ODIHR.GAL/56/07
28 June 2007

ENGLISH only

Office for Democratic Institutions and Human Rights

REPUBLIC OF ESTONIA

PARLIAMENTARY ELECTIONS
4 March 2007

OSCE/ODIHR Election Assessment Mission Report

Warsaw
28 June 2007

TABLE OF CONTENTS

REPUBLIC OF ESTONIA

PARLIAMENTARY ELECTIONS
4 March 2007

OSCE/ODIHR Election Assessment Mission Report

I. EXECUTIVE SUMMARY

In response to an invitation from the Minister of Foreign Affairs of the Republic of Estonia, the OSCE Office for Democratic Institutions and Human Rights (ODIHR) deployed an Election Assessment Mission (EAM) for the 4 March 2007 parliamentary elections.

The elections to the Riigikogu (parliament) reflected the democratic practice and tradition that have become characteristic of the electoral process in Estonia. A meaningful democratic exercise was underscored by the registration of an array of political parties and independent candidates, the conduct of the campaign, and diverse viewpoints expressed in the media. The election administration at all levels carried out its work transparently and effectively, and enjoyed a high degree of confidence from political parties and civil society.

Estonian legislation overall provides a sufficient framework for the conduct of democratic elections; it fully provides for the presence of international and domestic observers in accordance with OSCE commitments. However, a provision of the Riigikogu Election Act that prohibits outdoor political advertising during the official campaign period is unduly restrictive of political expression. In addition, the Chancellor of Justice challenged the current system of oversight of campaign finance as being unconstitutional.

Estonia has undertaken recognised efforts to naturalize and integrate the substantial population of persons without citizenship, largely of Russian origin. It is assessed positively that all residents of Estonia are permitted to vote in local elections, regardless of citizenship. However, given that 9.4 per cent of Estonian residents do not have citizenship of any country, the OSCE/ODIHR encourages further steps to facilitate citizenship for all persons in this category who so desire it, in order to enable these persons to fully exercise their political rights.

This was the first parliamentary election in the OSCE area in which voting by internet was available to all voters. This alternative voting method was only available during an early voting period prior to election day. Voters choosing this method had the option to recast their electronic ballot, cancelling any previously cast electronic ballot. They could also annul their electronic ballot by casting a paper ballot in a polling station during the early voting period. The election administration implemented the system in a fully transparent manner, and appeared to take measures to safeguard the conduct of internet voting to the extent possible.

While the use of internet voting increases the access of voters to the voting process, it also poses real risks to the integrity of elections due to the potential for external attacks or internal malfeasance. While only 5.4 per cent of voters chose to vote by internet, the risks will increase as the use of this voting method grows. Furthermore, as with other forms of

remote voting, the organization of voting outside the supervised and controlled environment of a polling station always raises the potential that the fundamental right to a secret ballot could be compromised.

Although the National Election Committee made considerable efforts to minimize the inherent risks, testing and auditing of the system could have been more comprehensive. Furthermore, there appeared to be almost no oversight of the internet voting process by political parties or civil society. The internet voting system as implemented appears to have functioned in the Estonian context on this occasion. Yet, unless the above-mentioned factors are effectively addressed, the authorities should reconsider whether the internet should be widely available as a voting method, or alternatively whether it should be used only on a limited basis or at all.

The OSCE/ODIHR EAM did not conduct systematic or comprehensive observation of the advance voting and election day procedures. Nevertheless, the mission was able to assess that the process was well-defined and regulated and was generally adhered to in polling stations visited. No political parties or candidates expressed concerns about the conduct of voting by paper ballot or regarding the counting process. The OSCE/ODIHR EAM noted the positive efforts made to recount all paper ballots cast.

Recommendations regarding election-related legislation and administration of the election process are included in the body of the text.

II. INTRODUCTION AND ACKNOWLEDGEMENTS

Following an invitation from the Minister of Foreign Affairs of the Republic of Estonia, the OSCE/ODIHR deployed an Election Assessment Mission for the 4 March 2007 elections to the Riigikogu.

The OSCE/ODIHR EAM was deployed from 20 February to 7 March 2007. It was led by Mrs. Mirjana Lazarova Trajkovska and consisted of 13 experts from twelve OSCE participating States. In addition to election experts based in Tallinn, including four electronic voting experts, teams were deployed to Tartu, Narva and Parnu. The OSCE/ODIHR EAM met with government representatives and state officials, election administration, political parties, academics, and civil society in order to form an overview of the electoral process and of specific legislative and administrative issues. In line with OSCE/ODIHR methodology, the deployment of the EAM did not encompass systematic or comprehensive observation of election day procedures.

The OSCE/ODIHR wishes to express its appreciation to the Ministry of Foreign Affairs of the Republic of Estonia and the National Election Committee, as well as to other interlocutors, for their cooperation during the Election Assessment Mission.

III. BACKGROUND

The Riigikogu election was the fifth parliamentary election since the restoration of independence and the first to be held since Estonia's accession to the European Union. The Riigikogu is a unicameral parliament, composed of 101 seats. In addition to legislative

responsibilities, the Riigikogu elects the President of the Republic and approves the nomination of the Prime Minister.

Members of parliament are elected from 12 multi-seat constituencies for four-year terms through a proportional, open-list system with a five per cent threshold at the national level for political party lists. Eleven political parties and seven independent candidates competed in the election, including the five parties represented in the outgoing Riigikogu.

The OSCE/ODIHR previously observed Riigikogu elections held on 5 March 1995 and 7 March 1999. After the 7 March 1999 elections, the OSCE/ODIHR concluded that the "elections were held in accordance with Estonia's OSCE commitments and with Estonian law." The OSCE/ODIHR conducted a Needs Assessment Mission in advance of the 2 March 2003 Riigikogu election but did not subsequently conduct an election observation activity.

IV. LEGAL FRAMEWORK

A. OVERVIEW

The legal framework of Estonia generally provides the legal basis for the conduct of elections in accordance with OSCE commitments and other international standards. The Riigikogu elections are conducted on the basis of the Constitution of Estonia and Riigikogu Election Act.[1] Since its adoption in 2002, the Riigikogu Election Act was significantly amended in 2003, 2004, 2005, and in 2006. Recent amendments included provisions for electronic voting by internet and the prohibition of outdoor political advertising during the campaign period (see Internet Voting and Campaign sections).

The Riigikogu elections were also regulated by the Political Parties Act and Broadcasting Act, which respectively established legal provisions for the financing of political parties and media regulation during the campaign period. The legislation was supplemented by National Election Committee (NEC) regulations, including the procedure for registration of candidates, format of ballot paper, and the accreditation and status of observers.[2]

In addition to review by the courts, legislation may be assessed by the institution of the Chancellor of Justice for its compliance with the Constitution, based either on a complaint or on his/her own initiative. If the Chancellor has concerns about the constitutionality of a law, he/she may make a non-binding request to Parliament to reconsider it. The Chancellor may also refer an issue directly to the Constitutional Chamber of the Supreme Court (see section VIII, Election Campaign).

B. VOTING RIGHTS

The Constitution provides that Estonian citizens who have attained 18 years of age on election day have the right to vote in parliamentary elections. The right to be elected as a member of parliament is granted to Estonian citizens who have attained 21 years of age and who have the right to vote.

---

1 Each level of elections is conducted in accordance with a separate law for that election.

2 The competence of the NEC is envisaged by Article 15 of the Riigikogu Election Act.

The Constitution limits the right to vote of persons who have been deprived of legal capacity by a court, and persons who have been convicted by a court and are serving sentences in penal institutions.[3] On the basis of this provision, the Riigikogu Election Act stipulates that a person who has been convicted of a criminal offence by a court and is imprisoned shall not participate in voting.

The restriction does not appear to be in accordance with European standards that a limitation on voting rights of a prisoner can be imposed only where the prisoner has been convicted of a crime of such a serious nature that forfeiture of the suffrage right is a proportionate punishment. In the case *Hirst v. United Kingdom*,[4] the European Court on Human Rights held that a blanket prohibition on voting rights of prisoners is not proportionate and constitutes a violation of Article 3 of Protocol No. 1 of the European Convention on Human Rights (right to free elections). In addition, it is a commitment for OSCE participating States (paragraph 24 of the 1990 Copenhagen Document) that any restriction of rights and freedoms must be strictly proportionate to the aim of the law.

The OSCE/ODIHR recommends that the Riigikogu Election Act be examined and amended by the Estonian authorities in light of OSCE commitments and jurisprudence of the European Court of Human Rights.

C. CITIZENSHIP AND NATURALIZATION

Estonia has a population of stateless persons or "persons with undetermined citizenship" stemming from the period of its annexation into the Soviet Union. Stateless persons are largely those who migrated from Russia and other parts of the Soviet Union after World War II, and their children, who did not obtain the citizenship of any State after the re-establishment of Estonian independence. The biggest ethnic group among these are Russians, but there are also Ukrainians, Belarusians and others.

According to information from the Citizenship and Migration Board, there are 126,000 persons with undetermined citizenship resident in Estonia, some 9.4 per cent of the total population of 1,342,000.[5] Most of these persons are eligible to become citizens but must go through a naturalization process to do so. In order to acquire citizenship, the legislation requires knowledge of the Estonian language, knowledge of the Constitution and the Citizenship Act, and a loyalty oath. Children are eligible for citizenship through an expedited process, on request of their parents.

In total, 142,999 persons have become Estonian citizens by naturalization since 1992, with 662 applications refused. Almost three-quarters of all naturalizations took place from 1992 to 1998, with the number of naturalizations per year being significantly lower after this date. After an increase in the naturalization rate in 2004 and 2005 associated with Estonia's entry into the European Union, the overall numbers of persons applying for naturalization appear to be declining. In 2006, 4,753 persons received citizenship by naturalization.

---

3 Articles 56 and 57 of the Constitution of the Republic of Estonia.

4 European Court of Human Rights (Grand Chamber), *Hirst v. United Kingdom* (Application number 74025/01), Judgment on 30 March 2004.

5 In addition, there are some 105,000 persons with citizenship of other States, mostly of the Russian Federation. Data of the Ministry of Foreign Affairs, www.vm.ee

Persons with undetermined citizenship do not have voting rights in Riigikogu elections. They are also not permitted to be members of political parties. However, permanent residents, including persons with undetermined citizenship, are eligible to vote in local elections in Estonia. This commendable practice is in accordance with the Convention on the Participation of Foreigners in Public Life at Local Level.[6] In addition to enabling participation in local government, this measure can affect the indirect election of the President, as in certain circumstances (including in the 2006 election) the body electing the President includes representatives of local authorities.

The Estonian authorities consider that full efforts have been made to facilitate the naturalization process for persons with undetermined citizenship. In their view, many of the persons remaining in this category do not wish to become Estonian citizens. In 2005, however, the Council of Europe's Advisory Committee of the Framework Convention for the Protection of National Minorities stated that "the number of persons without citizenship remains disconcertingly high. Despite positive measures taken to facilitate naturalisation, the language tests and other factors are still an obstacle for many." The Advisory Committee therefore encouraged the Estonian authorities to take additional steps to make the naturalization process more accessible.

There are no international standards which would require permitting persons who are not citizens to vote in parliamentary elections. Moreover, the extension of voting rights in local elections to persons with undetermined citizenship is assessed as a positive step towards their inclusion in the political life of Estonia. Nevertheless, the fact that a significant number of Estonia's permanent residents, some 90 per cent of whom are of voting age, do not have citizenship of any State and cannot fully participate in political life is an ongoing challenge for Estonia.

Given Estonia's considerable and apparently successful efforts towards the integration of naturalized citizens, the Riigikogu could consider the possibility of further facilitating the naturalization of persons with undetermined citizenship who wish to become citizens of Estonia.

V. ELECTORAL SYSTEM

Estonia is divided administratively into 15 counties and the cities of Tallinn and Tartu. For the purpose of elections to the Riigikogu, the country is divided into 12 multi-mandate electoral districts. Three of them are within the city of Tallinn; one incorporates the city of Tartu, while the other eight districts span one to three counties.

A proportional open list electoral system is used in the elections to the Riigikogu. Political parties compete for the mandates distributed in an electoral district by registering with the National Election Committee (NEC) the lists of candidates for each electoral district contested. The number of candidates on a party district list cannot exceed the number of district mandates plus two. The political parties also register with the NEC their national lists consisting of all candidates registered in the electoral districts (maximum 125). The

[6] Convention On The Participation Of Foreigners In Public Life At Local Level, CETS 144. Chapter C – "Right to vote in local authority elections" Article 6. Estonia is not a party to the Convention.

national lists are used for the allocation of seats remaining after the distribution of mandates in the electoral districts.

All registered candidates are assigned individual registration numbers, starting from 101, following the order of the parties determined by drawing lots. To cast a ballot, voters write the registration number of the candidate of their choice on the ballot when voting by ballot paper or mark the name of the preferred candidate when voting by internet. Voters may only vote for candidates registered in their electoral district.

The transformation of votes into seats is performed in three steps. First, in each of the electoral districts individual mandates are distributed to all candidates who collected a number of votes not less than the *simple quota* of their district.[7] Only parties satisfying the 5 per cent threshold at the national level participate in the further distribution of seats at the district level and at the allocation of compensatory seats at national level. During the second step each party district list is reordered in accordance with the number of votes received by each candidate on the list and is awarded as many seats as the number of times the total number of votes for the party candidates in the electoral district exceeds the *simple quota* of the district.[8] The mandates remaining undistributed after the first two steps are allocated as nationwide seats to the parties satisfying the 5 per cent threshold at national level using a version of the D'Hondt method.

In the current election, 75 parliamentarians were elected by districts, while 26 were determined by nationwide mandates.

VI. ELECTION ADMINISTRATION

A. ALLOCATION OF MANDATES

When an election is called, the 101 parliamentary mandates are allocated by the NEC to the 12 electoral districts proportionally to the number of eligible voters as of the first day of the month when the elections were called (1 November 2006). This number varies from 6 (Lääne-Virumaa) to 13 (Harju-ja Raplamaa). The numbers of voters used to allocate mandates do not include persons with undetermined citizenship who are residents of Estonia. Due to the concentration of these persons in several electoral districts, these districts may be underrepresented in the Riigikogu in terms of total population.

B. ELECTORAL COMMITTEES

The Riigikogu Election Act establishes a three-tiered election administration structure that is responsible for the preparation and conduct of the elections to Riigikogu. The National Election Committee (NEC) is at the top of the structure, with 15 County Electoral Committees and two City Electoral Committees[9] (CEC) at the second level and 657 Division Committees (DC) at the third level. Regulations issued by the NEC and decisions

---

7 The simple quota of an electoral district is produced by dividing the total number of valid votes cast in the district by the number of seats distributed in the district.

8 A 2006 amendment to the Riigikogu Election Act provides for the increase of this number by 1 in the case when the remaining votes are at least 75 per cent of the simple quota of the district.

9 In the cities of Tallinn and Tartu.

and instructions of superior electoral committees are binding for the lower level committees.

The NEC is a permanent body with seven members appointed for four year terms by, respectively, the Chief Justice of the Supreme Court (two judges), the Chancellor of Justice, the Auditor General, the Chief Public Prosecutor and the Secretaries of the Chancellery of the Riigikogu and of the State Chancellery. The NEC Chair and Vice Chair are elected by the members. The NEC's responsibilities include the right to suspend acts of lower level committees and to suspend members of lower level committees violating the Riigikogu Election Act, NEC regulations, or instructions of superior electoral committees. The NEC issues regulations for the procedures for nomination and registration of candidates, for the voting, verification of voting results and counting, and for the accreditation of observers. The NEC enjoys broad confidence of the political parties, civil society and the electorate of Estonia.

CECs are permanent bodies with up to 13 members, appointed for four-year terms by the relevant County Governor or by the city council in Tallinn and Tartu. The CECs are chaired by the county or city secretary, which secures a close working cooperation of CECs with the local administration, which fund the CECs and support their operations. CECs are responsible for the instruction and the supervision of division committees' activities, as well as for the tabulation and verification of the voting results in the relevant county or city. CECs are entitled to invalidate decisions of DCs from their county and to suspend DC members violating the law or regulations or instructions of superior electoral committees.

The division committees, composed of a chairperson and up to eight members, are responsible for the administration of the elections at polling station level. In contrast to higher level committees, DCs are temporary bodies that are partially nominated by political parties. The DCs are appointed by the local government councils at least 20 days before election day. Half of the members are nominated by the municipal or city secretary, while the other half are nominated by the political parties participating in the elections, with each party nominating no more than one candidate per DC.

In some municipalities, it appeared that there were not enough party nominations, perhaps due to the low pay of the DC members, and thus the required number of members were appointed by the municipal council, as provided by law. The OSCE/ODIHR EAM noted that the majority of the DC members had previous experience. The nomination process appeared to have gone smoothly, and no significant concerns were reported to the EAM. In the Narva region, the Pro Patria - Res Publica Union said that not all of their nominees had been appointed, although some had been appointed to DCs as alternate members.

In order to promote a proper check and balance at the polling stations, the NEC could consider formally reminding all political parties to nominate members of division committees prior to the deadline.

C. REGISTRATION OF CANDIDATES

An eligible citizen may be a candidate on a party list or run as an independent candidate. For the 4 March 2007 elections to the Riigikogu, 11 parties and 7 independent candidates submitted nomination documents. The parties represented in the previous Riigikogu and

the recently registered party of the Greens nominated the maximum number of 125 candidates. No nominated party list or candidate was rejected. Two candidates withdrew their candidacy within the deadline of three days after registration. In total, there were 975 candidates registered.

Political parties submitting candidate lists must pay a deposit equal to the amount of two minimum salaries per candidate. Independent candidates are subject to the same requirement. The deposit is refunded to the party if its candidates receive at least five per cent of the votes on the national level. Independent candidates receive a refund if they are elected. Four of the political parties registered for the election told the OSCE/ODIHR EAM that they did not nominate the full number of possible candidates due to the requirement to pay a deposit for each nominated candidate.

D. VOTERS LISTS

The preparation of the voters lists is organized by the population registry. Twenty days before election day polling cards are to be sent to voters in Estonia, indicating their personal data in the population register, the municipality or city and the polling division number where they are included in the voters list, and the location of their regular polling place.

The voters lists must be delivered to all polling divisions no later than 7 days before election day, when the advance voting starts in all polling stations. Requests for correction of personal data or inclusion in the voters lists are made to the municipality or city secretary. The relevant DCs are notified regarding decisions for corrections or inclusions and make the appropriate changes to the lists. A denial of application can be appealed to the local administrative court. The law provides that voters who find that they are not on the list on election day and who can prove their eligibility and identity are added to a Supplemental Voters List and are allowed to vote.

The system of preparation of the voters lists is transparent and during previous elections the office that maintains the popular register demonstrated the capacity to prepare reliable and accurate voters lists. According to the NEC, there were 897,243 voters eligible to cast a ballot in the 4 March elections.[10]

VII. INTERNET VOTING

A. OVERVIEW

Remote internet voting in the Riigikogu election was the first countrywide use of the internet as a voting method in a parliamentary election in an OSCE participating State. It was first introduced in the 2005 local elections. Internet voting is an additional voting method and is not obligatory.

---

[10] However, the NEC did not announce the preliminary number of voters according to the popular register as of one month before the elections, which was the base for the preparation and printing of the Voters Lists used in the polling stations.

The cornerstone of the internet voting system in Estonia is the use of a personal identification document (ID card) which is legally accepted for identification via the internet and to sign documents digitally.

The legislation introduced for the 2007 Riigikogu elections, similar to the legislation for local elections, provides that eligible voters with the digitally-enabled ID card may cast their ballot via internet during the advance voting period, from six to four days before election day. The law also permits voters to change their votes during the advance voting period, either by voting again through the internet or by casting a ballot paper at a polling station. The law establishes the primacy of paper balloting. The voter can change his/her vote an unlimited number of times electronically, with the last ballot cast being the only one counted, but a vote cast by paper is final and annuls all internet votes cast by the voter.

The introduction of remote internet voting prior to the 2005 municipal elections generated interest and some political controversy within Estonia. Two political parties, the People's Union and the Centre Party, informed the OSCE/ODIHR EAM that they had objected to remote internet voting on the grounds that the secrecy of the vote could not be ensured and that the system was not transparent, since the voting process could not be observed. These parties continue to oppose the system. Among citizens, there appears to be acceptance of internet voting, although its actual use remains limited, with 5.4 per cent of voters casting ballots choosing the internet as a voting channel in the 2007 election.

Remote internet voting is similar in many respects to remote postal voting, offering some of the same advantages, such as increased access of voters to the voting process, and some of the same disadvantages, such as the impossibility to observe the voting process fully and to ensure the fundamental rights of a free and secret vote. In addition, internet voting does not provide for a fully transparent counting procedure.

B. DEVELOPMENT AND INTRODUCTION OF INTERNET VOTING

The development of internet voting was closely linked to the development of the digitally-enabled ID card and was seen as a potential additional use of the digital capacities of the ID card. After passing the Identity Documents Act in 1999 and the Digital Signature Act in 2000, the first ID cards were issued in January 2002. As of November 2006 over one million digitally-enabled ID cards had been issued. The ID card contains certificates for legally accepted authentication and for digital signature stored on a chip embedded in the card. The ID card is compulsory and can be used for a number of State services provided electronically, including tax filing, as well as for insurance, public transportation, and other purposes.

In 2001 the Ministry of Justice announced intentions to introduce internet voting, and two preliminary technical analyses on internet voting were published by Estonian academic groups. According to the NEC and other interlocutors, the main goals of introducing the internet modality of electronic voting were to sustain and increase voter turn out, attract younger voters, and improve the convenience of voting.

In 2002 the Riigikogu adopted a new Riigikogu Election Act which provided for voting via internet with the use of digitally enabled ID cards and that the introduction of internet

voting would not take place before 2005. Two of the political parties then in Parliament opposed the introduction of voting by internet.

In August 2003, the NEC initiated an internet voting project, appointing a project manager and a six member steering committee. The project group finalized its General Concept paper in January 2004, after a security analysis in December 2003 from an expert group with IT specialists from the private sector and academics. On the basis of the General Concept paper, the NEC published a tender in March 2004, which was awarded to the Estonia-based software development company "Cybernetica AS". The NEC contracted the software developer in April 2004.

Prior to the 16 October 2005 local elections, specific legislation was adopted regulating the introduction of remote internet voting for those elections. The legislation enabling internet voting for the local elections was not supported by the Estonian Centre Party and the Estonian People's Union.

The President of Estonia at the time, Mr. Arnold Rüütel, refused to promulgate the law. He eventually referred the issue to the Constitutional Court, after the Riigikogu passed the legislation on three occasions with some modifications. The President's challenge was based on the argument that permitting voters who voted electronically to change their vote put them in a situation of inequality compared to voters who voted only by paper ballot, as the latter could not change their votes. The Constitutional Court, supported by an opinion of the Chancellor of Justice, found that since all voters have the possibility to vote electronically, the law did not violate the equality of voters.[11] In the opinion of Court, the possibility of recasting a vote serves a preventive function by reducing the motivation to influence the voter illegally and is therefore an essential supplementary guarantee for the secrecy of voting in remote electronic voting.

After this decision, the President promulgated the amendments, and a system enabling remote internet voting was developed and used in the 2005 local elections on a nationwide scale. In June 2006, the Riigikogu Election Act was amended to provide fully for remote internet voting in the parliamentary elections. There were no legal challenges to the use of remote internet voting for the Riigikogu election.

Nevertheless, some improvements to legislation could be made in relation to internet voting. The Riigikogu Election Act does not contain provisions regulating the security of the internet voting system. It does not foresee the responsibility of any institution, nor does it provide for specific grounds for application of sanctions in case of failure of the system.

The OSCE/ODIHR recommends that legislation in relation to internet voting be adapted accordingly.

---

[11] Judgment of the Constitutional Review Chamber of the Supreme Court number 3-4-1-13-05, "Petition of the President of the Republic to declare the Local Government Council Election Act Amendment Act, passed by the Riigikogu on 28 June 2005, unconstitutional," 1 September 2005.

C. GENERAL DESCRIPTION OF THE INTERNET VOTING SYSTEM

1. Actors, Roles and Responsibilities

The NEC is responsible for the overall administration of voting by internet. The NEC's Internet Project Director manages the technical aspect of the process. A number of other organizations also have a role in the process, including the following:

The Ministry of the Interior's Population Registry is responsible for providing the list of eligible voters and issuing national ID cards.

Estonian Informatics Centre is a part of the Department of Data Communications, the institution responsible for government IT infrastructure. The Centre is responsible for the physical hosting of the servers, as well as for providing the internet connections.

Sertifitseerimiskeskus AS is a private company contracted by the government to provide certification authority for authentication and digital signing to Estonian ID card holders. It is the only certification authority in Estonia able to issue legally accepted digital certificates proving an individual's identity.[12]

Cybernetica AS is a private company that developed the software for internet voting according to the specifications developed by the NEC. After delivery and testing of the software package, Cybernetica was not involved in the process and did not have contractual obligations to operate or maintain the software.

KPMG Baltics AS is a private auditing company contracted on the basis of a tender to audit the internet voting system. KPMG Baltics reviewed and monitored security sensitive aspects of the process continuously, such as updating the voters list, transfer of votes between components of the system, and the process of counting the votes.

2. Design and Components[13]

The internet voting process is designed to parallel the paper voting process to the maximum extent possible so as to be familiar and accessible to voters. The system checks the identity of the voter, provides a "ballot" to the voter, obtains the voter's signature, and finally allows the vote to be cast. Like remote postal voting, the system is designed to protect the anonymity of the voter through a "double envelope," in which the content of the voter's electronic ballot is not decrypted until it is separated from the voter's identity after the expiration of the advance electronic voting period.

For the hardware, operating system, and software components of the voting system, the NEC internet voting project team chose to use common, standard, and proven technology, rather than proprietary technology.[14] The Estonian internet voting system consists of following components (see diagram in Annex 2): Voter Application, Internet Web Server,

---

12 This company does not certify the internet voting equipment or software.

13 The components and functioning of the internet voting system is further described in the "E-Voting System Overview", National Election Committee, Tallinn, 2005, available on the NEC website.

14 "Debian" was used for the operating system, "Apache" for the server platforms and "Python" for server side scripting. The voter application used to log on and cast the vote via the web browser is written in C / C++.

Certification Server, Vote Storage Server, and the Counting Server. The Cybernetica AS software development company developed all of these components except for the Certification Server.

Voter Application: The Voter Application is the software application that voters use to cast the vote via internet. There are three types of voter applications, for three different operating systems (Windows, UNIX and Apple MacOS).[15]

Internet Server: The Internet Server application has several functions.[16] It hosts a webpage on the NEC internet site, receives the request to vote, provides the public key of the Vote Counting Server to the voter, receives encrypted and signed votes from the Voting Application, and forwards these votes to the Voting Server. During the voting process the Internet Server is physically hosted in a secured space of the Estonian Informatics Centre. Besides the operating system and web server, the Internet Server hosts the voting application and three lists: the voters list, the list of candidates, and the list of election districts.

Certification Server: The Certification Server is responsible for authentication of the voters by checking whether the certificate of a voter is valid. It is managed by the company "Sertifitseerimiskeskus AS".

Vote Storage Server: The role of the Vote Storage Server is to connect with the Certification Server to authenticate the voter and thereafter store the encrypted votes. At the end of election day, the vote is separated from the "digital envelope" containing the voter's digital signature and transferred by a CD-ROM to the Counting Server. The Vote Storage Server is also physically hosted at the Estonian Informatics Centre and is connected through the firewall to the Internet Server.[17]

Counting Server: The Counting Server is an offline, stand alone computer not connected to any network. It is stored at a secure location by the NEC, to be used at closing time of the elections. The role of the Counting Server is to count the votes once decrypted. The decryption of votes is performed using a Hardware Security Module connected to the Counting Server.

Hardware Security Module: The Hardware Security Module generates the public and private key of the Counting Server, which are respectively the public key used for encryption of votes and the secret key used for decryption of votes.[18]

3. Voting Process

The computer used by the voter must have a smart card reader installed in order to process the digitally-enabled ID card, as well as two PIN codes associated with the ID card.[19] With

---

15 The application designed for Microsoft Windows is integrated into an ActiveX Control component that is based on the Microsoft technology platform. It is accessed with normal internet browsers and hosted on the web page of the Internet Server. The applications designed for UNIX and MacOS operating systems are stand alone applications that need to be installed on the computer. These applications can be downloaded from the NEC website.

16 The Internet Server is built on Debian Linux operating system with an Apache web server.

17 The Vote Storage Server is built on Linux Debian Operating System.

18 The Hardware Security Module is produced by SafeNet (model Luna SA).

these elements, an eligible voter can cast his/her vote via internet from anywhere in the world.

The voting interface is provided through the Voter Application via an internet browser. Voters using Microsoft Windows open the internet web address www.valimised.ee with their browser, while for voters who use Mac OS or Linux the voting interface is a stand alone program.

The Voter Application requests data from the voter's ID card, which must be inserted into the smart card reader. To proceed, the voter types a personal code (PIN1) to identify her/himself. Through an SSL connection between the Internet Server and the voter's computer, the Voter Application checks whether the voter is on the voter list. If the voter is not on the list, he/she receives a message to contact the Population Register authority.

If the voter is on the voter list, the Voter Application will give information as to whether the voter has already voted.[20] If the voter has not already voted, the Voter Application displays the list of candidates by party according to the voter's electoral district. The voter chooses one candidate on a party list (or independent candidate) by clicking on the name of the candidate and then confirming the choice. In case the voter has already voted, the Voter Application will request the voter to confirm whether he/she wants to recast the vote.

The vote is encrypted with the public key of the Counting Server. In order to cast the vote, the voter must type in a second personal code (PIN2). This code is the confirmation that it is the voter him/herself who is voting. The PIN2 enables the card to sign the encrypted vote.

The encrypted vote is then sent to the Internet Server which checks whether the digital signature corresponds to the session owner – in other words, if the same voter initiated and finished the voting process.

The Internet Server then forwards the encrypted vote to the Vote Storage Server, which requests a check of the validity of the voter's certificate from the Certificate Server.[21] If valid, the Internet Server verifies the digital signature using the voter's public key from the voter's certificate.

At the end of the voting process, the voter receives an on-screen confirmation that the vote has been cast. The encrypted vote remains on the Vote Storage Server until counting and tabulation is performed on election day.

During the three days of advance voting by internet, the NEC updates the voter list daily with any new voter records provided by the Population Register.

---

19 Smart card readers can be purchased separately at a cost of approximately 20 Euro. Installation software must be downloaded. Some banks made the card readers available at reduced cost.

20 The Vote Storage Server checks whether the voter has previously voted.

21 If the Certification Server were to fail or be unavailable, voting by internet would not function. The OSCE/ODIHR EAM was informed that there is no Service Level Agreement with the Sertifitseerimiskeskus AS that would assign responsibility in this eventuality.

4. Counting Process

After receiving lists from polling stations regarding any voters who cast a paper ballot during advance voting and who also cast a vote by internet,[22] NEC staff mark the corresponding electronic votes on the Vote Storage Server as "not to be counted". They then burn a CD from this server containing the last electronic vote of each voter. This CD is sealed and given to the Chairman of the NEC.[23]

The counting of the electronic votes takes place on election day, one hour before the closing of the polling stations. The encrypted votes are transferred to the Counting Server by a CD-ROM.[24] The Counting Server decrypts the votes using the Hardware Security Module and counts them. By law, at least half of the NEC members, including the Chairman or Deputy, must be present in order to decrypt and count the votes. Decryption of the votes is performed by the Hardware Security Module (HSM). In order to enable the HSM, six physical keys must be inserted. Seven keys are in possession of the NEC members and two are held by the operators; four of the keys used must come from the NEC members.

After the votes are counted on the Counting Server, a new CD is burned with those results and they are taken to a personal computer where the results are processed so that they can be viewed in a spreadsheet.

For the 4 March parliamentary elections, counting was conducted in the Parliament building by NEC operators in presence of the NEC, auditors, press, and domestic and foreign observers. After the votes were decrypted and counted, the auditor announced that everything had been done in accordance with the procedures. While the OSCE/ODIHR EAM was present for the counting process, it was – as with any electronic counting – not possible to observe the actual counting of the votes, since this took place within the Counting Server.

The personal computer used to read the CD containing the results was connected to the internet during part of the time the counting procedure was conducted. In addition, it was not clear that this computer had been subject to the same security safeguards as other elements of the system.

The OSCE/ODIHR recommends that the NEC review the process of counting internet votes and announcing the results to ensure that all devices used are subject to adequate security measures.

D. CERTIFICATION, TESTING AND AUDITING

1. Certification

The Riigikogu Election Act does not provide specifications or minimum prerequisites of the internet voting system, nor the obligation to certify or test the system.

---

22 See section VII H below, Integration of Internet Voting With Paper Voting System.

23 The process of cancelling votes is logged in a file called "Log2".

24 All entries transferred to the Counting Server are logged in a file called "Log3".

The internet voting system was not officially certified by an independent body. The NEC stated that it had organized informal reviews of the software by representatives from banks, universities, state officials and ICT specialists at various times. The results of these reviews were not made public.

2. Testing

After local elections in 2005 some improvements were made to the software. The new version was internally tested by the Cybernetica company, including a load test[25] with over 600,000 votes, and delivered to the NEC with the test results in January 2007. The new version was formally accepted by the NEC.

Although testing was done on separate components of the internet voting process, no full end-to-end logic and accuracy test was performed on the system. Two weeks prior to the three-day advance electronic voting period, the internet voting system was tested by the public (4,000 voters) and by contracted testers. This test focused only on the operation of the Voting Application and the Vote Storage Server.

A limited test of the counting process was performed by the NEC two days prior to the advance voting period, directly after having set up the hardware and installing the software components. Only nine test votes were processed and counted.

In the assessment of the OSCE/ODIHR EAM, given the fact that the software had recently been modified, a more extensive counting test would have been warranted, as well as more thorough testing of the entire system.

The OSCE/ODIHR recommends that a full scale end-to-end test be performed on the entire system prior to each election. This would include all of the components and all transactions in the process. It is also recommended to test the system with a known outcome, for example, by predetermining how test voters should vote and comparing this with the actual tabulation of their votes.

3. Auditing

Auditing is conducted regarding all the technical activities related to internet voting which are under the control of the NEC. The auditing is conducted by an external auditing company, "KPMG Baltics," which monitors and checks the activities of the NEC against written documentation describing the necessary steps and procedures, including preparation of the hardware; installation of the operating system and software; testing; loading of election data; maintenance and renewal of election data; closing; and counting of the final results. In addition to the formal auditing, all of the above steps were videotaped. After the election, KPMG delivered a final report to the NEC. The report is not public.

The auditing undertaken appeared to be conducted in a very thorough manner. However, it does not appear that the auditors were asked to examine whether the procedures in place were adequate to achieving their objectives.

---

[25] A load test is a test in which a software system is made to process a high volume of data to check its ability to perform well during peak periods of use.

KPMG did not audit the source code for the system. According to the NEC, the source code was audited by an independent expert in January 2007, although it is not clear if this was done on a formal basis or what report was made to the NEC.

KPMG was not requested to conduct any post-election audits of the internet voting process.

The OSCE/ODIHR recommends that in addition to the audits of the process now conducted, all components of the system, including the source code, should be audited by an independent body in accordance with publicly available specifications, with all reports made public.

E. SECURITY

1. Overview

The core security architecture of the internet voting system is based on the separation of the vote storage server connected to the internet and the offline counting server (and the Hardware Security Module). This means that outside attackers cannot manipulate the counting software because this part is never connected to the internet. In addition, no one can decrypt votes other than the NEC members together. The private key does not leave the Hardware Security Module.

The NEC staff running the internet voting project were very knowledgeable about, and aware of, potential security threats. Technically, it appears that a number of security mechanisms were used in order to deter, detect, and prevent possible external attacks and internal malfeasance that would compromise the secrecy of the vote or the integrity of the voting process.

The servers and applications were installed and configured from component elements, starting with the operating system, to ensure that they were free of viruses, Trojan horses and other malware at the time of installation.

The installed voting software was checked to ensure that it was identical to the software received by comparing the checksum on the version installed on the servers with the checksum provided by Cybernetica AS. However, as noted above, it is not clear to what extent the software was formally audited after being received from the company.

According to the NEC, only the necessary functionality was installed on the servers, and the open ports and services to the internet were limited to those required by the voting process. There is a firewall between the Internet Server and the Vote Storage Server. Traffic to the Internet Server was monitored by system operators to attempt to identify any abnormalities or external attacks.

The Internet Server and the Vote Storage Server were located in a locked room which was guarded by a policeman and continuously filmed. In addition, these servers were sealed.[26] The Counting Server was sealed and stored in a vault at a separate location. All procedures

[26] Whenever seals are put on the server, the auditor notes the corresponding seal number in the protocol. Before unsealing, this number is checked against the protocol.

of the system operators were observed by an external auditor and checked against a user guide. All procedures were filmed.

The secure storage of votes was implemented by a tamper-evident Hardware Security Module which generates the digital key pair without revealing the private key. This module was stored in a secure place and was only used before the election for the set up procedure and after the election for the counting procedure. To ensure the availability of the election results in the event of failure of the Hardware Security Module, there was a backup of the private key which was kept secret by one of the members of the NEC. The existence of a backup key creates a hypothetical security risk, which was assessed by the NEC as being more acceptable than the risk of not having the results available.

2. Authentification of Voters

The authentication of voters is based on the Estonian ID card, which allows electronic authentication and digital signing of documents with two pin codes. While this system enables the use of internet voting, it is not possible to verify that the person entering the pin codes is in fact the voter (for instance, the voter could provide the ID card and pin codes to another person). However, the NEC considers that voters are unlikely to provide the ID card and pin codes to another person, since with this personal data it is possible to impersonate the individual using his/her legally binding electronic signature.

3. Secrecy of the Vote

Secrecy of the vote is composed of two aspects: the secrecy of the voting environment and the anonymity of the vote once cast. Because the voter is not voting in a supervised and controlled environment such as a polling station, it cannot be ensured that the voter is casting his/her vote in secret. Therefore, the Estonian internet voting system relies on the possibility of recasting the vote, which is intended to protect against violation of the secrecy of the vote or against possible coercion of the voter. According to the NEC and other interlocutors, the fact that a voter can recast his/her vote reduces incentives for potential coercion or vote-buying, since any person attempting such measures could not be sure that the vote cast under pressure or inducement would in fact be the final vote cast by the voter.

However, the OSCE/ODIHR EAM noted that one technical aspect of the system undermines the objective of the recast possibility. Namely, the vote storage server records the time that each voter casts his/her last electronic vote. This log, which is available to political parties and observers, could potentially be misused to know whether a voter did in fact recast his/her vote electronically. [27]

The second element of secrecy, the voter's anonymity, is secured by the fact that the vote storage server separates the voter's signature from the vote prior to decrypting the vote and by the secure storage of the private key used to decrypt votes.

The OSCE/ODIHR EAM recommends that the NEC consider modifying the design of the internet voting system so that the time of voting is not recorded. In the interests of

---

[27] Out of the 31,064 total votes cast by internet, 796 votes were recast, some 2.5 per cent.

maintaining the transparency of the system, however, the log should continue to be available to observers.

4. Security of Internet Communication

The communication over the Internet between the voter and the vote storage server is secured by SSL (with client side authentication). In addition to the encryption of the exchanged messages, this provides for the secrecy and integrity of the communication.

There is a risk of "denial of service" attacks in which external persons attempt to overwhelm an internet server so that it is unable to carry out its functions. These type of attacks cannot be prevented, although there are methods to protect against them. The NEC was aware of the issue, and during the advance voting period it informally arranged to have experts from different internet providers monitor network traffic for any unusual activity. However, there did not appear to be a formal plan to deal with this risk, nor did there appear to be any institution apart from the NEC formally assigned the task of comprehensively monitoring network traffic.

The internet voting system cannot prevent voters from using computers which have malware installed that could compromise the security of their vote. The NEC warns voters on the official web page only to use the internet voting system if their computer is free from malware. One potential threat is that malicious software could "spoof" the Internet address used for voting, causing a voter to believe that he/she is casting a vote on the official website but in reality interacting with another website.

The NEC stated that they could not prevent malware installed on a voter's computer from interfering with the voting process but had taken steps to limit the likelihood. These steps included advising voters to type in the correct IP web address rather than click on a link to the NEC website posted on another site, and publishing the server certificate in newspapers and on the NEC website so that a voter can verify that he/she is connected with the vote storage server. The voter could also obtain information to verify whether he/she has the proper voting application.

The vote storage server itself is monitored physically, but there was no check to detect whether there had been any unauthorized access to the server through the internet. No checks were conducted on the software to ensure that it had not been modified. The NEC staff informed the OSCE/ODIHR EAM that they were confident that the security measures implemented made such checks unnecessary.

The OSCE/ODIHR recommends that monitoring and response to potential threats coming from the internet should be more systematic and include a plan to deal with such threats, with well-defined roles for each institution. In addition, the monitoring of the Vote Storage Server should be improved to provide greater assurance that no unauthorized access via the internet has affected the integrity of the data.

F. VOTER EDUCATION

Prior to the elections, the NEC organised a public information campaign to draw attention to internet voting as a supplementary way of voting. This was done through different media channels, including television, radio, printed materials, and internet. In addition to

information on how to vote, the NEC website also provided a comprehensive and user friendly 'frequently asked questions' summary.

Before the parliamentary elections, from 15 January through 19 February, eligible voters were given the possibility to test the internet voting system in a mock election.[28] This public testing was organised in order to educate voters and encourage them to solve potential difficulties that might emerge prior to the real advance voting, such as acquisition of card readers and software, updating expired ID card certificates, and renewal of PIN codes. There was no test of the counting software using the votes cast in this mock election.

G. ACCESSIBILITY

Once the voter's computer is technically prepared and once the voter has obtained the necessary valid digital certificates and PIN codes, the system appears to be relatively easy to understand and operate. Voters must in some instances scroll down to see all candidates on the list, although there were no indications that this posed difficulties. Unlike the paper balloting, the system does not allow voters to cast a blank ballot or to spoil their ballot.

After the 2005 municipal elections, a "Help" function explaining the internet voting process in Russian and English languages was added to the NEC website (in addition to Estonian). However, the voting interface itself is only available in the Estonian language.

Given the considerable percentage of Estonian citizens who consider Russian as their first language, and given that some of these voters would meet the Estonian government's definition of a national minority, the OSCE/ODIHR recommends that consideration be given to making the voting interface available in the Russian language.

H. TRANSPARENCY

The management of the internet voting system was very transparent, although highly centralized. The NEC stated that all political parties and accredited observers were invited to observe the administration of internet voting in every phase of the process. This included the opportunity to review the documentation of the system, the source code of the software, and all of the setup procedures in the process. The OSCE/ODIHR was granted extensive access to the process, and NEC staff were forthcoming with information requested.

However, it appears that no political parties exercised their right to have access to the process and to observe the setup procedures, nor did NGOs or civic associations attempt to observe the process in a comprehensive manner.[29] Although the NEC organized a short training course on the system and invited political parties and the public to attend, only two persons completed the course. This lack of independent oversight by domestic organizations meant that for many stages of the process in which security would be

---

[28] Voters were asked to vote for the "king of the forest," with various animals as candidates.

[29] Domestic observers may have been present for some of the setup procedures, but if so, this was on an exceptional basis. The OSCE/ODIHR EAM never saw domestic observers at any of the pre-election procedures that it was able to attend.

enhanced by the presence of independent observers, security in effect relied only on trust in a small group of NEC staff and the private auditor.

One reason cited by some political party representatives for not observing the internet voting process was their overall trust in the internet voting system and in the NEC's administration of the system. Another reason cited was the lack of qualified personnel who could understand the process and provide effective control, or lack of funding to contract such experts. Some political parties told the OSCE/ODIHR EAM that it could be useful for political parties to receive additional funds to pay qualified experts who could observe the internet voting system on their behalf.

While trust in the system can be positive, that trust should be based on a full understanding of the security and transparency issues related to internet voting. Relatively few interlocutors, apart from information technology experts, seemed fully informed about these issues. For example, one view frequently expressed to the OSCE/ODIHR EAM from political party and civil society representatives was that internet voting is comparable to internet banking. According to this view, since internet banking can be made secure, internet voting can also be trusted.

However, it should be noted that while internet banking and internet voting appear to be alike from the point of view of the user, these two processes are substantially different. Internet banking requires the recording of the complete transaction with events traceable to every person involved in the process. Internet voting has a different requirement, as it should not be possible to link the vote with the voter.

The OSCE/ODIHR recommends greater participation of parties and civil society in monitoring of the internet voting system to provide an opportunity to identify potential weaknesses and security concerns. The OSCE/ODIHR further recommends consideration of a more defined division of duties among the staff implementing internet voting such that no one person would be involved with the entire process.

In addition, the OSCE/ODIHR recommends that unless the challenging issues pertaining to internet voting outlined in this report can be effectively addressed, the authorities should carefully reconsider whether the internet should be widely available as a voting method, or alternatively whether it should be used only on a limited basis or at all.

I. INTEGRATION OF INTERNET VOTING WITH PAPER VOTING SYSTEM

The NEC provided the CECs with a separate list for each polling division that contained the names of those who had voted via the internet. The DCs marked the voter list next to the name of the voter who cast their ballot by the internet. Voters who cast a vote by internet were not allowed to cast a vote on election day itself.

If it was noted that a person had voted by the internet and voted by paper ballot during advance voting, the DC chair sent this information to the NEC via internet in a password-protected web-based program. The NEC then cancelled that person's internet vote.[30] The advance paper ballot was counted in the normal counting process. The DCs were also required to print the list of cancelled internet votes and sign it, so that during the

[30] For accounting purposes, the internet votes were cancelled but not deleted.

verification phase after election day, the NEC could check whether the internet votes cancelled over the web interface corresponded to the printouts.

VIII. ELECTION CAMPAIGN

A. OVERVIEW

The election campaign officially started on 23 January 2007, after the registration of candidates, and lasted until the day before election day. The campaign was generally low-key and was mainly conducted via advertising in the mass media, small-scale meetings and events, and door-to-door campaigning. There were few major political rallies. For the most part, the parties concentrated their attention on domestic political issues such as economic policy, demographic indicators, increased resources for education and health care, and social inequality.

Issues such as citizenship and the use of Russian language in public life were not a major focus of the campaign. However, there was considerable discussion regarding the issue of the "Bronze Soldier" monument, which stood in the centre of Tallinn. On 16 February, parliament passed the Removal of Forbidden Edifices Act which defined the monument as a forbidden edifice and charged the government with organization of its removal within 30 days of the entry into force. The monument became the site of small-scale protests and counter-protests. The issue generated considerable emotion and attracted the attention of domestic and international media. The president refused to promulgate the Act prior to the election, as he found it in contradiction with the Estonian Constitution.[31]

B. PROHIBITION ON OUTDOOR POLITICAL ADVERTISING

Estonian legislation overall provides sufficient guarantees for the freedoms of speech and assembly fundamental to the conduct of democratic elections. However, a 2005 amendment to the Riigikogu Election Act that prohibits outdoor political advertising during the official campaign period considerably influenced the conduct of the campaign and raised concerns as a possible disproportionate restriction on freedom of expression.[32]

According to representatives of political parties, the amendment was originally intended as a response to public opposition to extensive outdoor political advertising during previous election campaigns, especially the use of building-sized billboards. The need to create a "level playing field" for all political parties and candidates, and to reduce campaign spending, were also cited by parties as a reason for the ban.

In September 2005, the Chancellor of Justice sent a report to the parliament that the prohibition may be unconstitutional and asked parliament to review the provision. The Chancellor noted that "substantial fundamental rights" were being restricted. While acknowledging that the aims cited by parliament in imposing the restrictions were

---

31 The monument was relocated on the night of 26 April 2007, generating violent protests in Tallinn. Subsequently, there was a series of internet "denial of service" attacks against Estonian websites.

32 Article 5-1 states that "Advertising an independent candidate, political party or person who runs as party nominated candidate, electoral coalition or person who runs as candidate in the list of electoral coalition, or their logo or other sign or programme on a building, facility, inner or outer side of public transport vehicle or taxi, or any other political outdoor advertising shall be prohibited during the active election campaigning period."

important, he noted "the limited efficiency of the measure" in achieving those aims could make the provision disproportionate.[33] While the parliament considered the issue in 2006, it did not amend the provision in this respect.

Indeed, most political parties and other interlocutors informed the OSCE/ODIHR EAM that the prohibition had proved to be overly broad and had unintended consequences. They stated that the campaign had lengthened compared to previous elections, as some political parties had put up outdoor advertising in the period before the official start of the campaign. Parties and media experts also claimed that the prohibition led to increased political advertising in the media during the official campaign and that these factors would increase the costs of the election campaign rather than create a "level playing field".

In addition, lack of clarity in Article 5-1 of the amended Election Act led to uncertainty on the part of candidates and political parties as to what campaign activity was prohibited. The NEC informed the OSCE/ODIHR EAM that it had been asked many questions as to what was the proper way for a candidate or political party to organize an outdoor campaign event without breaking the law. The NEC did not issue any instruction regarding this issue, considering it outside the scope of its competency. However, a memo was prepared on enforcement of the provision, presumably by the Ministry of Interior. The memo noted the concerns of the Chancellor of Justice and instructed the police to interpret the law restrictively to avoid infringing on political rights.

Several complaints regarding outdoor political advertising were reported during the election campaign, with at least two resulting in misdemeanour charges being filed for advertising materials displayed on vehicles and in a shop.[34] In Tartu, the police intervened to ask parties to remove signs on outdoor tents set up by the Reform Party and the Social Democratic Party respectively; however, the tents themselves were permitted to remain.

The OSCE/ODIHR recommends that the prohibition on outdoor political advertising during the official campaign period be eliminated, or substantially narrowed in scope, in order to eliminate undue restrictions on fundamental freedoms.

C. POLITICAL PARTY AND CAMPAIGN FINANCING

Political parties can be financed through individual donations, membership fees and loans, and income earned on assets. Political parties represented in the parliament have the right to allocations from the State budget, with the amount of the allocation being proportionate to the number of seats received in the Riigikogu elections. Parties not meeting the threshold for representation in the Riigikogu are also entitled to financing from the State budget if they obtain at least one per cent of the votes.[35]

All political parties and independent candidates conducting an election campaign are required to submit a report to the Riigikogu Anti-Corruption Act Enforcement Committee within one month after election day on their campaign expenditures and the sources of

---

33 Annual Report of the Chancellor of Justice. Tallinn, 2006. p.35. www.oiguskantsler.ee

34 On 22 February, a complaint was filed in Jogeva Courthouse regarding a Centre Party candidate. On 27 February, a case was brought before the Administrative Court of Tallinn regarding a People's Union candidate.

35 Article 12^5 of the Political Parties Act.

funds used.[36] These reports are publicly available; however, several interlocutors, including political party representatives, told the OSCE/ODIHR EAM that the reports are limited in detail and are largely a formality.

The Chancellor of Justice had made a formal proposal to the Riigikogu to change the system of control of political party financing, finding the current system of reporting and supervision to be non-transparent, inefficient and without the possibility to exercise control over hidden contributions. He noted that the supervisory body should be independent from political interests and have appropriate legal and factual competence.

After legislation to amend the system was rejected by the parliament, the Chancellor filed an application to the Supreme Court on 16 February 2007 to declare the Political Parties Act to be unconstitutional in the part where it does not establish effective supervision over the financing of parties.[37] In a press release, the Chancellor also stated, "It is regrettable that under such circumstances present elections will not be fair." At the time of writing, the Court had not finally ruled on the application.

IX. MEDIA

The media environment in Estonia is open and pluralistic. Besides the Estonian public television, there are two nationwide private terrestrial television broadcasters and some 30 radio channels, including public radio. Public television and radio broadcasts some programming in the Russian language, but most Russian language programming available in Estonia originates in the Russian Federation and Latvia. There are over 100 news publications, including over a dozen national and regional daily papers, several of which are published in the Russian language.

There is no provision for free air time for political advertising during the election campaign. Political parties wishing to place advertisements must do so in the private media, as all advertising is prohibited on public television and radio. Private broadcasters granting time to a political party or candidate are required to grant similar opportunities for other election contestants. Apart from advertising, private electronic and print media are largely unregulated with respect to elections and election campaigns.

Public television and radio are regulated by the Broadcasting Council, which is composed of 9 members, five of whom are MPs representing different political parties and four of whom are recognized media experts. The Broadcasting Council has no authority over privately owned broadcasters.

On 27 November 2006, the Broadcasting Council adopted, by consensus, regulations for coverage of the election campaign by public television and radio. These regulations stipulated that news coverage of the campaign must be unbiased and that government officials should be covered in their official capacity in the news only if unavoidable. The Broadcasting Council did not carry out structured monitoring of the public broadcasters during the campaign, as this would have been done only in response to a formal

---

36 Article 65 of the Riigikogu Election Act.

37 Submission of the Chancellor of Justice to Supreme Court of Estonia, on 16 February 2007.

complaint. The Broadcasting Council did not receive any complaints regarding the public media's coverage of the election campaign.

The Broadcasting Council regulations also determined the schedule and format for six televised debates that were held on public television during the campaign. According to the Broadcasting Council's decision, political parties with at least 101 registered candidates were invited to take part in five of the debates, each of which focused on a different topic. One debate was set aside for independent candidates and parties with less than 101 candidates on their lists. A similar schedule was set for the public radio. This decision was a change since the 2003 parliamentary elections, in which no such requirement regarding the number of candidates applied.

Seven of the political parties registered for the elections nominated at least 101 candidates and were able to participate in five of the TV debates. The four parties which did not nominate more than 100 candidates for the Riigikogu elections criticized the decision of the Broadcasting Council regarding the participation in debates on public TV, claiming that they did not have equal treatment. The Broadcasting Council noted that the rules had been set well before the candidate registration period and that all parties had the opportunity to nominate at least 101 candidates.

X. COMPLAINTS AND APPEALS

The legislative framework provides effective remedies and mechanisms for resolving the electoral disputes. According to Chapter 12 of the Riigikogu Election Act, complaints may be made by a voter, candidate or political party by filing an application with the relevant CEC or with the NEC. A decision of the CEC can be appealed to the NEC, and finally, to the Supreme Court. The Election Act provides for a three-day deadline for filing and reviewing a complaint.

Very few complaints were made regarding the administration of the elections or election results. At least two complaints were filed with the NEC. The Constitutional Party alleged that votes for its candidates may have been declared invalid and asked for a recount of invalid ballots. The NEC denied the complaint on the grounds that it was not specific to any election committee and that all ballots had been recounted at CEC level. An observer alleged in a separate case that an insufficient number of DC members had been present when processing advance votes in one polling station. The NEC ruled that even though a formal violation had occurred, the remaining procedures had been followed and that the violation did not affect the results.

There were a few cases reported of vote-buying schemes during advance voting. According to the CEC in Tartu, at least four cases were brought to the attention of Tartu authorities, with at least two persons admitting that they had received compensation for their vote. The ballot boxes in question were sealed, and a police investigation was initiated. The CEC later determined that the scale of the offence was so limited that cancellation of the results was not warranted. Investigations were also reportedly launched in Jogeva County. The Public Prosecutor took an active approach by publicly urging that any case of vote-buying be reported to the police.

As noted above, the Chancellor of Justice filed an application directly with the Supreme Court regarding political party financing.

XI. PARTICIPATION OF NATIONAL MINORITIES

As of 1 January 2006, the total population of Estonia was 1,345,000 persons, some 68 per cent of whom were Estonians and 32 per cent of other nationalities. The largest ethnic minority groups are Russians (25.7 per cent), Ukrainians (2.1 per cent), and Belarusians (1.2 per cent).[38] Geographically, the minority population is concentrated in Tallinn, where they comprise 46 per cent of the population, Narva (95 per cent) and Kohtla-Jarve (82 per cent).

Estonia has made efforts to integrate national minorities, including through a law on cultural autonomy. Most political parties are not formed on a national or ethnic basis but attempt to include minorities to various degrees. There were two political parties contesting the elections which were self-identified as representing Russian-speakers. Neither of these parties reached the five per cent threshold.

Estonia is a party to the Framework Convention for the Protection of National Minorities.[39] However, its ratification contained a limiting declaration according to which Estonia interprets the term national minority in a way which is applicable only to Estonian citizens and not to other permanent legal residents who are not citizens of Estonia.[40] The Advisory Committee on the Framework Convention stated in its 2005 report that Estonia has adopted an inclusive approach regarding the applicability of the convention and that the declaration has only limited practical impact.[41]

OSCE participating States made a number of commitments towards national minorities under the Part IV of the 1990 CSCE Copenhagen Document, stating that they "will respect the right of persons belonging to national minorities to effective participation in public affairs, including participation in the affairs relating to the protection and promotion of the identity of such minorities."

An important issue related to effective participation in public affairs is the use of minority languages. Although Estonian is the state language, a large number of citizens communicate in Russian. According to the 2000 census, 15.3 per cent of Estonian citizens speak Russian as their mother tongue.[42]

---

38 Data from the Ministry of Foreign Affairs of Estonia, www.vm.ee.

39 The Framework Convention was signed on 2 February 1995, ratified on 6 January 1997 and entered into force on 1 February 1998.

40 The declaration states, "The Republic of Estonia understands the term 'national minorities', which is not defined in the Framework Convention for the Protection of National Minorities, as follows: are considered as 'national minority' those citizens of Estonia who reside on the territory of Estonia; maintain longstanding, firm and lasting ties with Estonia; are distinct from Estonians on the basis of their ethnic, cultural, religious or linguistic characteristics; are motivated by a concern to preserve together their cultural traditions, their religion or their language, which constitute the basis of their common identity."

41 Advisory Committee on the Framework Convention for the Protection of National Minorities, Second Opinion on Estonia. Adopted on 24 February 2005.

42 Data from the Ministry of Foreign Affairs of Estonia, www.vm.ee

All major political parties made attempts to attract Russian-speaking voters. Most parties advertised in Russian language media and distributed campaign materials in Russian. In the regions where Russian language is predominantly used, candidates conducted their campaign meetings in this language.
Regarding election administration, there did not appear to be any practical obstacle to the use of Russian language in areas in which significant numbers of voters speak this language. In Ida-Viru county, the working language was Russian in all division committees visited by the OSCE/ODIHR EAM during advance voting and on election day, although voters who did not speak Russian were able to communicate in Estonian.

However, it appeared that official election materials were provided only in the Estonian language, which could affect the ability of election officials and voters who primarily speak the Russian language to have a full understanding of election procedures and requirements.

The OSCE/ODIHR recommends that official voter information and election committee materials be translated into Russian for areas in which this language is widely spoken, in order to ensure a uniform understanding of election procedures by all voters and election officials.

Although the information on the official webpage of the NEC contains guidelines on how to vote via internet in the Russian language, the interface of the E-voting site was only in the Estonian language (see Section VII, Internet Voting).

XII. PARTICIPATION OF WOMEN

Equal rights for men and women are guaranteed by the Constitution of Estonia. Additionally, on 21 October 1991, Estonia signed the Convention on the Elimination of All Forms of Discrimination against Women. In the 2007 Riigikogu elections, 27 per cent of candidates were women, while 24 women were actually elected out of the total of 101 MPs.[43] This is an increase from the 2003 Riigikogu elections in which 19 women MPs were elected.

Women were generally well represented in the election administration at all levels, especially at the division election committees. Two out of the seven NEC members were women. However, relatively few women hold senior leadership positions in political parties.

XIII. ELECTION OBSERVATION

Generally, Estonian election legislation provides wide access to domestic and international observers in accordance with its commitments undertaken in the Copenhagen Document of 1990. According to the Riigikogu Election Act, activities related to elections are public, including the meetings of electoral committees and the counting and verification of votes. The law gives the NEC the authority to regulate the status of observers. The NEC issued Regulation 17 on 8 November 2006. Observers can be from foreign countries,

[43] Ibid.

international organisations (both categories accredited by the NEC), and by local government bodies, political parties, or private persons (accredited by the CECs). Applications can be submitted up to election day.
The NEC regulation clearly describes all rights and restrictions for observers. Observers have access to the meetings of all election committees and can follow all electoral activities, including the voting process, counting and tabulation of results. Observers are generally not entitled to see the voter lists, although political parties may have access to the lists after the elections "to the extent necessary" in cases of "justified interest."[44]

The NEC invited political party observers to all stages of NEC activity, including the set up and testing of the internet voting system. As noted above, party observers did not use this possibility regularly. The OSCE/ODIHR EAM heard concerns from some political parties and candidates regarding the impossibility of observing the entire internet voting process.

While Estonian legislation provides considerable opportunities for observers, no domestic NGOs observed the elections in a systematic manner, nor did political parties actively use the opportunity to deploy observers. Political parties informed the OSCE/ODIHR EAM that they did not generally have party observers in polling stations due to their confidence in the election administration, party representation in the polling committees, and a lack of volunteers.

XIV. ADVANCE VOTING

A. OVERVIEW

The Riigikogu Election Act provides for a wide range of possibilities for Estonian citizens to exercise the right to vote. Voters in Estonia could cast their vote in advance at many locations or on election day in their polling station of residence or at home, if immobile. Voters permanently or temporarily residing in foreign countries could vote in advance by mail, in person in the Estonian representations abroad or in Estonia in polling stations for voting outside the place of residence. During the three days of the second period of advance voting, citizens could vote by internet (see Section VII of this report).

It was apparent to the OSCE/ODIHR EAM that significant organizational and managerial efforts by the entire election administration were required to coordinate the various elements of the voting process. This included security, printing and distribution of ballots, accurate accounting for advance votes cast outside the polling divisions (including those cast overseas), timely and secure delivery of all advance ballots to the relevant DCs, and the accounting for votes cast by internet. Considering the multiple options for voting provided in the Riigikogu Election Act, the NEC developed very detailed instructions for a complicated, but transparent and safe system for preventing multiple voting and for an accurate account of advance votes.

---

44 Riigikogu Election Act, Article 23.2.

B. ADVANCE VOTING IN POLLING STATIONS

Advance voting took place during two periods. In both periods, advance voting was conducted in polling stations as well as for homebound voters. In the second period, voting was additionally carried out in custodial institutions. In the first period, 19 - 23 February 2007, voting was conducted in 17 polling stations, with one in each county,[45] three in Tallinn, and one in Tartu. The primary purpose of this period is to facilitate voting by those who are not currently in the location of their residence. Every Estonian citizen could cast his/her ballot in any of these polling stations.

After signing their name on the voter list, voters received a stamped ballot paper and two envelopes. After marking the ballot paper, voters placed the ballot in the small blank envelope they were provided and then placed that envelope into the larger envelope, which listed the voter's name, identification number and address. In the first advance polling period, a total of 14,099 citizens exercised their right to vote.

During the second period of advance voting on 26 - 28 February, voters could cast their ballot in the polling station of the division of their residence, or in any of those designated by the municipalities as polling stations for voting outside the polling division of residence.[46] In the latter, two separate sealed ballot boxes were used, one for the ballots of the residents and the other for the envelopes of voters residing outside the polling division. The procedure for voting outside the division of residence was the same as in the first period of advance voting, while voters casting their vote in their own polling station voted without outer envelopes.

In the limited number of polling stations visited by the OSCE/ODIHR EAM during advance voting in Tallinn, Narva, and Tartu, voting appeared to be well organized and overall conducted in a professional manner by at least three division committee (DC) members, as provided by law. Ballot boxes were properly sealed and stored in a secured and guarded place overnight. All necessary materials were present and the DC members seemed familiar with the voting procedures. However, in Narva region, with a substantial majority of a Russian speaking population, some DC members had difficulties with understanding the election procedures manual, which had been prepared only in the Estonian language.

C. OUT-OF-COUNTRY VOTING

Estonian citizens residing permanently or temporarily abroad may vote in person, by internet, or by mail through the Estonian embassies or consulates. Voting in embassies was conducted for a minimum of two days during the period 15 to 10 days before election day. Other overseas citizens sent their ballots to the embassies by mail. Counting of ballots from overseas voters was done in Estonia in order to ensure that voters did not also vote in a polling station in Estonia or by internet during advance voting. Only the votes received by the NEC from embassies by the fourth day before the election were taken into account.

---

45 Except for Harjumaa and Tartumaa counties which are close to Tallinn and Tartu.

46 One in each municipality or city.

D. TRANSFER OF ADVANCE BALLOTS

At the end of the advance voting period, the sealed ballots of those who voted outside their polling division were delivered by the DCs to their CEC. On the next day, 1 March, the CECs sorted these envelopes according to county and by the cities of Tallinn and Tartu. In the areas that the OSCE/ODIHR EAM visited, the process appeared to be carried out in an orderly manner overall. On 2 March, the CECs delivered the packets with advance voting envelopes to the NEC, and in turn received the packets containing the advance votes designated for their county cast in other counties or abroad. To complete the process of accounting for all ballots, the CECs sorted the envelopes with advance votes received from other counties by polling divisions and organized their distribution to the DCs in the county. In addition, DCs had to account for any voters who had voted by internet (see section VII, Internet Voting).

In some of the polling sites visited, procedures for the transfer of advance ballots were not consistently applied, perhaps due to a lack of clarity of instructions and written procedures for the transferring of these ballots. In one location, for example, the Chair of the DC took ballots home in unsealed bags. In another location in Ida-Virumaa, the OSCE/ODIHR EAM noted that a municipal official was involved in the process of transfer of advance voting envelopes, which would not be in accordance with procedures. In addition, the official was at the same time a candidate for the parliament. In another polling station, it did not appear that there was appropriate cross checking to ensure that the number of ballots was correct.

The OSCE/ODIHR recommends that procedures for the transfer of advanced ballots be reviewed and applied consistently at each step of the process. It is also recommended that the NEC work with the CECs to ensure that no candidates or other unauthorized persons are involved in the handling of ballots.

XV. ELECTION DAY

A. VOTING PROCESS

Consistent with an OSCE/ODIHR Election Assessment Mission, the OSCE/ODIHR EAM did not undertake a systematic and comprehensive observation of the polling and counting process for this election. However, the OSCE/ODIHR EAM did visit some 30 polling stations on election day in Tallinn, Harjumaa, Tartu, Narva, Parnumaa, Paldiski, Keila, Saue, Ida-Virumaa, Harku, and Rakvere. There were 657 polling stations on election day.

Election day was calm and the process of voting and counting did not encounter any significant problems. The OSCE/ODIHR EAM noted that polling places visited appeared to be well-organized and prepared for the voters. Polling stations visited opened at 09:00 and closed at 20:00, as required by law. Members of DCs appeared to be well-trained, and all were cooperative with the OSCE/ODIHR EAM. Poll workers appeared to check voter identification systematically. Eligible voters could be added to the supplemental voter list upon presentation of a document from the municipal council certifying residence. Use of voting booths appeared to be uniform at polling stations visited. After marking the ballot, the voter folds the ballot. A poll worker stationed at the ballot box stamps the outside of the folded ballot and supervises the casting of the ballot by the voter.

The number of voters at the polling stations visited generally ranged from 1,000 to 4,600. Voters voting in polling stations with more than 3,000 voters on the list were more likely to face queues of voters or crowded conditions. In some instances, voters were given ballots even when no voting booth was available, which could lead to voters marking their ballot openly or leaving the polling station with ballots.

The OSCE/ODIHR recommends that consideration be given to increasing the number of polling places and setting a limit on the number of voters per polling station. In addition, the NEC may consider guidelines for the allocation of voting booths based on the number of voters assigned to each polling station and whether voters should be given ballots prior to a voting booth becomes available.

B. COUNTING PROCESS

The counting of ballots at the polling stations began at 19:00, when three to five DC members went to a separate room in the polling place to count the advance ballots. Observers were allowed in the room, and could not leave until the advanced ballots had been counted.

The counting of ballots cast on election day began at 20:00, when the poll workers accounted for the unused ballots and the number of voters who had signed the lists. They then opened the ballot box in full view of observers and proceeded to count the ballots. The OSCE/ODIHR noted that the counting procedures used were not uniform. Some polling stations placed counted ballots in envelopes that were marked with the candidates' number on the outside. Others just stacked ballots in piles. Some polling places faced difficulties in reconciling the votes with the ballots cast; however, after recounting the ballots, sometimes several times, these problems were solved. Few domestic political party or NGO observers were present at the polling places visited by the OSCE/ODIHR EAM.

While it did not appear that the different counting procedures used at polling places provided for inaccurate counts, the OSCE/ODIHR recommends that the NEC ensure that polling stations count ballots according to uniform procedures.

After the DCs completed the counting, they proceeded to enter the results on the NEC website. Each polling place was given a number and a password to use to access the database. The program used contains cross checks of data and does not allow mistakes to be submitted. Therefore, some DCs did not sign the final protocol until after their electronic protocol was accepted. The counted ballots were stored in sealed containers and transported to the CEC by the Chair and at least two DC members.

The day after the election, the CECs recounted all ballots to check the accuracy of the count and materials, including any advance ballots sent to the wrong polling station. Any discrepancies were reported to the NEC, which corrected their records before certifying the final returns.

Estonia is to be commended for the practice of recounting all Election Day ballots by the respective CECs. The OSCE/ODIHR recommends that the law be amended to require the

posting of results in each polling place, in order to further increase the transparency of the process.

XVI. ANNOUNCEMENT OF RESULTS

As each DC electronically entered its results, the NEC immediately uploaded and posted the results by polling station on its website. The last of the 657 polling places reported their results to the NEC shortly after midnight.

The final results were announced on 12 March (see Annex 1). The NEC reported that voter turnout was 61.9 per cent (555,463 of the 897,243 eligible voters). There were 550,213 valid votes. The total number of votes cast prior to the March 4 election day balloting was 174,769, which included 2,501 ballots cast abroad in person at embassies/consulates and 750 ballots sent by mail to the embassies/consulates; 141,275 advance votes cast nationwide at polling stations in Estonia; and 30,243 valid ballots cast by internet. These early voters represented 30.8 per cent of the total votes cast in the election.[47] These figures reflect the diverse opportunities Estonians are given to cast their ballots. As the figure for early voting was some 25 per cent of all votes cast in the 2003 parliamentary elections, the figures suggest that an increasing number of voters prefer to cast their ballots early.

Six of the eleven political parties competing in the election passed the five per cent threshold and won mandates. No independent candidates were elected. The five parties which did not receive mandates each received less than two per cent of the vote.

[47] All figures provided by the NEC either on the website or directly to the OSCE/ODIHR EAM.

ANNEX 1

FINAL RESULTS

Political Party	Number of Votes	Percentage of Votes	Number of Mandates
Reform Party (RE)	153 037	27,8	31
Centre Party (K)	143 524	26,1	29
Pro-Patria Union-Res Publica (IRL)	98 203	17,9	19
Social Democrat Party (SDE)	58 346	10,6	10
Greens of Estonia (EEE)	39 304	7,1	6
Union of Estonian People (ERL)	39 216	7,1	6
Christian People's Party (KR)	9 444	1,7	0
Constitution Party (KP)	5 466	1,0	0
Independence Party (EIP)	1 275	0,2	0
Russian Party of Estonia (VEE)	1 085	0,2	0
Estonian Left Party (VP)	608	0,1	0
Independent Candidates	564	0,1	0

Source: National Election Committee of the Republic of Estonia (www.vvk.ee).

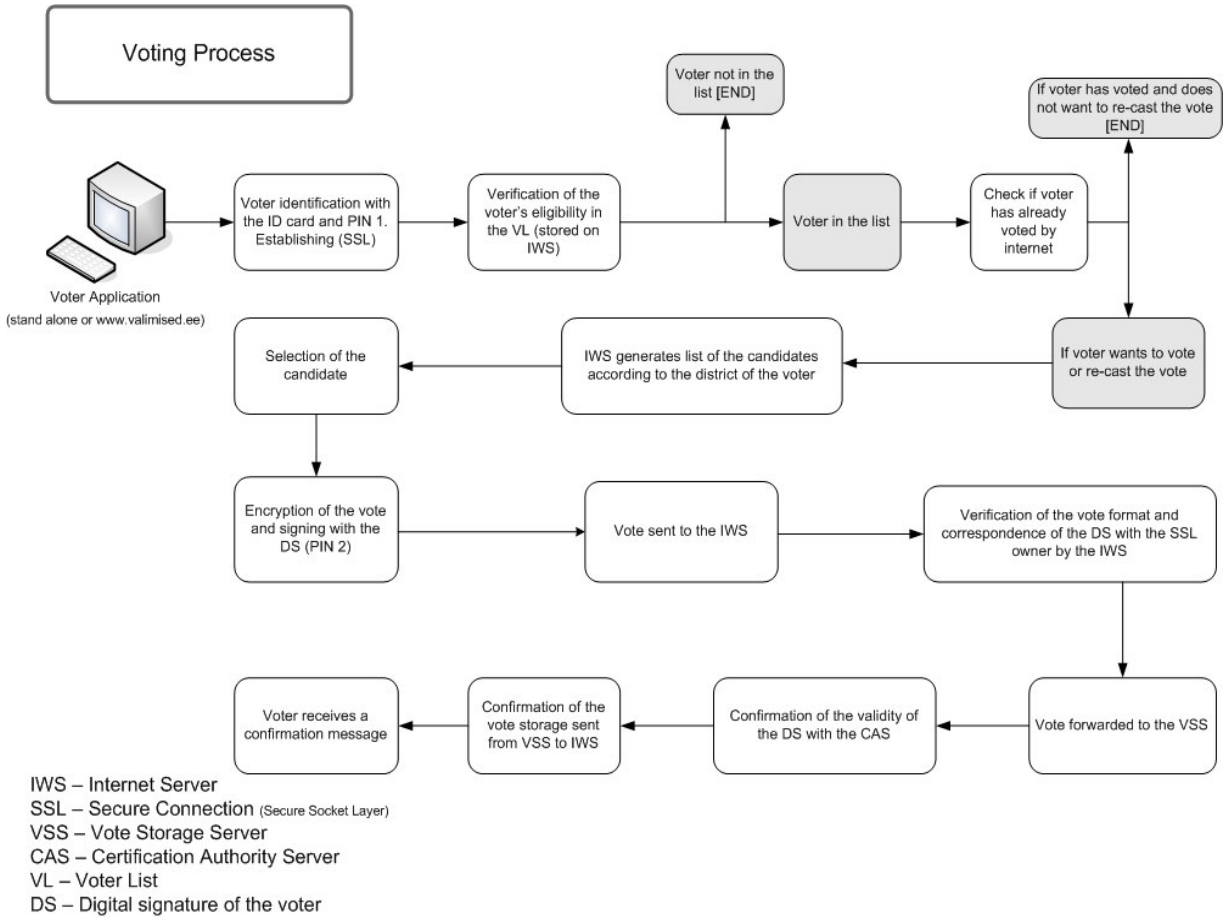
VOTING STATISTICS

General	
Number of Eligible Voters	897,243
Total Votes cast	555,463
Valid Votes	550,213
Turnout	61.9 per cent
Voters in Advanced Voting (including advance voting conducted in polling stations, abroad, and by internet)	174,769
Internet (E-voting)	
E-votes cast, including repeated	31,064
Repeated e-votes	789
Number of e-voters	30,275
Cancelled e-votes due to advanced paper voting	32
E-votes counted	30,243
Percentage of e-votes among all votes	5.4 per cent

Source: National Election Committee

ANNEX 2

INTERNET VOTING PROCESS:



Source: OSCE/ODIHR

ABOUT THE OSCE/ODIHR

The Office for Democratic Institutions and Human Rights (OSCE/ODIHR) is the OSCE's principal institution to assist participating States "to ensure full respect for human rights and fundamental freedoms, to abide by the rule of law, to promote principles of democracy and (…) to build, strengthen and protect democratic institutions, as well as promote tolerance throughout society" (1992 Helsinki Summit Document). This is referred to as the OSCE human dimension.

The OSCE/ODIHR, based in Warsaw (Poland) was created as the Office for Free Elections at the 1990 Paris Summit and started operating in May 1991. One year later, the name of the Office was changed to reflect an expanded mandate to include human rights and democratization. Today it employs over 130 staff.

The OSCE/ODIHR is the lead agency in Europe in the field of **election observation**. Every year, it co-ordinates and organizes the deployment of thousands of observers to assess whether elections in the OSCE region are conducted in line with OSCE Commitments, other international standards for democratic elections and national legislation. Its unique methodology provides an in-depth insight into the electoral process in its entirety. Through assistance projects, the OSCE/ODIHR helps participating States to improve their electoral framework.

The Office's **democratization** activities include: rule of law, legislative support, democratic governance, migration and freedom of movement, and gender equality. The OSCE/ODIHR implements a number of targeted assistance programs annually, seeking to develop democratic structures.

The OSCE/ODIHR also assists participating States' in fulfilling their obligations to promote and protect human rights and fundamental freedoms consistent with OSCE human dimension commitments. This is achieved by working with a variety of partners to foster collaboration, build capacity and provide expertise in thematic areas including human rights in the fight against terrorism, enhancing the human rights protection of trafficked persons, human rights education and training, human rights monitoring and reporting, and women's human rights and security.

Within the field of **tolerance** and **non-discrimination**, the OSCE/ODIHR provides support to the participating States in strengthening their response to hate crimes and incidents of racism, xenophobia, anti-Semitism and other forms of intolerance. The OSCE/ODIHR's activities related to tolerance and non-discrimination are focused on the following areas: legislation; law enforcement training; monitoring, reporting on, and following up on responses to hate-motivated crimes and incidents; as well as educational activities to promote tolerance, respect, and mutual understanding.

The OSCE/ODIHR provides advice to participating States on their policies on **Roma and Sinti.** It promotes capacity-building and networking among Roma and Sinti communities, and encourages the participation of Roma and Sinti representatives in policy-making bodies.

All ODIHR activities are carried out in close co-ordination and co-operation with OSCE participating States, OSCE institutions and field operations, as well as with other international organizations.

More information is available on the ODIHR website (www.osce.org/odihr).