements from other catalogues such as [3,6,1,4,13,10].

The PP for remote electronic voting defines only a basic set of security requirements, which are supported by several assumptions. Here we do not discuss the validity of these assumptions in general, nor their validity in the Dutch situation. The analysis evaluates the RIES-KOA system according to the requirements of the PP. There are some remarks on the general appropriateness of the assumptions in Section 5.4.

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 phases are analysed. Nevertheless, below we explain all three phases.

The main parties in the RIES-KOA system are: V_i (the i^{th} voter), the voting server, the tallier, and the election authority. Voters choose 1 candidate from the N candidates. Candidates are ranged over by $j, 1 \leq j \leq N$.

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

- a unique identifier: $sk_i(0)$.
- 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 $sk_i(0)$. These values represent the voter's possible choices.

Note that the credentials are not linked to any specific voter, but only to $sk_i(0)$. The credentials are then printed on official election paper and sealed. This sheet is put into an envelope together with an instruction booklet (which among others directs voters to the RIES-KOA web site to cast their votes). Finally,

these sealed envelopes are addressed using the election register (hence linking credentials to voters) and sent to the voters. So, if the process is implemented correctly no one knows which row was sent to which voter.

Before the vote casting phases starts, the election authority commits to the values $sk_i(j)$ by publishing a list on the voting server, consisting of $N+1$ elements $hash(sk_i(j))$, for $0 \leq j \leq N$, for each V_i. The table with the secret values is stored securely by an official notary. The list thus carries per voter an ordered list of hashes of all possible votes (= encrypted secret values) the voter can choose. Voters can verify that the received values constitute genuine, authentic voting material, by hashing the received $sk_i(j)$ to derive $hash(sk_i(j))$, $0 \leq j \leq N$ and comparing these to the listed values.

In the **election phase** the voter visits the election web site and the browser shows her the ballot. She makes her choice and enters her secret identifier, $sk_i(0)$, and her choice, $sk_i(j)$ (the voter-specific secret value denoting candidate j). The pair $(sk_i(0), sk_i(j))$ is transmitted to the voting server over an SSL channel.

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

In the **post-election phase**, the tallier computes and publishes the election results. The votes cast, represented by the pairs $(sk_i(0), sk_i(j))$, are published now on the voting server. Each voter can check that her vote has been counted, that is, appears on the voting server in the list of votes as well as whether the tally is correct. This is achieved by using the pre-election committed list and the $hash()$ function to link cast votes $sk_i(j)$ to candidates j.

4 Security Requirements

The security requirements are described in the Protection Profile [14]. The security objectives defined in the Protection Profile are restated below. They are labeled for cross-referencing in the analysis.

- *AuthorisedVoter.* 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 cleartext 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 must be recognisable as such.
- *after-ElectionSecrecy.* The system must prevent the possibility to determine how any specific voter voted after votes have been count 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.
- *CancelVote.* 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 its interfaces do not accept votes after the election is closed.
- *AnonElectionCommittee.* 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 authority to 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 has been 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 definitive.
- *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 was successfully stored in the

ballot box. Further, if a voter logs in again, the successful storage of her vote is confirmed on-screen.
- *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 must also 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 security requirements that the PP does not require of RIES-KOA but of RIES-KOA's environment 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 accessible by herself).
- The voter acts responsibly in securing the client device. 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 level of 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.

As can be inferred from the descriptions above, the PP has a limited scope. The PP only takes the voting period into account (including the counting process) and is focused on a set of basic requirements for usability and security. As such, compliance to the profile does not imply that the evaluated voting system is a secure system – it means that the evaluated voting system satisfies the set of basic requirements in an environment where the given assumptions hold.

5 Security Analysis

The analysis evaluates the compliance of RIES-KOA to the proposed Protection Profile [14]. 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.

Note that the scope of the PP is limited. The PP is written for elections adhering to the most basic election principals (universal, free, secret and democratic elections). This type of elections is common for e.g. national elections, however, specific elections may deviate from this norm (e.g. postal voting or voting by share holders). This PP cannot accommodate elections where some of these principals have been relaxed.

5.1 Used Sources

The analysis below is based on the official RIES-KOA documentation [12], augmented by additional insights from personal experience[1]. The official documentation focuses mainly upon 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 in [7].

[1] Most notably a meeting with ms. Beneder from the RIES-KOA project on 22 February 2007, and a workshop on the security of RIES organised by SURFnet on 15 May 2007.

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.

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. *INCONCL* means that the used sources did not provide enough information to determine a PASS/FAIL verdict.

objective	**result**	**objective**	**result**
AuthorisedVoter	PASS[1]	IntegrityElectionCommittee	INCONCL[8]
NoProof	FAIL[2]	SecretElectionCommittee	INCONCL[9]
IntegrityMessage	FAIL[3]	OverhasteProtection	PASS[5]
ElectionSecrecy	FAIL[3]	Correction	PASS[5]
SecretMessage	FAIL[3]	Confirmation	PASS[5]
after-Integrity	PASS[4]	Malfunction	INCONCL[10]
after-ElectionSecrecy	FAIL[2]	Log	INCONCL[11]
CancelVote	PASS[5]	OneVoterOneVote	PASS[12]
EndElection	INCONCL[6]	AuthElectionCommittee	FAIL[13]
after-BallotBox	PASS[5]	StartVoteCount	INCONCL[14]
AnonElectionCommittee	PASS[7]	VoteCount	PASS[5]

1. 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. However, the correct distribution (and handling) of voter credentials is covered by the assumptions. Hence the PASS verdict – note that these assumptions do not hold for the elections in which RIES-KOA was used.
2. The RIES-KOA system is specifically designed to have these proofs.
3. 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). Without specifying the SSL setup, we cannot assume that integrity or secrecy will hold.
   Note that with a correct SSL setup, the verdict would be PASS.
4. The set of votes is signed and made publicly available.
5. The RIES-KOA system supports this.
6. 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.
7. Note that this information *is* available on the server and thus to anyone with administrator access to the server. However, this is covered by the assumptions, hence a PASS verdict is in order.

8. RIES-KOA satisfies most requirements listed here, as it has no specific election committee interface. However, RIES-KOA has a provision for activating substitute voter credentials. This procedure violates the spirit if not the precise wording of this requirement.
9. The documentation does not mention when or how the voting server provides the set of collected votes. Specifically, there is no mention of any provision to prevent intermediate result from being calculated from a partial set of votes.
10. The documentation available provides no information on self-tests.
11. The documentation mentions several logs, amongst which a `sysstatlog` and an `eventlog`, but fails to specify exactly what is logged.
12. Note that the PASS relies on the assumption that no voter has access to two (or more) different sets of voter credentials (which follows from the assumptions in the PP).
13. Starting or halting 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.
14. The documentation fails to mention when access to the vote count becomes available.

5.3 Evaluation Conclusions

We reiterate the remark made in the beginning of this Section: note that the PP has a limited scope; care should be taken not to mistake a general PASS verdict for a "secure system".

The most obvious conclusion is that the available documentation of RIES-KOA has some profound gaps. 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*). Note that in the course of a full CC evaluation, one of the largest categories of errors found are documentation errors. In the course of a CC evaluation process, such errors are corrected. Hence, similar omissions in the RIES-KOA documentation do not seem too grave.

A second conclusion is that the design decision to grant receipts to voters to ensure verifiability implies that RIES-KOA fails the *NoProof* objective by design. This is a more serious issue and unnecessary to ensure verifiability (see e.g. [8]). However, this failure stems from a design issue in RIES, the consequences of which are well known to the involved parties.

The foremost conclusion of the analysis, however, is more grave. The documentation has several severe lacunes in addition to the ones mentioned before. There is insufficient information on self-tests, on access to the ballot box, on logging and on preconditions for starting or halting elections. In none of these cases, however, is there any indication in the available documentation that the RIES-KOA system complies with the requirements of the PP.

In more detail, the issues that were discovered were the following:

- The documentation fails to have any mention of self-tests. As self-tests facilitate detection of malfunctions in the system (*Malfunction*), it is unclear (even unlikely) that RIES-KOA will catch malfunctions.
- The documentation does not 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 logging 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*).

We believe these to be serious issues, the extent of which the involved parties may not completely realise. Neither do these seem to be merely documentation omissions. The provided documentation strongly indicates (without being conclusive) that RIES-KOA lacks the functionality needed to support these requirements.

In any Common Criteria analysis, the documentation is bound to be lacking. For those cases, where it is clearly an omission (e.g. SSL setup), this can be easily addressed. However, the documentation on RIES-KOA misses several issues that seem not to have been implemented in the system at all. Even if the questionable design decision of having voter proofs is assumed to be correct, the system (in its current state) still fails to meet the basic requirements as set forth in the PP.

5.4 Evaluation of the Methodology

This analysis brings to light not only several weaknesses of RIES-KOA but also some issues of the PP. Here we note the most important issues.

A lacune in the PP discovered during the analysis is the complete lack of requirements on verifiability. Verification of the result and of inclusion of a vote as cast by a specific voter is one of the foremost issues for generic acceptance with electronic voting – can the voters be convinced that the result is really based on the votes as cast?

A second issue in the PP is the reliance on very strong assumptions. It will be extremely difficult to ensure that none of the assumptions can be violated. The following two assumptions are the main problems in this regard:

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

The consequence of this assumption is that the PP only defines security requirements on the interfaces offered by RIES-KOA. However, this can be

insufficient. In the case of RIES-KOA, a database is used to store all data (including votes). Databases often have their own interface. By not covering this interface as well, a voting system compliant with the PP may still allow arbitrary manipulation of votes via a direct database interface. Other software used by voting systems (e.g. operating systems, web servers) can have similar features. Hence the PP should be updated to address the use of third-party software.

– *[. . .] the election preparation phase has been correctly carried out [. . .].*

This assumption covers the generation and distribution of the authentication data to the voter. The intention was that none but eligible voters receive voting credentials. To this end, the voting credentials must remain secret (e.g. they are not readable through the envelope using a bright light source). In systems such as RIES-KOA, however, this phase is essential to election secrecy. The election committee must not know the content of the election material – otherwise they can break election secrecy and (e.g.) cast votes in a voter's stead.

6 Conclusions

We analysed the Dutch RIES-KOA system used in November 2006 national elections for expatriate voting. This analysis was executed according to the Common Criteria Protection Profile (PP) describing basic requirements for remote electronic voting. The PP specifies quite a number of assumptions on the environment. The evaluation was done under the premise that these assumptions hold. Surprisingly, even given these relaxation of constraints on our part (the evaluation assumed that the system's environment indeed satisfies the assumptions of the PP), RIES-KOA cannot successfully meet the requirements of the PP. RIES-KOA fails to meet several security objectives outright, and might fail several more where we had to conclude "inconclusive".

The analysis also brought to light several limitations of the PP. On the whole, we can conclude that the PP enables a structured evaluation of remote electronic voting systems. The current PP should be viewed as an initial version outlining the most basic requirements. The PP does not (yet) capture all security aspects of e-voting as desired for most types of elections (such as verifiability). To achieve this, the PP needs to mature further.

Nevertheless, even this early version of the PP has already found issues in RIES-KOA. This underlines the need for a structured approach to security in e-voting, as offered by the PP.

Acknowledgments

We are very grateful for the insightful discussions on RIES with Berry Schoenmakers and Bart Jacobs. Funding for Melanie Volkamer's research visit at TU/e was provided by the German Academic Exchange Service (DAAD).

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. 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, Straßburg (2004)
4. Gesellschaft für Informatik, e.V.: Anforderungen an internetbasierte vereinswahlen. Informatik Spektrum 28(5), 432–435
5. Grimm, R., Krimmer, R., Meißner, N., Reinhard, K., Volkamer, M., Weinand, M.: Security requirements for non-political internet voting. In: Proceedings of the 2nd International Workshop on Electronic Voting. LNI 86, pp. 203–212 (2006)
6. Hertmann, V., Meißner, N., Richter, D.: Online Voting Systems for Nonparliamentary Elections - Catalogue of Requirements. Technical report, Physikalisch-Technische Bundesanstalt Braunscheig/Berlin (8.5.2004)
7. Hubbers, E., Jacobs, B., Pieters, W.: RIES - internet voting in action. In: COMPSAC (1), pp. 417–424 (2005)
8. Juels, A., Catalano, D., Jakobsson, M.: Coercion-resistant electronic elections. In: Atluri, V., De Capitani di Vimercati, S., Dingledine, R. (eds.) WPES 2005: Proceedings of the 2005 ACM workshop on Privacy in the electronic society, pp. 61–70. ACM Press, New York (2005)
9. Kruijswijk, L.: i-voting with RIES analyzed (November 17, 2006)
10. German Ministry of the Interior (BMI). Verordnung über den Einsatz von Wahlgeräten bei Wahlen zum Deutschen Bundestag und der Abgeordneten des Europäischen Parlaments aus der Bundesrepublik Deutschland. Bundeswahlgeräteverordnung (BWahlGV) (Vom 03.09.1975 (BGBl S. 2459) zuletzt geändert am 20.04.1999 (BGBl I S. 749)) (1999)
11. OSCE. The Netherlands parliamentary elections (22 November 2006) (March 12, 2007)
12. Pont, P.M., Hannink, A., Hoeienbos, J., Rijkschroeff, M., Schuurman, J.: RIES-KOA – functioneel ontwerp (November 13, 2006)
13. Volkamer, M., McGaley, M.: Requirements and Evaluation Procedures for eVoting. In: Dependability and Security in e-Government (2007)
14. Volkamer, M., Vogt, R.: Protection Profile - Central Requirements for Online Voting Systems. Technical report, German Research Center for Artificial Intelligence (2007)