REPUBLICA MOLDOVA
COMISIA ELECTORALĂ CENTRALĂ

SWEDEN

Norwegian Ministry
of Foreign Affairs

UNDP
Empowered lives.
Resilient nations.

Feasibility study on Internet Voting for the Central Electoral Commission of the Republic of Moldova

REPORT AND PRELIMINARY ROADMAP

Chisinau, 2016

Version of 28/06/2016

Table of Contents:

List of Abbreviations

CEC	Central Electoral Commission
ICT	Information and Communication Technology
IVIS	Internet Voting Information System
IDPN	Personal Identification Number
SAISE	State Automated informational System “Elections“
SRV	State Register of Voters
NCPDP	National Center for Personal Data Protection
MPass	Governmental authentication and access control service for electronic services
MSign	Governmental service for electronic signature
MCloud	Joint Governmental information infrastructure operating on the basis of “cloud computing” technology

EXECUTIVE SUMMARY

This Feasibility Study (hereinafter – The Study) was conducted to evaluate the possibilities of introducing of modern voting technologies in elections and referenda in the Republic of Moldova.

The structure of the Study. This Document consists of the following sections:

- Overview of the successful implementation of Internet Voting around the world in such countries like Estonia, Switzerland, Norway, Canada and Australia;
- Presentation of the main concepts of Internet Voting;
- Analysis of the current situation of the legal, technical, social and political election – related environment;
- Propositions of the Study;
- Preliminary implementation Roadmap;
- Cost – benefit analysis.

The key findings of the Study are the following:

- Election management in Moldova is centralized; Parliamentary Elections are only proportional closed-list elections. The Central Electoral Commission is the independent institution responsible for election management. Effective voter list management is in place. Every citizen of Moldova is being registered through the State Register of Population (SRP).
- Election regulation is concentrated in the Electoral Code of the Republic of Moldova and decisions of the CEC. Other provisions on the State Register of Voters (SRV), State Automated Information System for Elections (SAISE), regulations regarding registries are generally in place.
- There is no specific regulation of Internet Voting in the Constitution of the Republic of Moldova. The basic election principles stated particularly in the 38th Article of the Constitution must be ensured. At the same time, learning from the Estonian experience, the Constitutional Court of the Republic of Moldova could provide a more extensive interpretation of the 38th Article of the Constitution in the context of the Internet Voting Informational System.
- The Electoral Code of the Republic of Moldova does not include specific provisions regulating Internet Voting concepts, policies, rules, procedures, and relevant functioning and the management requirements for the Internet Voting Informational System. In order to create a proper legal framework for the implementation of the Internet Voting, the Electoral Code is to be modified by introducing Internet Voting concepts, vote verification and cancellation rules, voting secrecy assurance principles, voter identification aspects, information systems establishing the framework for its functional, security and audit requirements and other elements common to the Internet Voting. A new title on Internet Voting shall be introduced in the Electoral Code. The Central Electoral Commission could also consider, if deems necessary, to establish a separate Internet Voting Electoral Council (IVEC). Prior to the adoption of the amendments to the Electoral Code introducing specific Internet Voting legislation the opinions of the Venice Commission and OSCE/ODIHR shall be consulted.
- Moldova has a high penetration of internet and very good mobile coverage; Internet is accessible on the whole territory, mobile phones and computers are available in the majority of the households and are popular among individuals.
- Moldova has very few government e-services, which would be popular among general public. The effective means of personal identification online is gaining popularity at the very low rate.
- Special polling stations for Moldovan Diaspora abroad are being organized for voting on the same Election Day. During the last Parliamentary Elections, 95 polling stations abroad have been opened, where a total of cca. 73,311 Moldovans have voted.
- Emigration level is very high. According to various estimates, up to ¼ of the population are on permanent or temporary emigration, mostly in Russia, Italy, Spain, Portugal, Greece,

France, UK, Germany, Turkey, Israel, USA, Canada and Belgium.
- A special survey for Moldovan Diaspora abroad was developed by consultants and distributed through social networks. The results of the Study showed wide support for the introduction of Internet Voting among the Moldovans living abroad.

The main propositions of the Study are the following:

The introduction of new methods of casting a vote has to comply with all the existing standards and requirements for traditional elections. Most of those principles are set in the Constitution of the Republic of Moldova (universal, equal, direct, secret and freely expressed suffrage) and the Electoral Code.

The Study is focused on remote Internet Voting, as voters residing abroad won't benefit from other methods of Electronic voting (e.g. electronic voting machines).

After conducting the analysis of best world practices and comparing them with the legal, operational, political and social conditions in Moldova, the authors of this Study are proposing to work in two parallel directions.

Analysis of the legal environment, demographic situation, ICT development, conducted during assessment mission led to a conclusion to suggest that an Internet Voting Information System (*hereinafter - IVIS, or Internet Voting Informational System*) shall be created under auspices of the CEC, owned and managed by it as a Module of the SAISE based on the SRV.

The IVIS shall be used by CEC as an auxiliary alternative voting channel, which shall be used for Internet Voting in national elections, national referendums. For the official implementation of IVIS module an IVIS Pilot shall be implemented. The non-binding IVIS Pilot shall be conducted before the Parliament Elections in 2018. The elections may be organised the earliest in 2018. Thus, the IVIS Pilot shall be conducted at least one month before the Election Day (i.e. in September, 2018).

The IVIS Pilot should offer all the technical, operational and security features, as if it were legally binding elections, except the legal validity of the Pilot result. This is an important requirement both to test the security and reliability of the Internet Voting Informational System, and to gather valuable feedback from experts and general society. The necessary time to prepare the IVIS Pilot should be no less than 18 months; therefore the decision to initiate the Pilot shall be made no later than the 3rd quarter of 2016. A fully functional Internet Voting Information System shall be presented to the general public as well as to experts and auditors to test it before its actual use in legally binding political elections.

Voters could access the IVIS using MPass service. Only voters living abroad, who don't have means to use MPass service, could register in advance to vote on Internet and receive credentials for accessing the voting platform via post, email or SMS.

Internet Voting has to be with the following properties:

- Auxiliary voting channel – traditional voting stays;
- Advanced voting – voting via Internet shall be available during a period of several days and should end at least two days before the traditional voting by paper ballots starts;
- Multiple voting – Internet Voting should allow voters to vote multiple times and only the last vote should be counted in the final tally. This is considered to be an effective measure against vote buying and peer pressure.

The IVIS has to offer the following features:

- To be accessible, available, scalable, flexible and compatible with the country's existing electoral systems;
- Has to offer cast – as – intended verifiability;
- Has to offer recorded – as – cast verifiability;
- Has to offer counted – as – recorded verifiability;

- No information containing voting – related data shall be transferred unencrypted;
- There must be no single point, where the content of the ballot could be related to the voters' identity;
- Transparent, reliable and auditable.

Preliminary **Roadmaps** are proposed both for the official IVIS implementation and for the IVIS Pilot by 2018 when the regular Parliamentary Elections will take place.

The following conclusions were made in this Study:

Moldova has all the basic preconditions for introducing Internet Voting in the near future, such as (1) well developed Internet infrastructure; (2) high degree of mobile network coverage; (3) good level of public ICT literacy; (4) reliable voters list (SRV); (5) all polling stations equipped with Internet – connected computers that are constantly online and communicating with SAISE.

Introducing Internet Voting: (1) May give positive effect in terms of public trust in the public sector and government e-services; (2) May raise worldwide knowledge of the Republic of Moldova as a modern and technologically mature state; (3) Will likely increase accessibility to vote among people with disabilities and limited mobility; (4) Will most likely increase participation among Moldovan citizens living abroad; (5) Will reduce the "cost per voter" rate for voters living abroad; (6) Can reduce the number of required polling places in highly populated areas.

However, amendments to the Electoral Code for introducing Internet Voting (will be required, that would include regulation of the advanced voting, remote voting and multiple voting (last vote counts) for the Internet Voting, and other relevant changes in the legislation.

Special attention has to be addressed towards the legal concept of a Secret Voting, because remote voting via Internet implies voting in an uncontrolled environment, in some cases, which may rise some legal debates regarding constitutionality of such voting method.

The Existing Data Protection legislation is in place and the introduction of the Internet Voting solution as an extension to the existing SRV and SAISE system is legally possible. However, the piloting of the Internet Voting may require a preliminary permission from the National Center for Data Protection (NCDP).

1. INTRODUCTION

This Feasibility Study for Internet Voting in Moldova (hereinafter – The Study) is a result of cooperation among the United Nations Development Programme in Moldova, Central Electoral Commission of the Republic of Moldova and international consultant Jonas Udris and national consultant Iulian Groza.

The aim of this Study is to identify a necessary set of the legal, organizational and economic assumptions that would lead to the introduction of Internet Voting in the Republic of Moldova.

The Study was conducted during 28th of March – 31st of July, 2016.

The purpose of work for the current Study is to assess the introduction of Internet Voting in Moldova and to present a Roadmap for its piloting and further implementation. It shall be noted that, initially, according to the Terms of Reference for this Study, the aim was to assess the feasibility of the Electronic Voting (E-Voting) system in Moldova, which includes more types of electronic voting solutions, including Internet Voting.

Thus, prior to and during the inception Mission, upon the request of the Central Electoral Commission, the Purpose **of Work was narrowed down and limited to assessing the feasibility for the introduction of the remote Internet Voting Informational System in Moldova**, designed in particular to create alternative voting solutions.

The **main objective** of this Study is to assess the feasibility of developing and implementing remote Internet Voting Informational System in the Republic of Moldova, using examples from other European countries with similar electoral systems.

In May 2008 the Parliament of Moldova approved the Law No. 101 on the State Automated Informational System "Elections" (SAISE). The long-term objective of the SAISE is to achieve full automatization of the elections in Moldova. This includes developing the citizens' possibility to vote in any polling station, possibility to vote through electronic voting machines (e.g. using an electronic pen, scanner or other electronic reading device) and/or possibility to vote via Internet (using identification devices that can read electronic documents).

According to the Law No. 101, the electronic voting (further referred as Internet Voting) system is to be developed, tested and piloted by the Moldovan authorities by 2018 Parliamentary Elections. In this regard, CEC is currently planning to develop an Action Plan and a Roadmap for the implementation of the Internet Voting Informational System implementation in Moldova, including costs analysis.

The Study will seek to identify the operational, legal, privacy and technical considerations associated with the development of an Internet Voting Informational System and to recommend short and long term strategies for implementing the system. In order to achieve most efficient and comprehensive results of the Study, the analysis of the following four main aspects is necessary:

- **Legal framework:** legal documents, state governance institutions, legal experts, knowledge base and competence;
- **Social demand:** public awareness and understanding, public opinion and attitudes;
- **Technological maturity:** Internet penetration, mobile network coverage, technical infrastructure, level of ICT literacy in the country, necessary quantity and quality of technology experts and technology managers, sufficient experience and competences;
- **Political will:** long-term support of the majority of political parties, distribution of rights and obligations, stable and long-term sources of financing, coordination of inter-office efforts.

The Study was prepared in accordance with the agreed plan of actions, including the following:

- A series of meetings with the representatives of the Central Electoral Commission, political parties, ministries, government agencies and other stakeholders (see Annex III for full list of conducted meetings);
- The analysis of the best practices of the implementation of Internet Voting in other countries;

- The analysis of legal, technical, social and political environment in Moldova, using the results of conducted interviews, available documentation and personal observations.

A draft Roadmap for implementing Internet Voting in Moldova will be an integrated part of this Study.

2. ELECTRONIC AND INTERNET VOTING

2.1. Introduction

The use of information and communication technology (ICT) in the electoral process is continuously rising around the world. Even most of the applications emerge in the back-office, including the administration of the election like electronic electoral registers or mandate calculate, ICT is finally reaching the home of the voters[1]. In 2016, the usage of ICT is no novelty in the election management. Most of the countries throughout the world employ Internet and ICT in different ways. Some of them simply use special web-pages to publish election results, but keep the traditional methods of voting and vote counting, while others are exclusively using special offline electronic devices to both collect and count the votes (Brazil), or use Internet connected personal computers for voting (Estonia).

2.2. Types of electronic voting

The analysis of the world practice of electronic voting distinguishes several types of usage of ICT in conducting elections, which include the following:

- Voting using dedicated electronic devices (voting kiosks);
- Voting using ballot papers, but using special ballot boxes with ballot scanning machines installed, so the ballot is scanned before falling into the ballot box;
- Vote counting using handheld scanning devices (a.k.a. "e-Pen" technology), used to digitally identify marks on the ballot papers;
- Remote voting over the Internet, using standard computers and/or smartphones.

Types of E-voting	Pros	Cons
Electronic dedicated voting machines (voting kiosks)	• Fast data collection and counting • Impossible to spoil a ballot • Network independent	• Expensive to build and deploy across polling places • No use between elections, safekeeping and maintaining issues • Additional voter education required • Additional technical staff required to provide support to onsite voters • Changing management on the voting process • Software exploits may appear over time
Ballot scanning machines	• Same process for voters – no voter education needed • Accurate and fast results • Secure	• Technology involved, paper dependent • Validation workflow and additional staff required at each polling station • Ballots may require modification
e-Pen Solutions	• Electronic results and paper trail • Similar process for voters, ballots are deposited in a ballot box	• Inacceptable accuracy levels (never 100%). Validation process required. • Cost increase. Additional staff to provide validation and equipment • Bad track record. Solution not suitable for electoral environments
Remote Internet Voting using standard off-the-shelf hardware	• Alternative voting channel – traditional voting channels are not affected • No special hardware required for a voter • Basic IT knowledge is sufficient	• Network dependent

As already mentioned above, in this Study we will be analysing remote Internet Voting, as voters residing abroad won't benefit from other methods of Electronic voting, such as Electronics voting machines or ballot scanners.

[1] The E-Voting Readiness Index. Robert Krimmer, Ronald Schuster https://www.e-voting.cc/wp-content/uploads/Proceedings%202008/4.1.krimmer_schuster_e-voting%20readiness%20index_127-136.pdf

2.3. Internet Voting around the world

Many countries are already using, or are considering using Internet Voting for a number of purposes, including:

1. allowing voters to cast their votes from a place other than the polling station in their voting district;
2. facilitating the casting of the vote by the voter;
3. facilitating the participation in elections and referendums of all those who are entitled to vote, and particularly of citizens residing or staying abroad;
4. widening access to the voting process for voters with disabilities or those having other difficulties in being physically present at a polling station and using the devices available there;
5. increasing voter turnout by providing additional voting channels;
6. bringing voting up-to date with the new developments in the society and the increasing use of new technologies as a medium for communication and civic engagement in pursuit of democracy;
7. reducing, over time, the overall cost to the electoral authorities of conducting an election or referendum;
8. delivering voting results reliably and more quickly; and
9. providing the electorate with a better service, by offering a variety of voting channels.

In this section we will provide an overview of the most notable Internet Voting examples around the world. This overview focuses mostly on the examples of political and legally binding elections that use remote Internet Voting, the most notable examples of voting using voting machines being presented.

2.3.1. Estonia

The feasibility of E-voting in Estonia is based on the widespread Internet access and the use of digital ID cards. These personal identification documents with the size of a credit card allow citizens and residents to digitally sign documents and use private and governmental online services that require secure authentication.

They also allow citizens to cast legally binding digital votes with a high level of security. Participation in the electronic ballot requires a computer with an Internet connection and a" smart-card reader". Card readers are available for less than 10 euros at computer shops and supermarkets. Citizens may also access e-voting in public libraries or community centers, in fact any place with a secure Internet connection. In 2011, citizens could also electronically identify themselves with a so called "Mobile-ID", which requires a special mobile phone SIM card with security certificates and two pin codes. With Mobile-ID setup citizens can officially identify themselves using only their cell phone. The ID card is however still the most widespread method of digital identification. E-voting is available during the advance voting period via a website hosted by the Estonian National Electoral Committee (2005-2011). In order to vote online, people are required to insert their digital ID card into a smart reader connected to an Internet equipped computer. Next, they need to download a voting app, which is a standalone program for Estonian E-voting. Using their ID-card and a four-digit pin (PIN1), the user has to first identify themselves to the system, after which the system checks whether the voter is eligible according to age and citizenship to vote in the election. If affirmative, the e-voting system displays the list of candidates in the voter's district.

Voters can then browse the list of candidates and decide for whom to vote for. In order to cast an e-vote, the voter has to choose a candidate and provide a separate five-digit pin (PIN2) to vote. When certified correctly, the Internet vote is cast and sent to the server where it will be counted at an appropriate time, i.e. as prescribed by the procedures for Internet Voting.[2]

Brief description of the Internet Voting Informational System[3]

One of the traditional ways to vote is outside the polling district of the voter's residence. This means that during the voting, the voter puts his or her vote into double envelope and the envelope is delivered to the voter's polling division of residence. The general concept of I-voting has been derived from the voting outside the polling district of residence. Both voting methods use a similar way of checking that the vote has been cast only once and guaranteeing the anonymity of the vote.

In order to understand the Internet Voting Informational System better, the envelope voting method used in Estonia should be described herein:

1. A voter presents an ID document to be identified.
2. The voter then receives the ballot and two envelopes.
3. The voter fills in the ballot paper and puts it into the envelope, which has no information about the voter.
4. Then he encloses the envelope into an outer envelope on which the voter's information is written.
5. The envelope is delivered to the voter's polling place of residence. After the eligibility of the voter is determined, the outer envelope is opened and the inner (anonymous) envelope is put into the ballot box.

The system guarantees that the voter's choice shall remain secret and the registration of the vote in the list of voters in the polling district of residence prevents voting more than once.

I-voting is carried out according to the same scheme. The downloaded I-voting application encrypts the vote. The encrypted vote can be regarded as the vote contained in the inner, anonymous envelope. After that the voter gives a digital signature to confirm his or her choice. By digital signing, the voter's personal data or outer envelope is added to the encrypted vote.

I-voting is possible only during the 7 days of advance polls – from the 10th day until the 4th day prior to Election Day. This is necessary in order to ensure that there would be time to eliminate double votes by the end of the Election Day.

To ensure that the voters are expressing their true will, they are allowed to change their Internet vote by voting again electronically during advance polls or by voting at the polling station during advance polls.

For example, if a voter cancels his or her Internet vote by going to the polling station to vote, it is guaranteed that only one vote is counted per voter. To that end, all polling stations are informed of the I-voters on their list of voters after the end of the advance polls and before the Election Day on Sunday. If it is found at the polling district that the voter has voted both electronically and with a paper ballot, the information is sent to the Internet (Electronic) Voting Committee and the voter's I-vote is cancelled.

Before the ascertaining of the voting results in the evening of the Election Day, the encrypted votes and the digital signatures (i.e. the data identifying the voter) are separated. Then anonymous I-votes are opened and counted. The system opens the votes only if they are not connected to personal data.

Internet Voting principles

Time framework of Internet Voting: I-votes may be given during 7 days, from the 10th day until the 4th day before the Election Day.

[2] Mihkel Solvak, Kristjan Vassil, E-voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005 - 2015), http://skytte.ut.ee/sites/default/files/skytte/e_voting_in_estonia_vassil_solvak_a5_web.pdf
[3] http://vvk.ee/voting-methods-in-estonia/

Possibility to recast Internet vote: during the I-voting period a voter can recast his or her I-vote in which case the last I-vote counts.

Precedence of the ballot paper voting: if a voter who has already I-voted goes to the polling place during advance polls and casts his or her vote by using paper ballot, then the I-vote is cancelled. After that, the voter cannot recast his or her vote electronically or by using a paper ballot. On the Election Day the I-vote cannot be changed.

Similarity of I-voting to regular voting: I-voting adheres to the election acts, general election principles and customs. Thus, it is uniform and secret, only eligible voters may vote, every person may cast only one vote, it should be impossible for voters to prove the way they voted. The collecting of the votes is secure, reliable and verifiable.

The voter must be able to cast his or her vote freely and without any outside coercion or influence. Incitement to I-voting by offering a computer for that purpose or influencing voters in any other way is prohibited; among other things, no collective I-voting events (opening of I-voting offices or service desks, etc.) shall be organized insofar as such activities may be considered violation of the freedom to vote.

An I-voter shall vote himself or herself. Using another person's ID card (or mobile-ID) for voting and transferring the card's PIN codes to another person is prohibited. In order to avoid security risks, only a trusted computer should be used, either owned by the voter or a person the voter can trust.

During the Parliamentary Elections in 2007, about 30,000 voters used this voting method. (This number corresponds to 5 per cent of the participating voters). In the European Parliament elections in 2009 the number of I-voters had almost doubled – more than 58,000 voters used this method (this corresponded to about 15 per cent of all participating voters). In the local elections that took place on 18 October 2009, I-voting was used as a voting method for the fourth time, and there were about 104,000 I-voters (about 16 per cent of all the participating voters). 140,846 I-voters used this voting method in the Parliamentary Elections of 2011. In 2013, during local elections, more than 133,000 voters voted online. This number corresponds to about 22 per cent of the participating voters. In the European Parliament elections of 2014, more than 103,000 voters used I-voting – that is 31% of all voters.

2.3.2. Norway

Brief Description

The Ministry of Local Government and Regional Development (MLGRD) is in charge of managing the electoral processes in Norway. At the beginning of 2009, it invited tenderers to participate in a competitive dialogue process with the objective of providing Norway's 2011 elections with a national election administration system, as well as an Internet Voting solution allowing Norwegian citizens to cast their votes using the Internet. Given the success of the trial elections of 2011, the same system was authorized by the Parliament to be used again for the 2013 elections.

In both 2011 and 2013, Internet Voting was offered for early voting for nearly a month prior to Election Day. 17% of registered voters in the pilot districts voted online in 2011. During the second election in 2013, in the 12 districts that used Internet Voting, 36% of the registered voters voted over the Internet. That is more than a 100% increase in the use of Internet Voting. In 2013, approximately 70,622 voters voted online.

Objectives

The short-term main objective was to implement a secure Internet Voting platform to be used in 10 selected municipalities in the 2011 municipal and in county elections where voters would be able to cast their votes over the Internet.

After successfully executing 10 different pilot elections with different purposes, the Norwegian government successfully used the platform for the Municipal and County Elections, receiving all the ballots via Internet and consolidating the results in a fast and secure manner.

Norway's 2011 Internet Voting trial was considered a huge success, so authorization to use the Internet Voting platform was given again in 2013. The objective of this election was to consolidate Internet Voting as a reliable voting channel. This time 12 different districts used Internet Voting allowing 250,000 eligible voters to securely cast their votes electronically.

Project Description

A fully functional nationwide election administration and e-voting system was created. It consisted of:

- a remote Internet Voting Informational System;
- an election management system (EMS);
- an electronic counting system and a results consolidation system (RCP).

The key features of the system were the following:

- Voting system to cover County, Municipality, Parliamentary elections and Referendums.
- Strong cryptographic protocols, including Zero Knowledge Proofs. Full integration with existing Norwegian authentication methods.
- Internet Voting secured by specific computer terminals and remote Secure Internet Voting using standard PCs.
- Multilingual platform, including right to left languages. Multiplatform, cross browser compatible platform with over 100 combinations supported.
- Accessibility standards compliant. Compatible with screen readers for the visually impaired.

During both 2011 and 2013 elections, the Internet Voting Informational System was managed by the MLGRD after receiving the necessary training from the vendors' personnel. In order to mitigate the risk of voter coercion and vote buying, each voter could cast any number of electronic votes but only their final vote was counted. Voters could also vote traditionally on paper, either during early or advance voting or on Election Day, cancelling all their electronic votes.

The Internet Voting Informational System enabled voters to verify that their votes had been properly cast as intended through return codes. Voters were mailed a polling card with instructions on how to vote and a set of securely printed and unique return codes for each political party. The return codes were four digit numbers and were different for each voter. Voters voted by first identifying themselves, after which the system would guide them through a simple and intuitive voting process. After submitting a vote, voters received a return code as an SMS on their mobile phone and this code could be verified against the return code printed on their polling card.

Furthermore, for the first time in an Internet Voting election, the Internet Voting Informational System used a JavaScript client (instead of using a Java applet). This technology ensured strict security as well as ease of use without the need of any additional software from the client but the web browser.

The custom made Internet Voting and election management system offered the highest levels of audited security, usability and accessibility, being compliant with the Norwegian Election Law and the Council of Europe Recommendation Rec(2004)11.

It is important to note that the source code and technical documentation of the project has been made available on the ministry website, and has received general academic praise. This information can be found in the following link: http://www.regjeringen.no/en/dep/kmd/prosjekter/e-vote-trial.html?id=597658

Contact details

Name:	Henrik Nore
Position:	Project Director
Address:	Akersgata 59, Oslo (Norway)
Telephone:	+47 222 47270
Email:	henrik.nore@krd.dep.no

2.3.3. Switzerland. Canton of Neuchâtel

Brief Description

The Swiss Canton of Neuchâtel has used Internet Voting technology to carry out several e-consultations, binding electoral processes and referenda per year since 2005.

In June 2008, an Internet Voting solution was selected by the Swiss Federal Government to carry out the first Internet Voting process open to the Swiss citizens living abroad.

In 2011, the Canton of Neuchâtel used the opportunity of rebuilding their e-government portal to upgrade to the latest version of Internet Voting Informational System, which gave them access to new and enhanced features.

In 2014 a new protocol was implemented and integrated into the Neuchâtel's e-government portal. This new solution is based on a next generation e-Voting protocol, providing not only end-to-end encryption but also individual verifiability using advanced cryptographic algorithms based on a system of individual voter's return codes.

There is usually one electoral event per quarter, including both referenda and elections that, depending on the year, could be federal elections, cantonal or communal elections. During these events, the Internet Voting channel is usually open for fifteen to thirty days prior to the traditional paper-based election or consultation. In some cases more than 60% of the votes cast during the process have been electronic.

Objectives

By introducing Internet Voting, the Canton of Neuchâtel wanted to reduce the costs associated to their electoral processes, while introducing a more convenient and secure channel that would fall in line with the voting tendencies of their citizens, where more than 90% of voters use postal voting. Back in 2005 Neuchâtel was one of the Swiss Cantons selected to trial Internet Voting, leading the way in electoral modernization along with Geneva and Zurich.

The protocol changes introduced in 2014 responded to the new regulations on e-voting from the Federal government that would allow the Canton of Neuchâtel to increase the percentage of the population that can vote through this channel from thirty to fifty per cent.

Project Description

The Internet Voting Informational System was designed to meet Neuchâtel's requirements that were integrated with their e-government portal ('Guichet Sécurisé Unique'). The system consisted of:

- pre-election: An offline configuration module in charge of generating all the keys and codes required for each election;
- election Day: A remote Internet Voting Informational System integrated and accessible through the Neuchâtel's e-government portal 'Guichet Sécurisé Unique';
- post-election: An offline electronic ballot box post-processing module meant to validate and decrypt the votes.

The consolidation of the final results and the seat assignment is performed by Neuchâtel's own systems. The key features of the system are the following:

- A voting system to cover Federal, Cantonal and Communal elections and referenda;

- End-to-end encryption using the most advanced cryptographic protocols, including Zero Knowledge Proofs (ZKP);
- Individual verification to ensure that the votes were cast-as-intended;
- Vote confidentiality is preserved throughout the whole voting process since the system can never relate the voter to the contents of the vote (these two pieces of data are managed on separate air-gapped computers);
- The voter can verify whether the vote was recorded-as-cast using the voting receipt.

The Internet Voting Informational System enables voters to verify whether their vote has been properly cast as intended through Return Codes. Prior to the election start, voters are mailed individual voting cards with a set of securely printed and unique return codes for each voting option. These return codes are four digit numbers and they are different for each voter. Additional codes for authentication and vote confirmation are also present in the voting cards. In order to vote, the voters must first access the 'Guichet Sécurisé Unique' using strong authentication and then the system guides them through a simple and intuitive voting process. After submitting a vote by entering the authentication code printed on their voting card, voters receive the return codes that the server has calculated for each of the options selected during voting. The voters must then verify these calculated return codes in comparison those printed in their voting cards and confirm their accuracy by providing their unique confirmation code.

The Internet Voting Informational System uses a JavaScript client. This technology ensures strict security by allowing the ballot encrypting as soon as it leaves the voter's device, as well as an ease of use without the need of any additional software from the client, excepting a web browser.

The new generation of Internet Voting was successfully used by Neuchâtel for the first time in the Federal Referendum March 8, 2015. Citizens were asked two questions. No decrease in participation was observed due to all these changes, including the more complex voting verification process introduced.

Total # voters	Voters using GU	Internet votes	% Internet votes	% Traditional votes
111,080	23,927	5,132	**21,45**	36,18

Federal Referendum June 14, 2015

This was the second time when the new system was used. Release 2.2 was used for asking 4 questions to the citizens. No incidents were reported during any of the election phases.

In this election, the turnout was lower:

- Participation for e-voting: 17.61%
- General participation rate: 38.64%

Federal Elections 18-October-2015

This was the first time when the full functional Release 3.1 was used in a federal election. This release of Internet Voting Informational System included all the electoral models that were needed. The participation in this election was 4459 votes with a general participation rate of 37.27%.

Contact details

Name: Mr Danilo Rota
Position: Chef de développement, Service informatique de l'Entité neuchâteloise
Address: République et Canton de Neuchâtel, Faubourg du Lac 25, Neuchâtel
Neuchâtel 2001, Switzerland
Telephone: +41 032 889 8415
Email: danilo.rota@ne.ch

2.3.4. Canada. Halifax Regional Municipality

Overview

In September 2011 the Halifax Regional Municipality (HRM) approved the usage of Internet Voting for advanced polls as a continuation of their mission to improve the voting experience, increase voter participation and manage the election processes more efficiently. As a result a solution was contracted to provide integrated Internet and Telephone voting system for the October 2012 Municipal and School Board Elections.

The Internet Voting solution, together with the Telephone Voting solution, was used during advanced voting to offer voters of all ages and abilities the opportunity to vote whenever and wherever they choose, while providing secure, private and secret voting over the phone or Internet. Voters could also choose to cast their electronic ballot in one of the polling stations located across the municipality. Finally, voters were able to cast their paper ballot at polling stations on Election Day.

Although electors have three separate options available to them to cast their ballots, the solution guaranteed that only one vote per voter was counted. On top of the e-voting technology, other key services were provided to the Municipality, which include data cleansing; authentication PIN generation and distribution; voter notification generation and postage; training; on-site support and; hosting.

Objectives

The following objectives were considered when adopting a complementary voting channel:

- transparency, integrity and accountability of the election process;
- increased voter access to the electoral process across all areas of HRM;
- positive impact on voter participation; and
- faster and more efficient reporting of election results.

Contact details

Name:	Cathy Mellet
Position:	Municipal Clerk, Halifax Regional Municipality
Address:	Election Office, P. O Box 1749, Halifax Nova Scotia B3J 3^{a}5
Telephone:	+1 (902) 490-6456
Email:	melletc@halifax.ca

2.3.5. Australia. New South Wales Electoral Commission Australia. iVote[4].

Brief Description

The NSW Electoral Commission is responsible for the delivery of the State General Elections (SGEs) and the Local Government Elections as well as some business elections for the state of New South Wales (NSW) in Australia. In 2014, the existing iVote© system was upgraded and now allows users to cast votes by the Internet or telephone.

Voting is allowed on the iVote© system during the early voting period and on the election day, with users required to register in advance for the use of the system, with registration available from one month prior to the early voting period. In 2015, a significant amount of the electorate voted with the iVote© system, resulting in over 280,000 votes collected. Voters eligible to use the system where those who were blind or visually impaired as well as those who were out of the state or more than 20 km from a polling place. The use of the system saw a 500% increase from its original use in 2011.

The iVote system is an Internet delivered voting system for NSWEC which also supports telephone voting through the use of an IVR (Interactive Voice Response) system.

[4] Internet Voting platform

• Country of Election:	Australia
• Election conducting authority:	New South Wales Electoral Commission
• Name of the Election:	New South Wales State General Election 2015
• Election dates:	16 March 2015 to 28 March 2015
• User satisfaction survey result:	97% satisfied or very satisfied.
• Votes collected:	286,000 (at the time, the world’s largest binding Government election)

General information

The Customer maintains public information on the system:	https://www.elections.nsw.gov.au/voting/ivote http://www.elections.nsw.gov.au/voting/ivote/overview
A trial interface for the system is available at:	https://practise.ivote.nsw.gov.au
System specifications:	http://www.elections.nsw.gov.au/about_us/plans_and_reports/ivote_reports/ivote_sge_2015_specifications
Video – user experience / advertisement:	http://www.scytl.com/en/2015-state-elections-new-south-wales/
Video – description of the election:	https://www.youtube.com/watch?v=lBlfPBIaBfs

Objectives

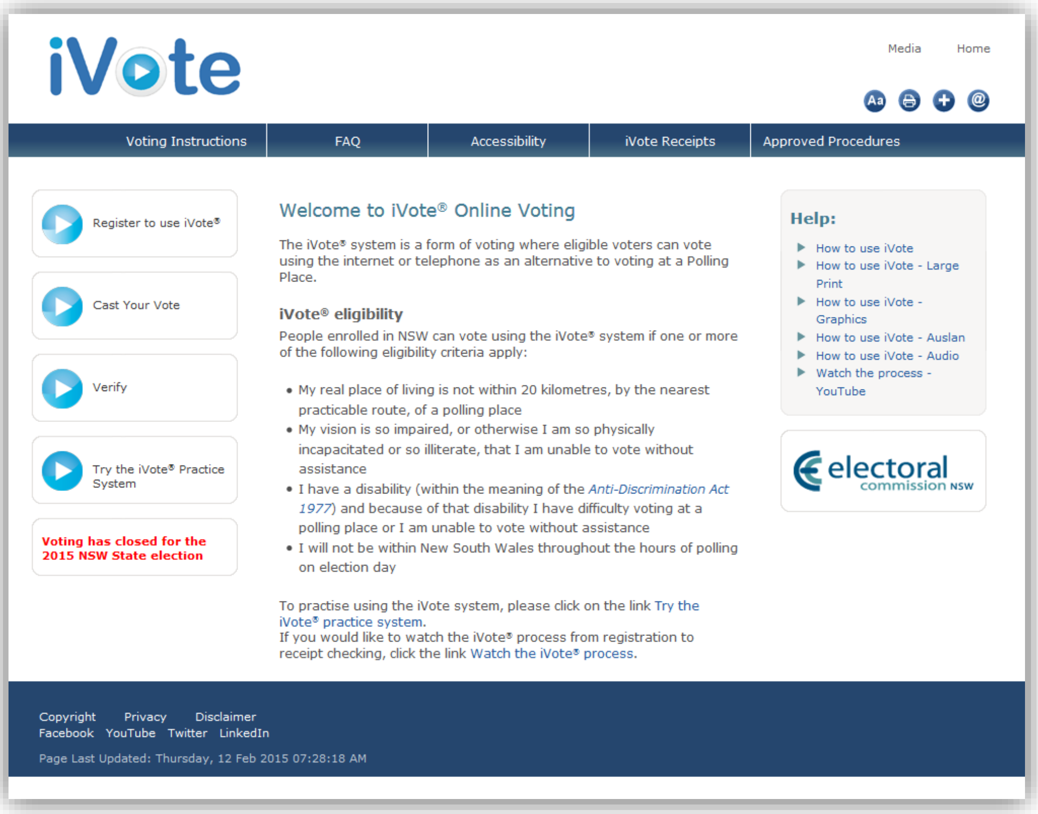
The primary objective of the NSWEC was to update the *iVote* system to be a more secure solution in order to avoid the scandal that had affected the original implementation of the system by another vendor. The market for iVote was established in law and the Customer was determined to avoid negative publicity based on poor implementation.

Operational Objectives:

- Meet the legislative requirements to deliver Internet and telephone voting to eligible voters. Eligible voters are from the following groups:
  - More than 20 km from a polling place
  - Have a disability that prevents the voter from voting in private
  - Will not be within New South Wales on election day
  - Visually impaired
- Ability to re-cast votes

Technical Objectives:

- Internet delivered electronic voting system
- Vote encryption in the browser (JavaScript client)
- Supports IVR / telephone votes
- Support of two parliament races and a referendum – preferential system, STV
- Enabled for visually impaired (largely AA compliant)
- Offers ability to verify your vote (non-technical)
- Runs on Windows
- Segregated operations



Voting has closed for the 2015 NSW State election

Welcome to iVote® Online Voting

The iVote® system is a form of voting where eligible voters can vote using the internet or telephone as an alternative to voting at a Polling Place.

iVote® eligibility

People enrolled in NSW can vote using the iVote® system if one or more of the following eligibility criteria apply:

- My real place of living is not within 20 kilometres, by the nearest practicable route, of a polling place
- My vision is so impaired, or otherwise I am so physically incapacitated or so illiterate, that I am unable to vote without assistance
- I have a disability (within the meaning of the *Anti-Discrimination Act 1977*) and because of that disability I have difficulty voting at a polling place or I am unable to vote without assistance
- I will not be within New South Wales throughout the hours of polling on election day

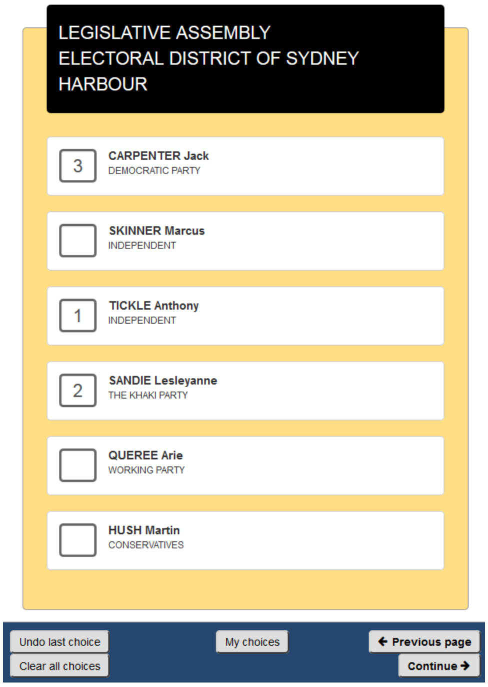
To practise using the iVote system, please click on the link Try the iVote® practice system.
If you would like to watch the iVote® process from registration to receipt checking, click the link Watch the iVote® process.

Help:

- How to use iVote
- How to use iVote - Large Print
- How to use iVote - Graphics
- How to use iVote - Auslan
- How to use iVote - Audio
- Watch the process - YouTube

Page Last Updated: Thursday, 12 Feb 2015 07:28:18 AM

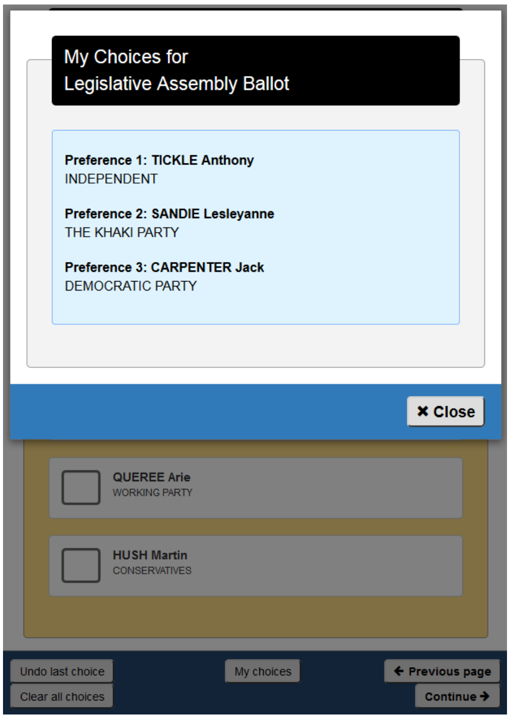
iVote main page



LEGISLATIVE ASSEMBLY
ELECTORAL DISTRICT OF SYDNEY HARBOUR

3	CARPENTER Jack DEMOCRATIC PARTY
	SKINNER Marcus INDEPENDENT
1	TICKLE Anthony INDEPENDENT
2	SANDIE Lesleyanne THE KHAKI PARTY
	QUEREE Arie WORKING PARTY
	HUSH Martin CONSERVATIVES

Sample iVote voting screen (Legislative Assembly)



My Choices for
Legislative Assembly Ballot

Preference 1: TICKLE Anthony
INDEPENDENT

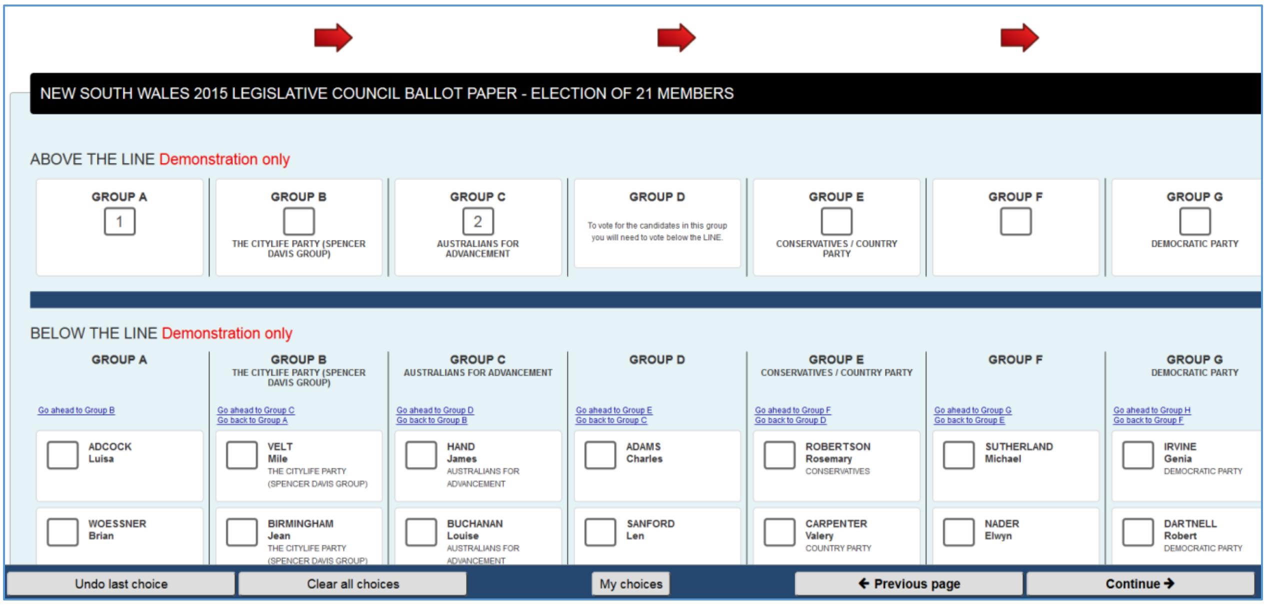
Preference 2: SANDIE Lesleyanne
THE KHAKI PARTY

Preference 3: CARPENTER Jack
DEMOCRATIC PARTY

QUEREE Arie
WORKING PARTY

HUSH Martin
CONSERVATIVES

Reviewing choices screen



NEW SOUTH WALES 2015 LEGISLATIVE COUNCIL BALLOT PAPER - ELECTION OF 21 MEMBERS

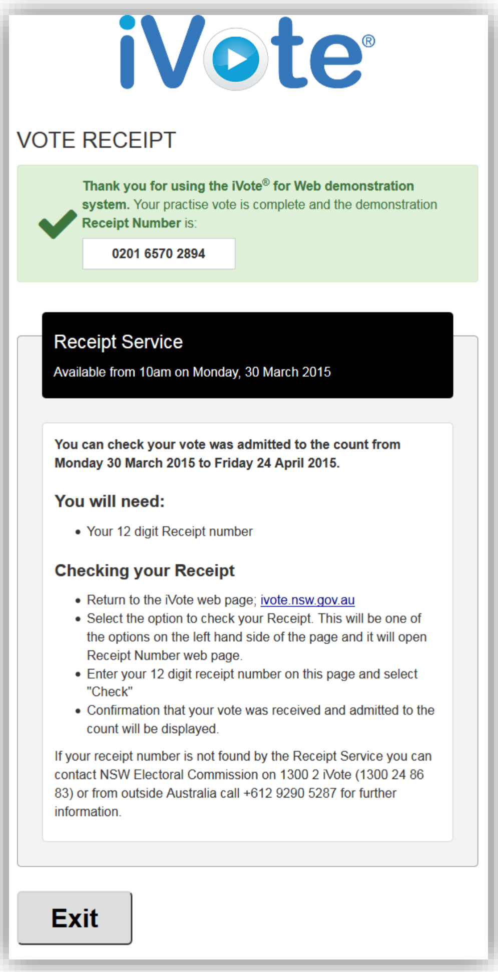
ABOVE THE LINE Demonstration only

GROUP A	GROUP B	GROUP C	GROUP D	GROUP E	GROUP F	GROUP G
1	□	2	To vote for the candidates in this group you will need to vote below the LINE.	□	□	□
	THE CITYLIFE PARTY (SPENCER DAVIS GROUP)	AUSTRALIANS FOR ADVANCEMENT		CONSERVATIVES / COUNTRY PARTY		DEMOCRATIC PARTY

BELOW THE LINE Demonstration only

GROUP A	GROUP B THE CITYLIFE PARTY (SPENCER DAVIS GROUP)	GROUP C AUSTRALIANS FOR ADVANCEMENT	GROUP D	GROUP E CONSERVATIVES / COUNTRY PARTY	GROUP F	GROUP G DEMOCRATIC PARTY
Go ahead to Group B	Go ahead to Group C Go back to Group A	Go ahead to Group D Go back to Group B	Go ahead to Group E Go back to Group C	Go ahead to Group F Go back to Group D	Go ahead to Group G Go back to Group E	Go ahead to Group H Go back to Group F
□ ADCOCK Luisa	□ VELT Mile THE CITYLIFE PARTY (SPENCER DAVIS GROUP)	□ HAND James AUSTRALIANS FOR ADVANCEMENT	□ ADAMS Charles	□ ROBERTSON Rosemary CONSERVATIVES	□ SUTHERLAND Michael	□ IRVINE Genia DEMOCRATIC PARTY
□ WOESSNER Brian	□ BIRMINGHAM Jean THE CITYLIFE PARTY (SPENCER DAVIS GROUP)	□ BUCHANAN Louise AUSTRALIANS FOR ADVANCEMENT	□ SANFORD Len	□ CARPENTER Valery COUNTRY PARTY	□ NADER Elwyn	□ DARTNELL Robert DEMOCRATIC PARTY

Sample iVote voting screen (Legislative Council)



VOTE RECEIPT

✓ **Thank you for using the iVote® for Web demonstration system.** Your practise vote is complete and the demonstration **Receipt Number** is:

0201 6570 2894

Receipt Service

Available from 10am on Monday, 30 March 2015

You can check your vote was admitted to the count from Monday 30 March 2015 to Friday 24 April 2015.

You will need:

- Your 12 digit Receipt number

Checking your Receipt

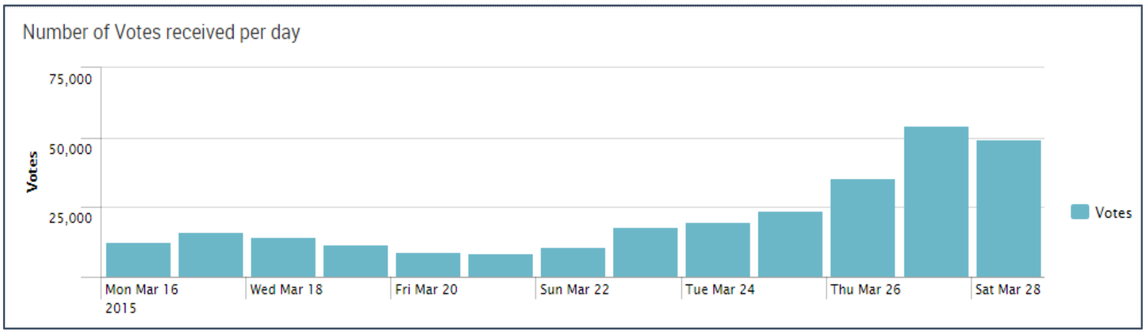
- Return to the iVote web page; ivote.nsw.gov.au
- Select the option to check your Receipt. This will be one of the options on the left hand side of the page and it will open Receipt Number web page.
- Enter your 12 digit receipt number on this page and select "Check"
- Confirmation that your vote was received and admitted to the count will be displayed.

If your receipt number is not found by the Receipt Service you can contact NSW Electoral Commission on 1300 2 iVote (1300 24 86 83) or from outside Australia call +612 9290 5287 for further information.

Voting receipt screen

Voting profile

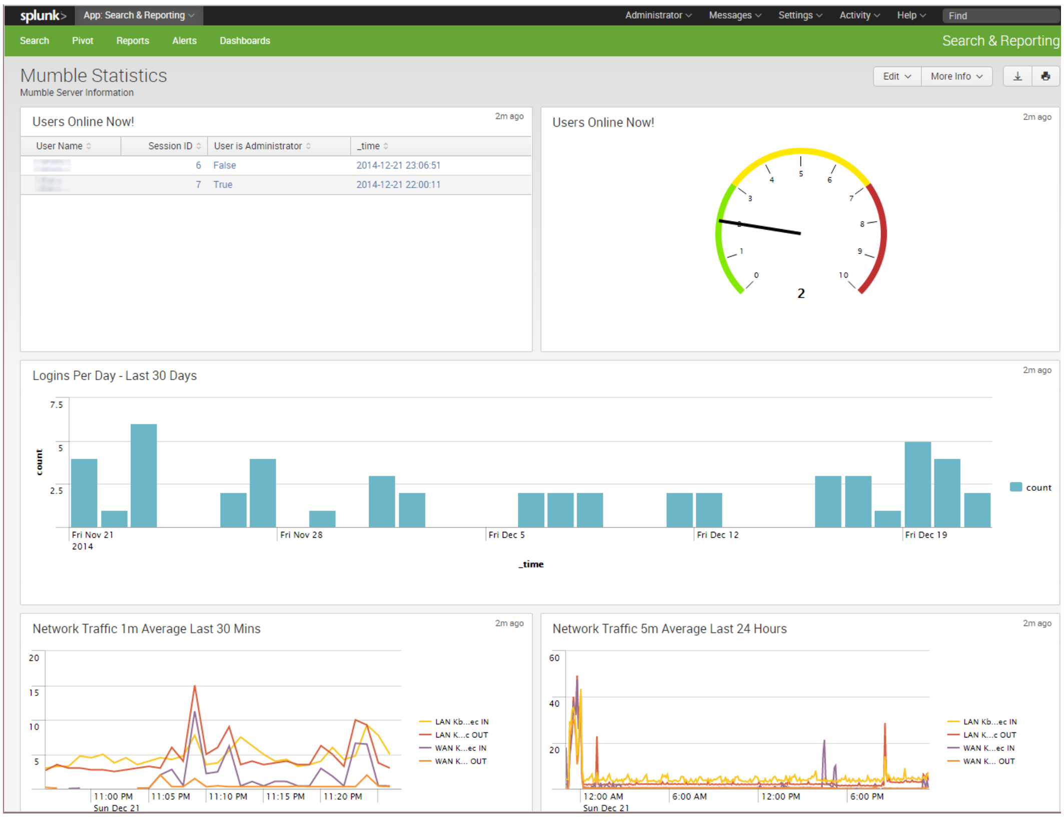
The votes per day can be seen in the following diagram. Note that on the last day, registration closed at noon as planned, thus only taking votes for 30% of the time that the polling booth was open.



Number of Votes received per day

Reporting

A control dashboard was also implemented to monitor the voting process. The figure below depicts an example of the monitoring station:



Mumble Statistics

Mumble Server Information

Users Online Now!

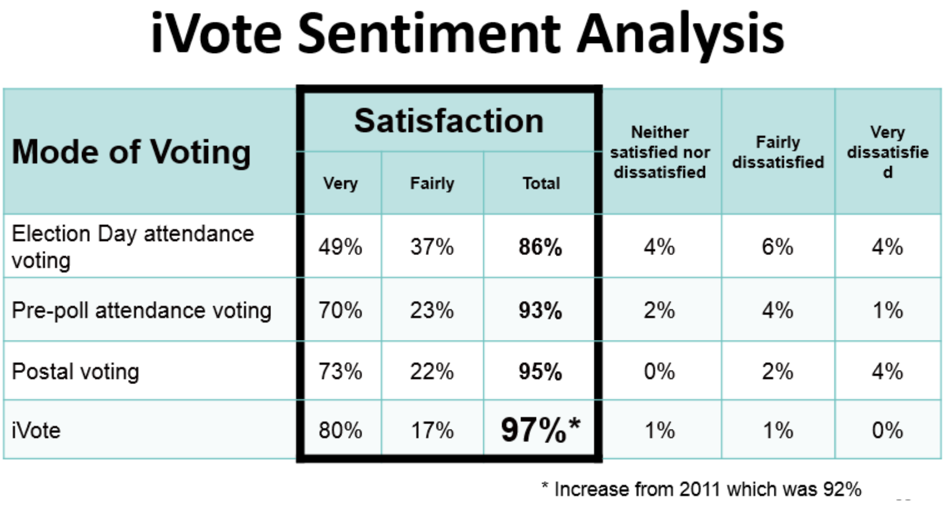
2m ago

User Name	Session ID	User is Administrator	_time
[redacted]	6	False	2014-12-21 23:06:51
[redacted]	7	True	2014-12-21 22:00:11

Figure 1 – Sample control dashboard

iVote reception by users

The following statistics were collected by IPSOS, an independent reporting agency that interviews polling users at the completion of the polling.



iVote Sentiment Analysis

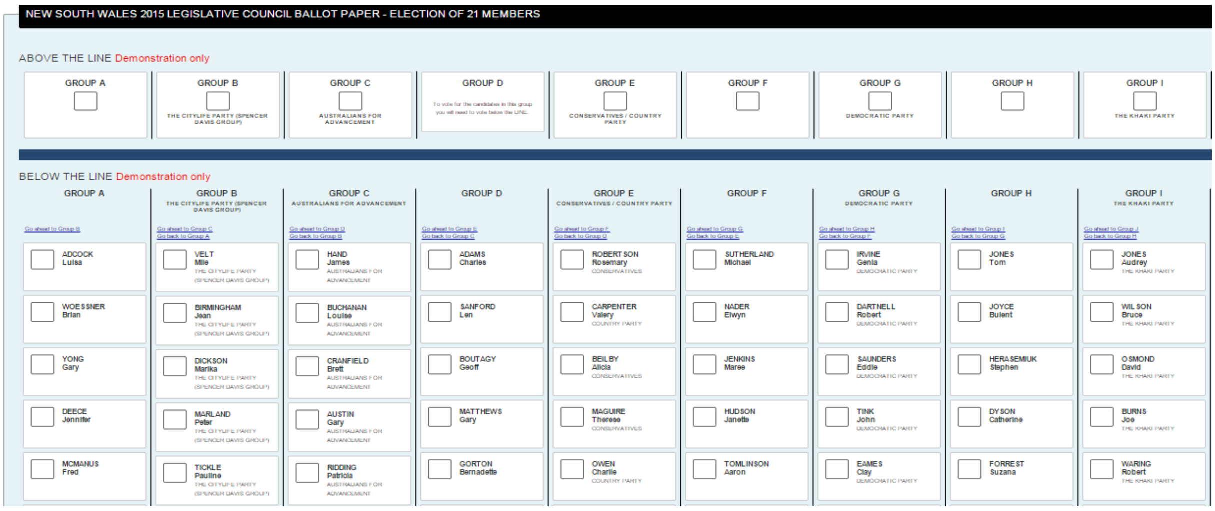
Mode of Voting	Satisfaction			Neither satisfied nor dissatisfied	Fairly dissatisfied	Very dissatisfie d
	Very	Fairly	Total			
Election Day attendance voting	49%	37%	**86%**	4%	6%	4%
Pre-poll attendance voting	70%	23%	**93%**	2%	4%	1%
Postal voting	73%	22%	**95%**	0%	2%	4%
iVote	80%	17%	**97%***	1%	1%	0%

* Increase from 2011 which was 92%

iVote Sentiment Analysis

Ballot Paper

The following screenshot depicts the upper house ballot paper on screen.



NEW SOUTH WALES 2015 LEGISLATIVE COUNCIL BALLOT PAPER - ELECTION OF 21 MEMBERS

ABOVE THE LINE Demonstration only

GROUP A	GROUP B	GROUP C	GROUP D	GROUP E	GROUP F	GROUP G	GROUP H	GROUP I
□	□ THE CITYLIFE PARTY (SPENCER DAVIS GROUP)	□ AUSTRALIANS FOR ADVANCEMENT	To vote for the candidates in this group you will need to vote below the LINE.	□ CONSERVATIVES / COUNTRY PARTY	□	□ DEMOCRATIC PARTY	□	□ THE KHAKI PARTY

BELOW THE LINE Demonstration only

GROUP A	GROUP B THE CITYLIFE PARTY (SPENCER DAVIS GROUP)	GROUP C AUSTRALIANS FOR ADVANCEMENT	GROUP D	GROUP E CONSERVATIVES / COUNTRY PARTY	GROUP F	GROUP G DEMOCRATIC PARTY	GROUP H	GROUP I THE KHAKI PARTY
Go ahead to Group B	Go ahead to Group C Go back to Group A	Go ahead to Group D Go back to Group B	Go ahead to Group E Go back to Group C	Go ahead to Group F Go back to Group D	Go ahead to Group G Go back to Group E	Go ahead to Group H Go back to Group F	Go ahead to Group I Go back to Group G	Go ahead to Group J Go back to Group H
□ ADCOCK Luisa	□ VELT Mile THE CITYLIFE PARTY (SPENCER DAVIS GROUP)	□ HAND James AUSTRALIANS FOR ADVANCEMENT	□ ADAMS Charles	□ ROBERTSON Rosemary CONSERVATIVES	□ SUTHERLAND Michael	□ IRVINE Genia DEMOCRATIC PARTY	□ JONES Tom	□ JONES Audrey THE KHAKI PARTY
□ WOESSNER Brian	□ BIRMINGHAM Jean THE CITYLIFE PARTY (SPENCER DAVIS GROUP)	□ BUCHANAN Louise AUSTRALIANS FOR ADVANCEMENT	□ SANFORD Len	□ CARPENTER Valery COUNTRY PARTY	□ NADER Elwyn	□ DARTNELL Robert DEMOCRATIC PARTY	□ JOYCE Bulent	□ WILSON Bruce THE KHAKI PARTY
□ YONG Gary	□ DICKSON Marika THE CITYLIFE PARTY (SPENCER DAVIS GROUP)	□ CRANFIELD Brett AUSTRALIANS FOR ADVANCEMENT	□ BOUTAGY Geoff	□ BEILBY Alicia CONSERVATIVES	□ JENKINS Maree	□ SAUNDERS Eddie DEMOCRATIC PARTY	□ HERASEMIUK Stephen	□ OSMOND David THE KHAKI PARTY
□ DEECE Jennifer	□ MARLAND Peter THE CITYLIFE PARTY (SPENCER DAVIS GROUP)	□ AUSTIN Gary AUSTRALIANS FOR ADVANCEMENT	□ MATTHEWS Gary	□ MAGUIRE Therese CONSERVATIVES	□ HUDSON Janette	□ TINK John DEMOCRATIC PARTY	□ DYSON Catherine	□ BURNS Joe THE KHAKI PARTY
□ MCMANUS Fred	□ TICKLE Pauline THE CITYLIFE PARTY (SPENCER DAVIS GROUP)	□ RIDDING Patricia AUSTRALIANS FOR ADVANCEMENT	□ GORTON Bernadette	□ OWEN Charlie COUNTRY PARTY	□ TOMLINSON Aaron	□ EAMES Clay DEMOCRATIC PARTY	□ FORREST Suzana	□ WARING Robert THE KHAKI PARTY

Legislative Council Ballot Paper

Project Budget

$1.2M AUD for 250,000 votes + additional fees to be charged for future use based on the use and the votes collected.

Contact details

Name:	Ian Brightwell
Position:	CIO
Address:	Level 25, 201 Kent Street, Sydney, NSW, 2000
Telephone:	(02) 9290 5999
Email:	Ian.Brightwell@elections.nsw.gov.au

2.3.6. *France. Ministry of Foreign Affairs*

Overview

The French Ministry of Foreign Affairs has introduced a secure Internet Voting platform to the French citizens living overseas. This platform has been used three times since its introduction in 2009.

In May 2009, 310.000 French voters residing in Africa and Americas were able to cast votes over the Internet in order to elect their representatives to the Assembly of the French living abroad (AFE). Poll-site voting was held on June 7, 2009. The AFE directly elects 12 senators who represent the French living abroad. This was a high-profile project in France. In October 2010, Internet Voting was used again in a by-election, involving approximately 40,000 French voters in North-America.

In 2012, the French Parliament (Assemblée Nationale) introduced 11 new seats that represent the interests of the French citizens living abroad. In May-June 2012 more than one million electors from around the world were able to vote for their representative. Around 700.000 voters with a valid email address were entitled to vote electronically during 2 weeks from any Internet-connected computer. Poll-site and postal votes were also allowed. The Internet Voting platform was available 24/7 to cover the time zone differences between the countries. More than 240.000 votes were cast online, thus resulting in the largest government binding election where Internet Voting has been used. With an impressive 73% of overseas votes in the US and Canada districts being cast online, the 2013 French Legislative Partial Elections represented a significant increase in secure online participation, with over a 65.5 % of votes cast electronically in 2013 vs. 55.5% in June 2012 national legislative election.

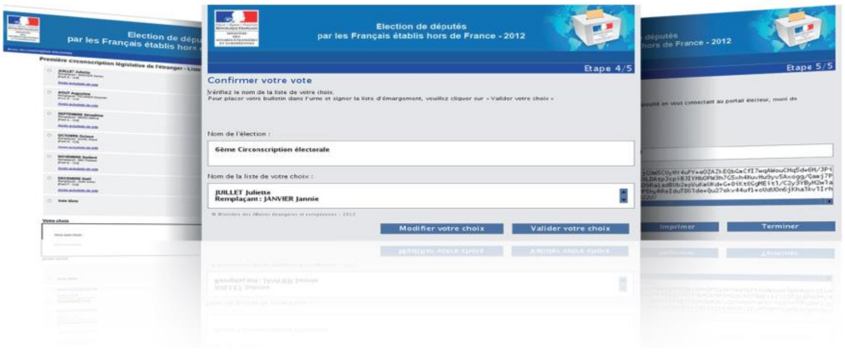
In May 2014, the elections to the Assemblée des Français de l'Etranger (AFE) once again leveraged secure Internet Voting technology. Once again, the Internet has represented the most important voting channel in a national election, marking a significant milestone in the history of e-Democracy in France.

Private vendors have provided the software and hardware*[5] required for the project:

- Internet Voting software, in compliance with the French security normative.
- Offline infrastructure and related services.

The entire solution was completely operated from France by the Ministry during the entire electoral process.

The Internet Voting solution complied with the highest standards in terms of confidentiality, security and auditability. The solution was audited by an independent auditing firm and by the national IT security agency (ANSSI), the latter certifying the solution as "RGS-certified". It is the first Internet Voting Solution to acquire this kind of certification.



Election de députés
par les Français établis hors de France - 2012

Etape 4/5

Confirmer votre vote

Vérifiez le nom de la liste de votre choix.
Pour placer votre bulletin dans l'urne et signer la liste d'émargement, veuillez cliquer sur « Valider votre choix »

Nom de l'élection :
6ème Circonscription électorale

Nom de la liste de votre choix :
JUILLET Juliette
Remplaçant : JANVIER Jannie

[5] Software was developed by Scytl, Online infrastructure was provided by Atos.

On the other hand, as a complement to the Internet Voting Solution, a tool meant to test the configuration of the voters' computers, as well as a 24/7 French speaking support service meant to assist the voters were provided.

Objectives

The objective of the French Ministry of Foreign Affairs was to approach the difficulties that the overseas citizens have when participating in the country's electoral processes. The limited number of polling places abroad and the unreliability of foreign mail services have traditionally resulted in a very low turnout. The objective of using Internet Voting was to enfranchise more overseas citizens in the Country's democratic process, while simplifying logistics, cutting costs, increasing security and still protecting voter's privacy. All these objectives have been successfully accomplished.

Project Description

In 2010, France's CNIL's, the country's body responsible for ensuring that citizens privacy is respected through Internet Voting, defined new security constraints. The evolved e-voting solution was reviewed by an independent audit company that audited the solution in a 3 steps process: before, during and after each election. A risk assessment analysis was also made concerning the implemented security processes.

On the other hand, the solution was certified by the ANSSI (National Agency of Information Systems Security) as being compliant with the RGS (Référentiel Générale de Sécurité), the French IT security standard. In order to obtain this certification the solution had to comply with the highest security standards and constraints, provide extensive and detailed documentation and pass a thorough source code audit.

Project Duration

- First election: January 2009 – July 2009
- Second election: July 2010 – October 2010
- Third election: April 2011 – June 2012
- Fourth election: June 2013
- Fifth election: May 2014

Contact details

Name:	François Saint-Paul
Position:	Director DFAE (direction des Français à l'étranger et de l'administration consulaire)
Address:	48 Rue Javel, 75015 Paris (France)
Telephone:	+33143179112
Email:	francois.saint-paul@diplomatie.gouv.fr

2.3.7. Iceland. Municipality of Ölfus

Brief Description

In order to gradually introduce and empower Internet Voting in Iceland, as well as to provide real experience and indicators to Registers Iceland in this matter, two pilot elections were to be executed during 2015. For this purpose, a customized Internet Voting platform was created that was successfully used in the first ever fully online residents' referendum in Iceland that took place in the month of March in the municipality of Ölfus.

In the Ölfus referendum, the 1432 residents aged 16+ were able to cast their vote during 10 days to decide on issues relevant to their community and they were able to do so in four different languages: Icelandic, English, Polish and Thai. The voting process was centered on whether Ölfus should enter negotiations with other municipalities for a possible merger and on choosing a date for a popular festival in Ölfus. The final participation rate of 43% of the municipality´s residents was a clear demonstration of the possibility to leverage the channel for more participatory, agile and secure referendums. In general, the participation percentage increased in the older age groups, with the participation of men over 75% surpassing the 63% participation rate.

Voters could vote from any device having access to the Internet, including mobile devices such as smartphones and tablets. For citizens with no access to the Internet, the municipality provided access to computers with Internet connection and all the necessary help at the Municipal Library.

The online citizen referendum held in the municipality of Ölfus is intended as the first of many future online referendums in the country that will be taking place across a list of selected municipalities in Iceland.

Project Description

The Internet Voting solution was integrated with the Registers Iceland Authentication System (SAML) for delegated voter authentication purposes, so that logging in to the e-voting server would be transparent to voters once they had been authenticated using the usual national service.
The Internet Voting Informational System provided for the first referendum in Iceland consisted of the following:

- A credential generation tool.
- A back office application for configuring the election data and consolidating the results.
- A voting portal accessible from any device having Internet connection.
- A receipts portal for publishing vote receipts after the election.
- A monitoring tool (Splunk) for data monitoring and analysis during the election.

The key features of the system were the following:

- A voting system to cover Municipal Referendums with end-to-end security, integrity and confidentiality.
- Integration with the existing Registers Iceland authentication system.
- Remote secure Internet Voting using standard PCs and mobile devices.
- A multilingual platform, including Icelandic, Polish and Thai languages, as well as English.
- Cross browser compatible platform with several combinations supported.
- A voting receipt mechanism for the voter to verify that the vote was recorded-as-cast.

Contact details

Name:	Bragi Leifur Hauksson
Position:	Verkefnastjóri / Project manager
Address:	Borgartúni 21, IS-105 Reykjavík
Telephone:	+354 515 5372
Email:	blh@skra.is

2.4. Maintaining the principles of democratic elections in Internet Voting Informational Systems

The introduction of new methods of casting a vote has to comply with all the existing standards and requirements for traditional elections. Most of those principles are set in the Constitution (universal, equal, direct, secret and freely expressed suffrage) and the Electoral Code.

The Article 21 of the Universal Declaration of Human Rights (UDHR)[6] stipulates the basic elements of the right to democracy and to democratic elections, stating in particular that „[…] everyone has the right to take part in the *government of his country, directly or through freely chosen representatives [...], and that the will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be* ***by universal and equal***

[6] http://www.un.org/en/universal-declaration-human-rights/

suffrage** and shall be held **by secret vote** or by **equivalent free voting procedures". At the same time, the Council of Europe Committee of Ministers Recommendation (2004) 11 on legal, operational and technical standards for e-voting[7] outlines in its Appendix I, the reflection of the basic elections principles and how these shall be maintained in the context of Internet Voting procedures.

Thus, we shall provide below a brief description of the respective co-relation of the elections principles:

Universal suffrage - The voting interface of an Internet Voting Informational System shall be understandable and easy to use. Possible registration requirements for Internet Voting shall not pose an impediment to the voter participating in elections via Internet. Internet Voting Informational Systems shall be designed, as far as it is practicable, to maximize the opportunities that such systems can provide for persons with disabilities. Unless channels of remote Internet Voting are universally accessible, they shall represent only an additional or optional means of voting (an additional voting channel).

Equal suffrage – During any election or referendum, a voter must not double vote. However, this principle is not to be confused as contradictory to "multiple voting - last vote counts" principle, which ensures uniqueness of the vote by allowing a voter to cast as many votes as he/she wants, and only the last one is counted in the final tally. Multiple Internet Voting ensures, in this way, the respect of other two basic elections principles i.e. vote secrecy and freedom of expression of the vote. Moreover, multiple voting could be an efficient instrument against purchasing of votes as the e-voters possibility to change their Internet vote reduces the motivation to exercise any influence or pressure including offering money or goods for any votes[8]. Thus, if a voter chooses to vote again when he or she has already have cast his or her vote via Internet, the previous vote shall be cancelled and replaced by the final vote casted. Consequently, the Internet Voting Informational System shall operate in such way that no double voting is possible.

Secrecy of the vote – This principle implies two dimensions: first, the voter's anonymity and second, privacy of the vote. *Anonymity* - The Internet Voting shall be organised to exclude at any stage of the voting procedure and, in particular, at voter authentication, anything that would endanger the secrecy of the vote. The Internet Voting Informational System shall guarantee that the votes in the electronic ballot box and the votes being counted are, and will remain, anonymous, and that it is not possible to reconstruct a link between the vote and the voter. Moreover, the system shall be designed in a way that the expected number of votes in any electronic ballot box will not allow the result to be linked to individual voters. Finally, the electoral body (CEC) shall ensure that the information needed during electronic processing cannot be used to breach the secrecy of the vote. *Privacy* – as the teleological interpretation of the Estonian Supreme Court showed, the remote Internet Voting requires in the first line rethinking of the principle of privacy. Voting in privacy should not be regarded as an aim by itself. To vote in secret is both a right and an obligation of the voter. The privacy dimensions of the vote secrecy are there to protect an individual from any pressure or influence against her or his free expression of political preference.[9] Thus, it's up to the voter's obligations to make sure that his or her vote is cast in privacy, free of any possible pressure. At the same time the voter shall have the freedom of choice to vote over Internet or by the traditional way. However, the traditional paper ballot will be of highest priority as Internet Voting is only an additional voting channel. ***Free voting procedures*** - The organization of Internet Voting shall secure the free formation and expression of the voter's opinion and, where required, the personal exercise of the right to vote. The way in which voters are guided through the Internet Voting process shall be designed to prevent precipitate voting or voting without reflection. Voters shall be able to change their choice at any point during the Internet Voting process before casting their vote, or to break off the procedure, without their previous choices being

[7] http://www.coe.int/t/dgap/democracy/Activities/Key-Texts/Recommendations/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf

[8] E-voting in Estonia 2005. The first practice of country-wide binding Internet Voting in the world, Ülle Madise, Tarvi Martens http://neu.e-voting.cc/wp-content/uploads/Proceedings%202006/1.1.madise_martens_e-voting_in_estonia.pdf

[9] Drechsler, W.; Madise, Ü. E-voting in Estonia. – TRAMES 2002, 3, vol 6 (56/51)

recorded or made available to any other person. The system shall not allow any manipulative influence to be exercised over the voter during the voting and it shall provide the voter with a means of participating in an election or referendum without the voter exercising a preference for any of the voting options, for example, by casting a blank vote. The Internet Voting Informational System shall indicate clearly to the voter when the vote has been cast successfully and when the whole voting procedure has been completed. The Internet Voting Informational System shall prevent double voting. Thus, as already described above, in case of multiple voting, only the last vote shall be counted; the other vote shall be automatically cancelled[10].

The Internet Voting procedures implies a set of additional specific concepts that build on the basic elections principles, namely:

a. **Alternative voting channel**. Internet Voting is not aimed to replace traditional voting. The introduction of Internet Voting means that all traditional voting methods stay. Voters are offered and auxiliary voting channel as a convenient alternative.
b. **Advanced Internet Voting**. All Internet Voting Informational Systems, if they are used as alternative voting channel, are available to use before the actual Election day, i.e. in advance, usually for a period of two to four days, say Monday to Thursday before Election Day. This is necessary for two reasons. First, this allows effective multiple voting (further explained more in detail); second, it offers sufficient time after the end of advanced voting period to Election day to mark all those voters who have voted on Internet in the voters' lists, so uniqueness of the vote is preserved, i.e. voter could not vote by paper ballot, without prior removal of his/her electronic ballot from the digital ballot box.
c. **Multiple Internet Voting (last vote counts) – highest priority vote.** As mentioned already, multiple voting does not mean double voting, which in all cases shall be considered a violation of the principle of equal suffrage. In fact, this concept means that a voter, who wants to vote on Internet, can do so multiple times during advanced Internet Voting period, and only his/her last vote will be included in the final tally. This is considered as an effective measure to prevent peer-influence on the voter. Moreover, the concept of multiple voting implies as well another concept i.e. the highest priority of the paper vote. Thus, as Internet Voting is only an alternative voting channel to the traditional elections, the right of the voter to choose to vote on paper during the Election Day, if he or she has cast an electronic vote during the Internet Voting period, shall be guaranteed. The final paper ballot vote is considered valid and of highest priority and the electronic vote is automatically cancelled by the Internet Voting Informational System.
d. **Remote voting in the uncontrolled environment**. Currently Moldovan voting system recognizes only voting in a controlled environment, i.e. voting at the designated polling station, where voters' privacy is ensured by a number of polling station officials and election observers. Remote voting over the Internet means voting from an uncontrolled environment, i.e. from home, office, or any other location where Internet access is provided.

Conclusion:

The international good practice of Internet Voting procedures provide relevant examples of how the basic election principles, as stated by the UDHR and ECHR, can be preserved. While considering the implementation of the Internet Voting Informational System, the Moldovan legal framework on elections shall be reviewed in order to adapt new specific concepts accompanying Internet Voting, such as remote Internet Voting, multiple voting – last vote counts and advanced voting. In this regards, it has to be mentioned that over time scholars and politicians have contested some of these concepts, in particular, multiple voting and voting remotely in an uncontrolled environment. Fortunately, there are already specific guidelines/recommendations on the level of the Council of Europe and practical legal solutions offered by the Estonian example, which solve and clarify the role and relevance of these concepts both to the effective implementation of the Internet Voting and to the practical preservation of the basic elections principles. It the context of the Central Electoral Commission, it may be a challenging endeavor, however a crucial one for the successful implementation of the Internet Voting Informational System in Moldova.

[10] Examples of Denmark, Sweden, UK and of Estonia since 2005.

2.5. Means of identifying the voter online and login credential delivery

Voter authentication is related to the login access to the voting system. In many ways it is equivalent to the voter's authentication process used when sending a postal ballot using a dual envelope process. Authentication mechanisms are used to identify a voter, and are to ensure that only eligible voters can cast a vote. Various means of voter identification are possible for Internet Voting.

Identification using Digital certificates

To Vote Online in Estonia, a voter has three options: ID card, digital ID or Mobile ID. To vote by means of ID card a voter needs **ID card with PIN codes, Computer** with Internet connection, **Smart card reader** and ID card **software**.

The Internet Voting by means of **digital ID.** Digital ID, i.e. digi-ID, is a document which allows identifying a person in the electronic environment and giving digital signature. Digi-ID is similar to an ID card, but without a user's photo, and it can only be used over the Internet. The stages of I-voting and the means of using digi-ID are similar to the ones used with ID card.

The I-voting by means of **mobile-ID.** This method was used for the first time during the 2011 elections to the Parliament. It required **Mobile-ID SIM card** with PIN codes and certificates, a **Computer** with Internet connection and a **Mobile phone.** There is no need to install a card reader and special software to the computer; the mobile phone with the respective SIM card performs the functions of the card and card reader simultaneously. Mobile-ID must be activated by ID card before is used.

Other countries are using different means of delivering voting credentials.

Blind envelopes

The credentials are printed in special envelopes (like the ones used by banks to issue a PIN) and sent through postal mail to each voter. This system is preferred in Canada, City of Markham:

1. Voters were sent a Voter Information Package (VIP) by mail that included instructions on how to register to vote online. The registration period was open for 3 weeks.
2. Voters that registered to vote online were required to provide private information (the PIN from the VIP and additional information) and choose a personal password.
3. Following the registration, an Internet Voter Information Package (IVIP) was sent to voters.

One Time Link (OTL)

A special link that can be clicked only once is sent to the voter's e-mail address. Once clicked, he will be redirected to a portal where he has to provide some shared secret (usually personal data like last name, date of birth, etc.) Then the credentials are shown to the voter. Optionally, they can also be sent by e-mail or SMS, or a combination of both (e.g. username by mail, and PIN by SMS). This system was used in Mexico during the Mexico City Governor election that took place on July 1st, 2012.

Mixed

In New South Wales, they used a mixed approach. The voter had to call to a Call Centre, identify himself and provide the password he wanted to use for voting. Then, the username was sent to him via e-mail, SMS, postal mail or telephone call.

3rd party integration

The authentication of the voter can depend on a third party. A service from an authorised third party takes care of the authentication and then redirects the voter to the voting platform.

3. SITUATION OVERVIEW

3.1. Overview on the electoral system of the Republic of Moldova

The Republic of Moldova is a parliamentary republic with the executive power exercised by the Government, and lead by a Prime Minister. The legislative power is exercised by the Parliament formed by 101 members of Parliament. The Parliament is elected for a 4-year term through proportional representation in a single nationwide constituency. To enter the Parliament, independent candidates must obtain 3% of the total number of votes. The political parties must pass a 6% threshold, and the electoral blocs that consist of two parties at least 9%. The electoral blocs consisting of more than two political parties must receive at least 11% of the votes. Elections are validated if the turnout is over 33%. Following the last Parliamentary Elections from 30th November 2014 five parties entered the Parliament: the Socialist Party of the Republic of Moldova - PSRM (20.51% votes), the Liberal Democratic Party of Moldova-PLDM (20.16%), the Communists Party of the Republic of Moldova-PCRM (17.48%), the Democratic Party of Moldova - PDM (15.80%) and the Liberal Party of Moldova-PL (9.67%). The current composition of the Parliament has been reshuffled in 2015-2016.

The President of the Republic of Moldova was elected via direct General Elections since 1994 until 2000. After a revision of the Constitution of the Republic of Moldova in 2000, the President was elected by the Parliament with 3/5 of votes of the members of Parliament. According to the Decision of the Constitutional Court of the Republic of Moldova issued on 4th March 2016[11], the direct election of the President was reintroduced after the Court declared non-constitutional the constitutional revisions from 2000. Thus, the Parliament of the Republic of Moldova is currently reviewing the provisions of the Electoral Code and other relevant special legislation in order to ensure the implementation of the renewed constitutional provisions and consequently to create the necessary legal conditions for the direct Presidential elections to be organized as scheduled on the 30th October 2016.

The electoral system of the Republic of Moldova is established primarily by the Constitution, the Electoral Code, other special laws, as well as by Decisions of the Central Electoral Commission (CEC). CEC is the main elections management public authority established to implement the election policy, to organize and conduct Parliamentary Elections, Presidential Elections[12], General Local Elections, Republican and Local Referendums.

3.2. The Role of the Central Electoral Commission[13]

The Central Electoral Commission is an independent state body, established to carry out electoral policy aimed to ensure proper conduct of elections, to oversight and check on compliance with the legal regulations on funding the political parties and electoral campaigns.

In its activity, CEC is guided by the Constitution of the RM, by the Electoral Code, by other laws and resolutions adopted by the Parliament, by the Moldovan President's Decrees, by Government written orders and resolutions, by field-related international treaties to which the Republic of Moldova is a party, by the CEC Rules of Procedure and by other regulatory acts.

The CEC consists of 9 members: 1 member is nominated by the President of the Republic of Moldova, the rest of the 8 members by the Parliament, ensuring the proportional representation of the Parliamentary majority and of the Parliamentary opposition.

[11] http://www.constcourt.md/ccdocview.php?tip=hotariri&docid=558&l=ro

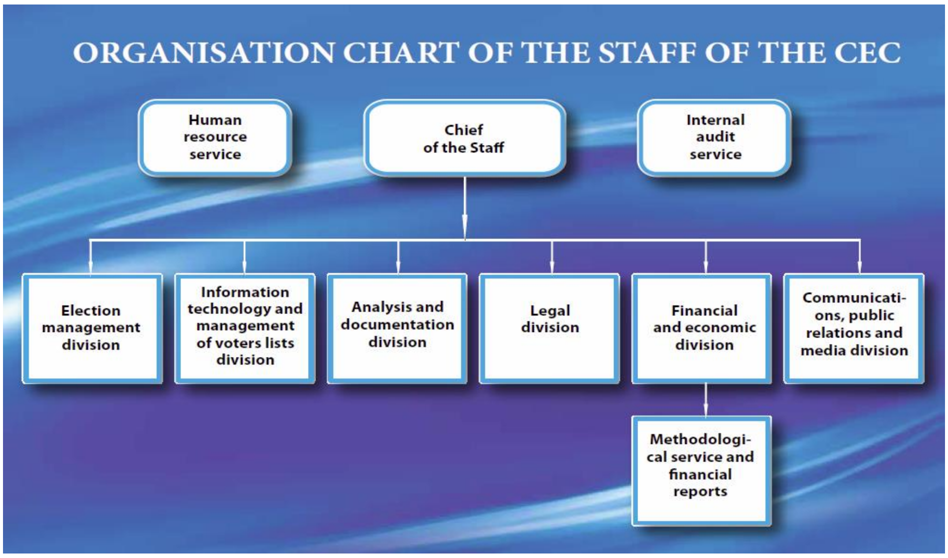
[12] Due to the Decision of the Constitutional Court issued on the 4th March 2016, the Parliament of the Republic is currently review the provisions of the Electoral Code to reintroduce the legal provisions for the organization of the direct elections of the President of the Republic of Moldova.

[13] *The Role of the CEC in the establishment and piloting the Internet Voting Information System shall be elaborated latter in the in the implementation Roadmap part of the Study.*

The mandate of the Central Electoral Commission is five years. Thus, the mandate of the current composition of the CEC expired on 11 February 2016. However, in line with the provisions of the Electoral Code[14] law can extend the mandate for 90 days.

On 17th June 2016, the Parliament of the Republic of Moldova appointed the new composition of the CEC[15].

The structure of the CEC Staff includes a chief of staff, 6 divisions (Election Management Division, Legal Division, Information Technology and Management of Voters Lists Division, Communication, PR and Media Division, Analysis and Documentation Division, Financial and Economic Division) and 2 autonomous services (Internal Audit Service and Human Resources Service) – see chart below. According to the approved numeric composition of the staff, the Staff has 37 units, currently occupied by 20 women and 8 men, with most employees aged between 25 and 40.


ORGANISATION CHART OF THE STAFF OF THE CEC
Human resource service
Chief of the Staff
Internal audit service
Election management division
Information technology and management of voters lists division
Analysis and documentation division
Legal division
Financial and economic division
Communications, public relations and media division
Methodological service and financial reports

Source: CEC[16]

3.2.1. Key Objectives of CEC

One of the key objectives of the CEC is to implement in the electoral system of the Republic of Moldova specific solutions aiming to ensure transparency, confidentiality, efficiency and accessibility of voters to the electoral process. In May 2008, the Parliament of the Republic of Moldova adopted the Law on the Concept on the State Automated Informational System "Elections" (SAISE)[17].

The long-term objective of the CEC is to implement a fully automatized electoral system in Moldova. According to the CEC Strategic Development Plan (2012-2015), during the last Parliamentary elections in 2014, the SAISE was operationalized. Thus, the State Register of Voters (SRV)[18] was introduced. The Registry is maintained by the CEC and is based on data provided by the State Register of Population[19]. Taking into account certain functioning problems of the SAISE during the 2014 Parliamentary Elections, CEC is permanently improving the SAISE and SRV operability. According

[14] Article 17 al. (6), Electoral Code of the Republic of Moldova

[15] http://www.cec.md/index.php?pag=news&id=1042&rid=15909&l=ro

[16] http://cec.md/index.php?pag=page&id=1436&l=en

[17] Law no 101 from 15.05.2008 on the Concept on the State Automated Informational System Elections (SAISE), http://lex.justice.md/md/328369/

[18] CEC Decision no 2974 from 19.11.2014 approving the State Register of Voters, http://lex.justice.md/viewdoc.php?action=view&view=doc&id=356379&lang=1

[19] The State Enterprise *Registru* maintains the State Register of Population based on data from Civil Status Service (place of residence, births, marriages and deaths), Ministry of Interior (detainees and prisoners), SE Cadastre and Agency of Land Relations and Cadastre (addresses and land demarcation), and Border Control Service.

to the CEC Strategic Development Plan (2016 - 2019)[20], CEC is aiming to develop and implement new technical solutions in order to further automatize the electoral procedures. In this regard, new technical requirements are to be developed to develop and test SAISE modules. Furthermore, aiming to create new alternative voting solutions in particular for the Moldovan citizens residing abroad, the distance/Internet Voting shall be piloted in 2018.

3.3. Legal framework

For the purpose of the present Study, an overview of the national legal framework on electoral system of the Republic of Moldova will be presented. A particular focus will be dedicated to the general legislation regulating the electoral system as well as to the specific legislative provisions related to the elections management, personal identification system, registries, digital signature and data protection.

3.3.1. Constitution of the Republic of Moldova[21]

According to the Constitution of the Republic of Moldova the President of the country[22], the members of the Parliament, the representatives in the local councils and the mayors are elected by universal, equal, direct, secret and freely expressed suffrage[23]. The Constitution also includes general provisions related to the referendums. There is no specific regulation about Internet Voting in the Constitution. As in case of the special electoral provisions, the legal framework on Internet Voting should be regulated in a special electoral law i.e. the Electoral Code of the Republic of Moldova. A set of general recommendations on Internet Voting that shall be considered to be included in the Electoral Code will be presented in the next chapter. Herewith, for the scope of the study in the context of Internet Voting, one constitutional provision would require a particular attention, namely the basic elections principles as stated in the Article 38 of the Constitution:

„Article 38. Right to Vote and Right to Stand for Election
(1) The will of the people shall constitute the basis of the State power. This will is expressed by free elections which are periodically conducted by way of a ***universal, equal, direct, secret and freely expressed suffrage.***
(2) The citizens of the Republic of Moldova, having attained the age of 18 on or by the voting day inclusively, are entitled to vote, except for the persons banned from voting by the law.
(3) The right to stand for election is guaranteed to all citizens of the Republic of Moldova enjoying the right to vote, according to the law."

In the previous chapter of the Study (i.e. *Chapter 2.4 Maintaining the principles of democratic elections in the Internet Voting Informational Systems*) the authors have provided a detailed analysis on how the Internet Voting Informational System shall be implemented so that the basic election principles provided as well by the Article 38 of the Constitution could be preserved. The authors also outlined the non-traditional elections concepts common for the Internet Voting procedures i.e. remote voting, advanced voting and multiple voting-last vote counts and explained how these concepts relate to the basic election principles. Nevertheless, a short overview of the Internet Voting implications on the Constitutional provisions shall be presented below.

From the outset, it has to be reiterated that during the implementation of Internet Voting in Moldova the respect of the basic elections constitutional principles must be ensured. Internet Voting is, first of all, an additional voting channel and the traditional voting still needs to be considered as the main and ultimate voting option. Moreover, the main rationale for introducing Internet Voting is to provide the voter with alternative possibilities to cast their vote, thus contributing to the increase of the election turnout. Therefore, without any question, the universality of the suffrage is further enhanced in Internet Voting by enlarging the possibilities for the citizens to express their vote. This is in

[20] CEC Strategic Development Plan (2016-2019) http://cec.md/files/files/Planuri%20si%20Rapoarte/Planul%20strategic%202016_2019%20(aprobat%20in%20sedinta).pdf
[21] The Constitution of the Republic of Moldova, http://lex.justice.md/document_rom.php?id=44B9F30E:7AC17731
[22] According to the Decision of the Constitutional Court no. 7 from on 05.03.2016 the Law no. 1115 from 05.07.2000 on revision of the Constitution (elections of the president) was declared non-constitutional and previous provisions of the Constitution were reintroduced (with the exception of the age limit for the candidates that was kept to 40 year old)
[23] Articles 38, 41, 61, 62, 63, 75, 78, 79 of the Constitution of the Republic of Moldova

particular relevant for the voters residing abroad who are willing, but are not able to cast the vote due to long distance up to the polling station. The internal migrants, in particular students, shall also benefit from Internet Voting. The same is relevant for the voters residing in the Transnistrian region, who met obstacles while expressing their vote during previous elections. Finally, Internet Voting could and should better meet the needs of disabled voters.

At the same time, as mentioned already, the international experience on Internet Voting was influenced as well by a number of contradictory debates among scholars and politicians over the constitutionality of the application of Internet Voting in particular in relation to the secrecy of vote over the Internet. Fortunately, the Council of Europe Committee of Minister Recommendations Rec (2004) 11 on legal, operational and technical standards for e-voting have provided concrete guidelines and explanations on how the basic principles of democratic elections could and should be respected during the implementation of the Internet Voting Informational System. Moreover, a constructive solution based on a teleological interpretation of the Constitution by the Estonian Supreme Court on the application of the secrecy of vote principle in Internet Voting was found[24]. Namely it provided that the Internet Voting act is to be seen, not as aim, but as a measure to guarantee freedom of voting, and the anonymity aspect of the principle of secrecy can be guaranteed. However, the authorities must ensure special procedures to ensure the anonymity, security, auditing and observation of Internet Voting.

In this context, it should be mentioned that the Constitutional Court of the Republic of Moldova has already ruled in 2000[25] that the secrecy of vote is not only the right of the voter, but is also an obligation. Thus, in any elections using all the existing or new channels to cast the vote, the state authorities must create all the necessary conditions to ensure the secrecy of the vote. Furthermore, in its most recent Decision from 12.02.2012[26], the Constitutional Court of the Republic of Moldova has grounded its opinion on the secrecy of vote in particular on the Council of Europe Resolution 1590 (2007) on the secret ballot – European code of conduct on secret balloting, including guidelines for politicians, observers and voters[27]. The Resolution calls on the CoE members states to guarantee the secret voting for all citizens, including the most vulnerable groups such as the elderly, people with disabilities and the illiterate, and to make sure that appropriate facilities are provided to enable such individuals to vote in secrecy.

The Resolution has also provided a list of concrete actions from the state authorities to guarantee the secrecy of the vote, which shall be respected including in the context of possible implementation in Moldova of the Internet Voting Informational System, thus ensuring its constitutionality, in particular:

- Preserve voter anonymity;
- Respect the individuality of voting and enable the voter to cast their vote freely;
- Ensure maximum security in electronic (Internet) voting by providing secure data transfer and preserving voter anonymity;
- Make sure that electoral officials do not interfere with secret voting;
- Provide and expand facilities and equipment that guarantee secret voting (polling stations, polling booths, mobile ballot boxes, etc.), thereby ensuring confidentiality.

Thus, the recent constitutional practice of the Republic of Moldova, in particular the 2012 Decision of the Court paves a way for the application of the Internet Voting in Moldova in relation to the vote secrecy. However, we may still anticipate further internal academic, political and legal debates in Moldova about the constitutionality of Internet Voting. In this regards, the legislator shall take into account the existing practices and experience of other countries, which are using Internet Voting for

[24] Supreme Court of Estonia, Constitutional Judgment 3-4-1-13-05 from 1.09.2005 http://www.nc.ee/?id=381
[25] Constitutional Court Decision nr. 39 from 04.12.2010 http://www.constcourt.md/public/files/file/Actele%20Curtii/acte_2000/h_39.pdf
[26] Constitutional Court Decision nr. 1 from 12.01.2012 http://lex.justice.md/md/341979/
[27] Council of Europe Resolution 1590 (2007) on Secret Ballot http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=17609&lang=en

national and local elations, as in the case of Estonia. From this perspective, the Constitutional Court of the Republic of Moldova may be called to provide a more extensive interpretation of the Article 38 of the Constitution in the context of the Internet Voting Informational System with reference to the secret nature of the electronic voting (in particular, the privacy dimension of the principle).

General Conclusion of Constitutional provisions:

There is no specific regulation of Internet Voting in the Constitution of the Republic of Moldova. The basic election principles stated particularly in the Article 38 of the Constitution must be ensured. At the same time, learning the lessons of the Estonian experience, the Constitutional Court of the Republic of Moldova may be called to provide a more extensive interpretation of Article 38 of the Constitution in the context of the Internet Voting Informational System.

3.3.2. Electoral Legislation of the Republic of Moldova

3.3.2.1. The Electoral Code of the Republic of Moldova[28]

The Electoral Code of the Republic of Moldova (hereafter the Electoral Code), structured in 7 titles and 205 Articles, is the special national law regulating the application of the basic elections principles, the electoral system, voters lists, the role and competencies of the Central Electoral Commission and its subsidiary elections management bodies, the preparation and conduct of the referendums and the national elections of the members of Parliament, the President of the country[29], the local elections of the representatives in the local councils and mayors.

The Electoral Code does not include specific provisions regulating Internet Voting policies, rules, procedures, and relevant functioning and the management requirements for the Internet Voting Informational System. Moreover, on top of a special attention that has to be paid to the respect of the constitutional election principles during the implementation of the Internet Voting Informational System, the legislator must as well introduce in the Electoral Code new concepts specific to the Internet Voting that are not currently regulated in Moldova. For instance the Electoral Code does not provide for the advanced voting concept, as only one voting options is allowed i.e. vote on Election Day. Also, there are no provisions on remote voting from an uncontrolled environment. The Electoral Code does not stipulate provisions that would explain the principle of multiple voting-last voting counts, taking into account that Internet Voting involves the possibility for repeated vote cast of the electronic ballot.

In addition to these concepts, in order to create a proper legal framework for the implementation of Internet Voting, the Electoral Code shall be amended introducing Internet Voting verification and cancellation rules, voting secrecy assurance principles, voter identification aspects, information systems establishing the framework for its functional, security and audit requirements.

Finally, a new Title on Internet Voting shall be introduced in the Electoral Code. The Central Electoral Commission can also consider, if deems necessary, to establish a separate Internet Voting Electoral Council (IVEC), created on the same principles as District or Local Electoral Councils.

In this regards, taking into account the existing recommendations and resolutions of the Council of Europe and OSCE/ODIHR, as well the existing legal framework adopted in Estonia on Internet Voting[30], we shall present below a set of basic guidelines for the Central Electoral Commission that could be taken into account during the preparation of the relevant legislative amendments to the Electoral Code on Internet Voting. For more detailed reference to specific provisions on Internet Voting that shall be transposed in the legislative amendments, Chapter 2.4 (principles and concepts)

[28] The Electoral Code of the Republic of Moldova, http://cec.md/files/files/blocul_COD_Elect-2014__eng_07-11-12_corect_FINAL.pdf

[29] The provisions of the Electoral Code on the elections of the President of the Republic of Moldova are currently being reviewed by the Parliament, due to the Decision of the Constitutional Court on the basis of which direct elections of the President was reintroduced (Decision of the Constitutional Court no. 7 from on 05.03.2016)

[30] https://www.riigiteataja.ee/en/eli/ee/514112013015/consolide/current

and Chapter 4 (propositions for the Internet Voting Informational System in Moldova) of the Study shall be consulted.

General Provisions: Definitions and Principles

- The following definitions shall be introduced: Internet Voting; remote Internet Voting; advance Internet Voting; electronic ballot box; electronic ballot; vote in a controlled and an uncontrolled environment;
- The following Internet Voting concepts have to be introduced: Internet Voting is an alternative voting channel, remote voting in uncontrolled environment, advanced voting, last vote counts, priority of the vote cast on a paper during the Election Day; Internet Voting secrecy.

I. A separate Internet Voting Title (ex. Title II1) shall provide for:

- Provisions on the procedures for appointing and formation of the Internet Voting Electoral Council (IVEC) within the Central Electoral Commission, if deemed necessary by the CEC. The main functions and competences of the IVEC shall be expressly provided in particular underlining its role in the management, preparation and organization of Internet Voting.
- Preparation of Internet Voting including: preliminary registration of voters willing to vote over the internet, preparation and approval of the electronic ballot and electronic ballot box, creation of the encryption key for the Internet vote and the vote-opening encryption key for the members of the Central Electoral Commission;
- Procedures related to the preparation, initiation, counting and termination of Internet Voting, including: voting time, identification of voter, vote casting, encryption of the electronic vote, submission of the vote in the electronic ballot box, cancelation procedures, verification, vote changing, Internet Voting counting, priority of the paper ballot during the Election Day, special provisions for Internet Voting abroad;
- Functional and security requirements of the Internet Voting Informational System, including: the ownership and management of the IVIS; minimum requirements to cast a vote online; voter identification process; conditions to start Internet Voting implementation, the conditions for ensuring secrecy of Internet Voting; vote verification process; avoidance of double voting, Internet vote auditing, cyber security.

II. Final Provisions

- The final provision should provide for the implementation of the Internet Voting Informational System and, thus, the timeframe for entering into force of the Internet Voting amendments to the Electoral Code.

General Conclusion on Electoral Code:

The Electoral Code does not include specific provisions regulating Internet Voting concepts, policies, rules, procedures, and relevant functioning and the management requirements for the Internet Voting Informational System. In order to create a proper legal framework for the implementation of Internet Voting, the Electoral Code shall be amended introducing the Internet Voting concepts, vote verification and cancellation rules, voting secrecy assurance principles, voter identification aspects, information systems establishing the framework for its functional, security and audit requirements and other elements common to Internet Voting. A new Title on Internet Voting shall be introduced in the Electoral Code. The Central Electoral Commission can also consider, if deems necessary, to establish a separate Internet Voting Electoral Council (IVEC). Prior to the adoption of the amendments to the Electoral Code introducing specific Internet Voting legislation the opinions of the Venice Commission and OSCE/ODIHR shall be consulted.

3.3.2.2. Special legislation relevant to the introduction of the Internet Voting Informational System

Law no. 101 on the Concept of the State Automated Informational System "Elections" (SAISE)[31]

The Law no 101 provides for the legal basis for the development and implementation of the State Automated informational System "Elections"(SAISE). The overall objective of SAISE is to conduct entirely automated elections in Moldova. Thus, the automated management of the electoral process is aiming at reducing the costs and improving the control and transparency of the electoral system of the Republic of Moldova[32].

The Concept envisaged the preparation of almost all election-related documentation, including voter lists, identification of citizens in the electronic electoral system, implementation of digital signature procedure, observer accreditation documents, authorizations, and various forms and protocols through SAISE.

The Concept foresees the future development of a separate SAISE module that would introduce electronic (Internet) voting as an alternative elections option[33], using digital means with certified e-signature[34].

However, one provision of the Law no 101 shall be reviewed in parallel with the legislative amendments to the Electoral Code for the introduction of Internet Voting, clarifying the difference between double voting, which shall be ensured in all cases and the concept of multiple Internet Voting-last vote counts, including paper ballot vote priority. The 4th paragraph of the introduction part of the Concept reads that *if a vote was cast electronically, there shall not be permitted to cast a vote on paper at another polling station*. This shall be valid for the electronic vote cast using electronic voting kiosk at the polling stations, however it shall not be relevant for the vote casted over Internet. As described in the previous chapter, the Internet Voting implies specific concepts that shall be implemented. The concept of last vote counts and the ability of the voter to choose to vote again on paper if he/she considers so, should be ensured, as it is there to enhance the respect of the basic election principle of the vote secrecy and freedom of elections in Internet Voting. Moreover, Internet Voting is an alternative channel for casting the vote. The right of the citizen to vote by paper ballot should be kept, even for those voters who have already expressed their vote over the Internet. Thus, it shall be clear that if a person cast his or her vote over the Internet, he or she should be allowed to vote again during the Internet Voting period or on paper during the Election Day. At the same time, the Internet Voting Informational System shall ensure the automatic cancellation of the previous vote. Only the last vote shall be counted, avoiding double voting.

The Law also introduces the State Register of Voters (SRV), which is developed on the basis of the data from the State Register of Population (SRP), and is managed by the Central Electoral Commission. The SRV is operational since November 2014.

SAISE is owned, managed and maintained by the CEC[35]. SAISE data registrars are authorized on the basis of the CEC decisions. For every electoral period a separate data base resource is created by the CEC, which is updated until the end of the mandate of the electoral bodies[36]. After the termination of the electoral period, the respective date resource is archived and is accessible only in the "view" regime to the persons entitled by the CEC. The Concept also foresees 3 levels of infrastructure: central (CEC), regional (Districts – II level localities) and local (I level localities).

[31] http://lex.justice.md/md/328369/
[32] Introduction part of the Concept, 4th para.
[33] Law no 101 on the SAISE Concept, Chapter I, Chapter. III p. 9, 5), letter c)
[34] Law no 101 on the SAISE Concept, Chapter. II p. 8 letter b)
[35] The SAISE Concept, Point IV.10
[36] The SAISE Concept, Chapter IV. Data Resources

According to the Concept[37], 7 Function Blocks of the SAISE were envisaged to be developed, namely:

1. *"Voter Lists" Block* – aiming to implement functions associated with compilation, verification, printing and editing of voter lists.
2. *"Preparation" Block* – has the function of registering lists of polling stations, election administration members and accredited observers.
3. *"Competitors" Block* – aiming to manage the data of political parties and candidates competing in elections and their authorized representatives.
4. *"Documentation" Block* – aiming to prepare accreditation documents, authorizations to elections officials, generation of all election-related documents such as voter lists, various protocols, other acts, among other things.
5. *"Voting" Block* – aiming to provide the possibility of marking voters who were issued ballots in an online system to prevent double voting; introduction of Internet (electronic) voting enabling automatic aggregation of data (e.g. electronic pens, ballot scanners; conduct of electronic voting for voters in all polling stations and from abroad; compilation of reports on voter turnout and aggregation of elections results).
6. *"Rotation" Block* – aiming to manage records of persons who have to leave an elected post and of their replacements.
7. *"Financial Control" Block* – provides for the recording of various statements on financial expenditures submitted by electoral competitors, the recording of loans granted by the state and control over these loans by calculating the amounts to be returned based on the election results.

***Conclusion:** The law no. 101 on SAISE provides the necessary legal provisions stated in Chapter II and III of the Concept to initiate the creation of the Internet Voting Informational System. At the same time, the provision on double voting mentioned in the introduction of the Law shall be clarified so that multiple voting on the condition of last vote counts and highest priority paper vote is allowed. However, as the Electoral Code shall be amended to introduce the new concepts, rules and requirements specific for the functioning and management of the Internet Voting Informational System, the current Law shall be reviewed as well in particular in its part related to electronic voting.*

Law on registers[38]

The law establishes the legal framework of the establishment, registration, maintenance, evidence, reorganization and liquidation of registers in the Republic of Moldova. The law also regulates the types of registers, the forms of keeping data records, the relationship and the principles of interoperability of the system of state registers, as well as the responsibilities and functions of the owners of the registers and of the control authorities. The law refers to all types of register, regardless of their form of ownership.

***Conclusion:** The law provides the main legal basis for the development and functioning of the State Register of Voters owned by CEC.*

Law of the Republic of Moldova on Informatization and State Information Resources[39]

The law establishes the basic rules and conditions for the creation and development of a national information infrastructure as the operating environment of the information society in Moldova. The law also regulates the legal relations arising in the process of creating, training and using the automated state informational resources, technologies, networks and the information systems.

***Conclusion:** The law provides for the main legal basis for the development and functioning of the State Automated Informational System "Elections" and respectively for the creation of Internet Voting Informational System.*

[37] The SAISE Concept, Chapter III. Functions of the SAISE
[38] http://lex.justice.md/md/325732/
[39] http://lex.justice.md/md/313189/

Law on the identity documents from the national passport system[40]

The law establishes the legal framework for the types of identity documents issued to the citizens of the Republic of Moldova. The law regulated the following types of identity documents: passports, ID cards and residence permits. A separate Governmental Decision regulates the issuance of the electronic ID cards[41].

According to the law the Ministry of Information Technology and Communication is the issuing authority. At the same time, the State Owned Enterprise "Centre for State Information Resources "Registru", subordinated to the Ministry of Information Technology and Communication, is the public service provider for the issuance of all types of identity documents.

Conclusion: *The law provides the necessary legal framework for the voter authentication in the IVIS using the E-ID cards. The specific legal requirements and further developed in the Governmental Decision on the implementation of the E-ID. However, it has to be noted that the identification of the voter in IVIS shall not be limited to the E-ID cards as the number of E-ID cards holders in the Republic of Moldova is still not numerous.*

Law on electronic signature and electronic document[42]

The law provides the legal regime of the digital signature and electronic document, including the essential requirements of their use, and certification services. The law transposes the provisions of the EU Directive 1999/93/CE on digital signatures. The law regulates the types of digital signatures, namely simple electronic signature, non-qualified advanced digital signature and qualified advanced digital signature. Article 5 of the Law provides that all digital signatures, regardless of the degree of protection, produce legal effects. However, only the qualified advanced type of the signature has the same legal effect as the handwritten signature on hard copy document.

Individual persons can generate private and public keys used for the creation of the nonqualified advanced digital signatures. Private and public keys used for the creation of qualified advanced digital signatures are generated by the certification service provider using a special secured device for the creation of the signature, integrated in the ID card or via SIM card device for the mobile electronic signature. The validity of the certificate for the public key of the certification service provider varies from 10 to 20 year (depending on the grade). The validity of the certificate for the public key of the user is established by the certification service provider but shall not be longer than 1 year. The law states provisions on the creation, verification and use of the digital signature. The law states provisions and conditions on the recognition of the foreign digital signatures. The law also regulates the legal regime of the *electronic documents*, which are signed with the digital signature. According to the law an electronic document must meet the following requirements:

- to be created, processed, shipped, received, maintained, altered and/or destroyed by technical means and/or a program;
- to contain, for confirming its authenticity, one or more digital signatures;
- to be created and used by methods and in a form that would allow identification of the signatory;
- to be displayed in a perceivable form;
- to allow repeated use.

Conclusion: *The law provides the necessary legal conditions for the electronic authentication of the voter within the IVIS by means of qualified advanced electronic signatures issued by the accredited national certification authority* (mobile Signature, E-ID cards or digital means). Moreover, the law provides for the Central Electoral Commission to be the accredited entity to issue special certified electronic credentials for the voter in order to authenticate and/or cast an electronic vote within the IVIS for those voters who are not able to access the Mobile signature, E-ID cards or other certified digital means.

[40] http://lex.justice.md/md/311641/
[41] http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=350151
[42] http://lex.justice.md/md/353612/

Law on personal data protection[43]

This law regulates relations arising in the course of the processing operations of personal data performed wholly or partly by automatic means, and otherwise than by automatic means, which are part of a filing system or are intended to be included in such a filing system. The law is transposing the EU Directive 95/46/EC on the protection of individuals regarding the processing of personal data and the free movement of such data.

The law requires all processors of personal data to notify the National Data Protection Authority (National Center for Personal Data Protection - NCPDP) of an intended processing operation before it is performed. Moreover, a supplementary processing operation may not be performed until a new notification is submitted. After giving notification, processing operators will receive a registration number that must be reflected on all acts by which personal data is collected, stored or, transferred.

Processors carrying out certain operations – such as the processing of personal data by electronic means within systems that generate individual decisions about the solvency or professional competence of individuals – will have to pass supplementary preliminary checks by the NCPDP on whether the operations comply with the new legislation or not. These preliminary checks must not exceed 45 days from submission (in complex cases, plus an additional 45 days). Processing personal data without the NCPDP's authorization is prohibited. The NCPDP is keeping a register of all personal data processors in Moldova. At the same, time the trans-border transfer of personal data must be authorized by the NCPDP, who will give authorization only if the destination country ensures adequate protection of the data. This will be decided on a case-by-case basis.

The NCPDP may authorize the cross-border transfer of personal data even if the destination country does not ensure an appropriate level of protection, but subject to the condition that the processor present sufficient guarantees to ensure protection (i.e. an agreement signed between the processor and persons processing the personal data abroad).

Conclusion: *The existing legislation on personal data protection required for the introduction of the* IVIS *is generally in place. According to the law any personal data shall be subject to consent for the processing of personal data. Article 3 of the Law on personal data protection states that the consent for processing personal data is any freely given, expressly and unconditionally indication of will, in written or electronic form, according to the requirements of the electronic document, by which the personal data subject signifies his/her agreement to personal data relating to him/her being processed. Thus, for the introduction of the Internet Voting Informational System, a preliminary registration shall be performed and a validation of the voter's consent to deliver credentials shall be considered. At the same time, a check box for the online processing of the personal data of the voter shall be introduced in the Internet Voting Informational System. In another context, it has to be noted that for the creation, operation and management of the IVIS, CEC shall apply for the authorization from the NCPDP, even in the piloting phase.*

General Conclusion on the special legislation:

The existing special legislation on SAISE, registries, ID documents, E-Signature provides the necessary minimum legal provisions for establishing the Internet Voting Informational System. However, the Law on SAISE may require to be amended as well in part it relates to Internet Voting. As for the data protection requirements related to Internet Voting, a preliminary registration of the voter shall be performed, including a validation of his/her consent to deliver credentials shall be considered. At the same time, a check box for the online processing of the personal data of the voter shall be introduced in the Internet Voting Informational System. In another context, it has to be noted that for the creation, operation and management of the IVIS, CEC shall apply for the authorization from the NCPDP, even in the piloting phase.

3.3.2.3. Governmental Decisions

Governmental Decision on the implementation of electronic identification document[44]

The Governmental Decision provides the legal provisions for the implementation of the electronic identification document (E-ID cards) for the purpose of accessing electronic documents and for the

[43] http://lex.justice.md/md/340495/
[44] http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=350151

generation of the electronic signatures. The E-ID cards contain the means for the electronic signature, and are serving as an identification and authentication document of the persons in the informational resources and systems, as well as for the provided electronic services.

The Decision is based on the provisions of the Law no. 273 on the identity documents from the national passport system and the Law no 71 on registers. The issuing authority by the law is the Minister of Information Technology and Communication, performed by the SE "Registru", which is the service provider authorized for the issuance, use and actualization of the public keys certificates and electronic signatures issued under the E-ID cards.

Conclusion: *The Governmental decision on electronic identification of document provides the specific regulation of the E-ID implementation in line with the Law no. 273 on IDs.*

Government Decision on the integrated electronic service for authentication and access control (MPass)[45]

The Decision establishes the Regulation on the operation and management of the electronic governmental service for the authentication and access control service for electronic services. MPass governmental service enables a better control of personal data and users' permissions, thus reducing the costs associated with their management.

The user authentication function may be exercised by various methods - mobile signature, national electronic identity (E-ID cards), and digital certificates. Using one of the authentication methods, the user can access multiple electronic services in a secure way and without directly registering at service providers. Access control and authorization features allow the monitoring and the administration centralization for various electronic services.

The MPass service is owned by the E-Government Center[46] and the technical operation management authority is of SE "Center for Special Telecommunications". The participants of the MPass service are: the MPass service owner, technical operator of the service, MPass beneficiaries; identification provider, authorization provider, validation of user accounts operator, MPass service administrator, access administrator and MPass (legal entities and individuals). The MPass service is hosted by the governmental integrated electronic platform – *MCloud*.

Conclusion: *The governmental Decision on MPass provides the legal framework and technical requirements for the use of MPass governmental service for the identification of the voter in the IVIS.*

Governmental Decision on the governmental integrated electronic service for electronic signature (MSign)[47]

The Decision establishes Regulations for the operation and management of electronic government service integrated for the electronic signature (MSign).

MSign is a governmental service, which offers the possibility for the user of all types of electronic signatures to interact in an on-line space, sign and verify the authenticity of the electronic signatures in guaranteed secured environment. The MSign service is owned by the E-Government Center[48] and the technical operation management authority is of SE "Center for Special Telecommunications". The MSign service is hosted by the governmental integrated electronic platform - *MCloud.*

Conclusion: *The governmental Decision on MSign provides the legal framework and technical requirements for applied the electronic signature by the voter the IVIS.*

General Conclusion on Governmental Decisions:

The special legal provisions offered by the Governmental Decisions provide the necessary legal and technical requirements for the creation, functioning, management of the IVIS. At the same time, the existing provisions provide

[45] http://lex.justice.md/md/351035/
[46] https://mpass.gov.md/?lang=en
[47] http://lex.justice.md/md/353239/
[48] https://msign.gov.md/?lang=en

the conditions needed for the identification, casting and verification of the electronic vote with an electronic signature processed in the IVIS.

3.3.2.4. CEC Decisions

CEC Decision approving the Regulation on State Register of Voters[49]

The Decision regulates the functioning of the State Register of Voters (SRV). SRV is a single integrated informational system, part of the SAISE, however, which operates independently as the functioning of the SRV is not dependent on the functioning of the SAISE.

The Regulation provides the creation of the register, its content, functions, and maintenance rules, responsibilities of the owner, administrator and registrar, the legal regime of data processing, access, use and development of the voter's lists on the basis of the SRV.

SRV is owned by the Central Election Commission and is developed on the basis of data of the State Register of Population (SRP) developed and owned by the Ministry of Information Technology and Communications.

The protection and security of the personal data processed in the SRV, is ensured by the Central Electoral Commission, through the implementation of the Information Security and Quality Management within the Central Electoral Commission Standard EN ISO 9001:2008 and SR ISO/CEI 27001:2013.

SRV keeps records of the voters from the Republic of Moldova. The Register is designed to collect, keep, update and analyze data about citizens of the Republic of Moldova who have reached the age of 18 years and do not have legal impediments to vote. The creation, management, amendment and update of the State Register of Voters are ensured by the Central Electoral Commission. SRV is designed exclusively for election processes and are accessible on the website of the Central Electoral Commission, each voter having access only to his/her personal information.

The following information about each voter is included in the SRV:

- surname and given name;
- date, month and year of birth;
- state identification number (IDPN);
- domicile address (state, settlement, street, house, apartment);
- residence address (state, settlement, street, house, apartment);
- group and number of the identity document (national ID, passport, military ID).

Voters with domicile or residence abroad, as well as voters who are temporarily located abroad, are included in the SRV upon a request with the respective information about their last domicile or residence.

Conclusion: *The CEC Decision on SRV provides necessary preconditions for the introduction of the IVIS. In fact the IVIS shall be created on the basis of the SRV and SAISE. However, further development of SRV modules shall be ensured in line with the CEC Strategic Development Plan (as mentioned below).*

CEC Decision approving the Strategic Development Plan of the Central Electoral Commission 2016-2019[50]

The CEC Strategic Development Plan is the main managerial and strategic planning document that refers to the organization and conduct of elections and referenda as well as political party and electoral campaign financing. From this perspective, CEC sets the strategic objectives and concrete actions required to attain the established objectives, analyses, evaluate the previous activities, proposing improvement measures.

[49] http://lex.justice.md/md/356379/

[50] http://www.cec.md/files/files/Planuri%20si%20Rapoarte/Planul%20strategic%202016_2019%20(aprobat%20in%20sedinta).pdf

The first Strategic Development Plan of CEC covered the period of 2012-2015[51]. The current Plan provides actions to be implemented in the following years, 2016-2019 and is part of a continuous, cyclical and repetitive planning process, which includes new comprehensive strategic objectives and actions to underpin the development and upgrade of the electoral process for these years.

CEC's priority in the development period 2016-2019 is to ensure a modern, efficient and accessible electoral process, in particular by the development and the implementation of new technical solutions for automating the electoral procedures. Thus, the main objective of the Plan is to develop all the necessary technical requirements of the SAISE Modules, according to the Law No. 101 on the SAISE Concept.

Conclusion: *The CEC Strategic Development Plan aims to extend the term for the on-line registration of overseas voters and to conduct the piloting of the Internet Voting by 2018 Parliamentary Elections.*

CEC Decision on preliminary registration of Moldovan citizens residing abroad who have the right to vote[52]

The decision establishes the Regulation that provides for the preliminary registration of the Moldovan voters residing abroad. The Regulation states as well the procedures for the selection of the countries and places for the opening of the additional polling stations outside the Diplomatic and Consular missions; a better organization of the voters' lists residing abroad, taking into account that from the moment of the preliminary registration the voter is excluded from the main voters' lists where the person is registered as residing in the Republic of Moldova and is registered at the place of residence abroad; establishing the number of ballot papers that shall be distributed at the polling stations abroad[53]; prolongation of the deadlines for the preliminary registration, which by rule starts 6 month prior to the expiration of the mandate of the previous Parliament (2 month in the case of early elections) and ends 40 days before the Election Day.

The main goal of the preliminary registration is to bring the polling stations as close as possible to the voter abroad. A special on-line application for the preliminary registration is made available by CEC at www.alegator.md.

Conclusion: *The CEC decision on preliminary registration of voters abroad provides already a solid legal and technical basis for the further development of the SRV and implementation of the Internet Voting Informational System. However, as stated in the CEC Strategic Development Plan the extension of the time limit for preliminary registration is necessary in order to identify accurately the potential overseas voter, and in the mid-term perspective will be used for the preliminary registration of voters who choose to vote over Internet.*

General conclusion on the CEC Decisions:

The existing CEC decisions provide the necessary technical requirements for the preparation and initiation of the CEC internal procedures for piloting and establishing the Internet Voting Informational System. However, a separate Regulation on the Internet Voting shall be considered and adopted by the Central Electoral Commission. Although according to the CEC Strategic Development Plan (2016- 2019), Internet Voting is foreseen to be piloted in 2018, a special Decision on Piloting of the Internet Voting should be prepared and adopted by CEC, describing all required procedures to ensure its implementation in line with the findings of the present feasibility study and proposed implementation Roadmaps (piloting and full implementation of IVIS).

3.3.3. International documents

Electoral standards based on public international law are well-elaborated in documents issued by intergovernmental organizations such as the United Nations; the Council of Europe; including its European Commission for Democracy through Law (the Venice Commission); the European Union; the Organization for Security and Cooperation in Europe (OSCE); and other bodies. These sources

[51] http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=341800
[52] CEC Decision no. 2547 from 21 May 2014
[53] According to the Electoral Code the polling stations abroad and in Moldova are opened from a maximum of 3000 voters.

illustrate a common understanding of the content of international electoral standards, drawing directly from the wording of Article 21 of the Universal Declaration of Human Rights, Article 25 of the International Covenant on Civil and Political Rights (ICCPR), other articles in those documents related to the exercise of rights that are essential to democratic elections, and other human rights treaties, declarations and instruments.

The core of these international electoral standards can be defined as the non-discriminating right of citizens to take part in government and public affairs, directly or indirectly through freely chosen representatives, by exercising their right to vote and to be elected through genuine, universal, equal elections, held by secret ballot and guaranteeing the free expression of the will of the electors. This combines with the right to seek, receive and impart information (i.e., the freedom of expression) about the nature of electoral processes, forming the basis for electoral transparency[54].

Given previous international practice in the implementation of the Internet Voting in other countries, in particular Estonia, the following international documents were analyzed for the purposes of this Study:

- Code of Good Practice in Electoral Matters, adopted by the Council for Democratic Elections of the Council of Europe and the European Commission for Democracy through Law[55].
- The Recommendation Rec (2004)11 on legal, operational and technical standards for e-voting[56].

The Recommendation defines e-voting as an e-election or e-referendum that involves the use of electronic means in at least the casting of the vote. Furthermore, the Recommendation refers to remote e-voting as a type of e-voting where the casting of the vote is done by a device not controlled by an electoral official. The use of electronics in "at least the casting of the vote" means, in practical terms, that e-voting covers the use of electronic voting machines and Internet Voting with ballots in electronic format.

The Section (iv) of the Paragraph 3.2 of Code of Good Practice in Electoral Matters states that “electronic voting should be used only if it is safe and reliable; in particular, voters should be able to obtain a confirmation of their votes and to correct them, if necessary, respecting secret suffrage; the system must be transparent”.

The Explanatory report of the Code of Good Practice in Electoral Matters articles 42-44:

“*42. Several countries are already using, or are preparing to introduce mechanical and electronic voting methods. The advantage of these methods becomes apparent when a number of elections are taking place at the same time, even though certain precautions are needed to minimise the risk of fraud, for example by enabling the voter to check his or her vote immediately after casting it. Clearly, with this kind of voting, it is important to ensure that ballot papers are designed in such a way as to avoid confusion. In order to facilitate verification and a recount of votes in the event of an appeal, it may also be provided that a machine could print votes onto ballot papers; these would be placed in a sealed container where they cannot be viewed. Whatever means used should ensure the confidentiality of voting.*

43. Electronic voting methods must be secure and reliable. They are secure if the system can withstand deliberate attack; they are reliable if they can function on their own, irrespective of any shortcomings in the hardware or software. Furthermore, the elector must be able to obtain confirmation of his or her vote and, if necessary, correct it without the secrecy of the ballot being in any way violated.

[54] Emerging Electronic Voting Standards. https://www.ndi.org/e-voting-guide/emerging-electronic-voting-standards

[55] http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2002)023rev-e

[56] http://www.coe.int/t/dgap/democracy/Activities/Key-Texts/Recommendations/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf

44. Furthermore, the system's transparency must be guaranteed in the sense that it must be possible to check that it is functioning properly."

Conclusion: *For the introduction of the Internet Voting Informational System in Moldova, CEC shall be guided by the art. 21 of the UDHR and the art. 3 of the 2nd Protocol of the ECHR. Moreover, the experience and in particular the constitutional practice of Estonia, provides a precedents of applying the Venice Commission Code of Good Practices on electoral maters and the CoE Council of Ministers Rec Recommendation (2004) 11 on legal, operational and technical standards for e-voting for performing the implementation of the Internet Voting Informational System, including for the promotion of necessary legal amendments in the Electoral Code of the Republic of Moldova.*

3.4. Internet Voting and international commitments on human rights, Open Government objectives and UN Sustainable Development Goals

Human Rights

As described in the previous chapter, the Right to Vote is one of the fundamental human rights as provided by the Universal Declaration of Human Rights, relevant international and European human rights treaties, including the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights, and the European Convention for Human Rights. Consequently, the introduction of the Internet Voting as an alternative voting channel for the national and local elections, as well as for conducting national and local referendums shall provide for an enhanced implementation of the Article 21 of the UNDHR and article 3 of the ECHR II Protocol, allowing a broader civic participation in elections.

The introduction of Internet Voting shall provide for additional opportunities for men and women, in particular for those with mobility disabilities; for citizens residing abroad who are willing to vote, but don't have the possibility because the overseas polling stations are far away from them; for internal migrants, including students; as well as for the Moldovan citizens who are residing in the Transnistrian region.

Open Government Objectives

In addition, as member of the Open Government Partnership[57] since 2012, Republic of Moldova committed to implement the basic Good Governance principles. In this regards, the introduction of Internet Voting would provide for the implementation of the main pillars of the Open Governance in Moldova, ensuring more transparency, accountability, effectiveness, responsiveness to citizens and the public participation in the decision making process and the effective use of innovative information and communication technologies.

Since 2012, Moldovan Government adopted Annual Open Government Action Plans implementing the OGP commitments. So far, the Action Plans have not provided for specific actions that would contribute to the introduction of online public services in the election management system of Moldova. However, indirect actions relevant to the implementation of IT in the election management process were provided.

Recently, the E-Governance Center of the Republic of Moldova, the national coordination authority of open data and online public services, have initiated the process of public consultations on a new Action Plan on Open Government for the years 2016-2018[58]. Thus, as the implementation of open governance principles shall not be limited to the Governmental bodies, it is recommended that relevant actions for the preparation, piloting and introduction of Internet Voting in Moldova should be introduced in the respective Action Plan. This will contribute to the synergy of actions of the Central Electoral Commission and Governmental authorities in the implementation of the piloting of Internet Voting by the regular 2018 national Parliamentary Elections as provided in the law no. 101 on the Concept of SAISE.

[57] http://www.opengovpartnership.org/about/open-government-declaration
[58] http://www.egov.md/ro/communication/news/vino-cu-propuneri-la-planul-de-actiuni-pentru-o-guvernare-deschisa

UN Sustainable Development Goals (2030)

On 25th September 2015, during the UN Sustainable Development Summit, the Agenda for Sustainable Development was adopted, which includes a set of 17 Sustainable Development Goals (SDGs)[59] to end poverty, fight inequality and injustice, and tackle climate change by 2030. Moldova committed as well to implement these goals.

At first glance, one may find difficult to identify the relevance of Internet Voting to the general implementation of SDGs. However, we consider that this alternative voting solution would improve democratic participation and non-discriminatory inclusiveness of Moldovan citizens, in particular of those willing to express their right to vote, but who are not able to. Thus, it will address at least one of the SDGs, namely 16 SDG which aims to promote justice, as well as a peaceful and inclusive society. In our case, a definite impact of the Internet Voting solution will be produced on three objectives of this SDG, in particular, (1) on the development of effective, accountable and transparent institutions at all levels; (2) on the assurance of responsiveness, involvement and representative decision-making at all levels and (3) on the promotion and enforcement of non-discriminatory laws and policies for sustainable development.

3.5. ICT in Election Management

Moldova has relevant experience in using ICT in election management. In May 2008 the Parliament of the Republic of Moldova has passed the Law no. 101 which refers to the conception of the SAISE. The long term objective is to hold fully-automated elections in Moldova. This includes the development of opportunities for citizens to vote in any polling place, to vote through electronic polling terminals and/or to vote through Internet.

At the time of conducting this Study, CEC has been using ICT for voters' lists management through SRV, which is receiving daily data updates from State Register of Population[60]. Thus, every eligible voter in Moldova is on the database of SRV, therefore no person can be on more than one polling station list of voters, and there is no eligible voter who is not on the list of SRV. *Additional updates to the functionality of SRV may be necessary in order to facilitate input of information about the voters who have voted on Internet in advance.*

Every polling station in Moldova is equipped with portable computers and mobile Internet connection that is using VPN network to communicate with the SRV server. Every voter that comes to vote is being registered. This workflow enables to get fast results about election turnout and technically enables voters to vote at any polling station, however, the law does not allow this functionality at the time of this Study. *If Internet Voting would be introduced, the existing infrastructure would enable the voter, who has cast his/her vote on Internet in the period of time reserved to Internet Voting, to instruct the election management body to remove his/her electronic ballot from digital ballot box and allow him/her to vote by paper on Election Day at the polling station.*

N.B. Additional procedural instructions have to be drafted and adopted to facilitate such functionality.

ICT is also widely used in election management to collect and transmit election results and track political campaign finance, but this is out of the scope of this Study.

3.6. Demographic situation

Population of the Republic of Moldova (voters)

According to the recent Data issued by the National Bureau of Statistics[61] the population of the Republic of Moldova by 01.01.2016 amounted to **3,553,100 people**. More than half (i.e. 57,5%),

[59] For more information please access: https://sustainabledevelopment.un.org/

[60] Interview with CEC staff.

[61] http://www.statistica.md/newsview.php?l=en&idc=168&id=5156

2,042,000 people live in rural areas and 1,511,100 citizens live in urban areas (i.e. 42,5%). According to the data published by the Ministry of Information Technology and Communications[62], the owner of the State Register of Population, there are currently over **3,165,000** Moldovan citizens residing or having their domicile in the Republic of Moldova. At the same time, according to the recent data offered by CEC, by 1st April 2016 there were over **3.233.100 citizens with the right to vote registered with the State Register of Voters (SRV)** and **over 2.848.600 citizens who were enlisted as eligible voters** distributed among electoral constituencies.

History of the Election turnout (2001 - 2015)[63]

Over the last 15 years, Republic of Moldova held six Parliamentary Elections, four General Local Elections and one Referendum. For the purpose of the current Study a detailed overview over the recent elections turnout, with a particular focus on elections organized abroad, is presented in the table below:

TYPE OF ELECTION/ YEAR	NUMBER OF ELIGIBLE VOTERS IN MOLDOVA	NUMBER OF VOTERS THAT VOTED IN THE REPUBLIC OF MOLDOVA	ELECTIONS PARTICIPATION RATE	NUMBER OF VOTERS THAT VOTED ABROAD	NUMBER OF POLLING STATIONS OPENED ABROAD
GENERAL LOCAL ELECTIONS 14.06.2015	2814262	1380737	48,63%	---	---
PARLIAMENTARY ELECTIONS 30.11.2014	2800827	1576091	57,28%	**73311**	**95**
GENERAL LOCAL ELECTIONS 05.06.2011	2677103	1475495	54,35%	---	---
PARLIAMENTARY ELECTIONS 28.11.2010	2645488	1668850	63,37%	**64201**	**75**
REFERENDUM 05.09.2010	2662052	798724	30,29%	**19705**	**78**
PARLIAMENTARY ELECTIONS 29.07.2009	2603158	1574213	58,77%	**17544**	**33**
PARLIAMENTARY ELECTIONS 05.04.2009	2586309	1539167	57,54%	**16916**	**33**
GENERAL LOCAL ELECTIONS 03.06.2007	2313571	1257868	54,61%	---	---
PARLIAMENTARY ELECTIONS 06.03.2005	2270668	1566061	64,84%	**10018**	**23**
GENERAL LOCAL ELECTIONS 25.05.2003	2200696	1339470	58,26%	---	---
PARLIAMENTARY ELECTIONS 25.02.2001	2256241	1602899	67,52%	**3804**	**20**

Mapping of Country (Diaspora) Voting

Various numbers are presented when it comes down to the **numbers of Moldovan citizens living abroad**. According to the State Register of Population (SRP) in 2015 over **102,000 are officially registered as residing or living abroad**.

The Bureau for the Relations with Diaspora[64] does not possess official/accurate data on the exact number of Moldovan migrants abroad, due to absence of a national policy for their compulsory registration. However according to the NEXUS studies[65] there are currently approximately **700,000 Moldovan citizens** residing or living abroad. Among them, more than 450.000 are long-term migrants (majority of them are labour migrants); over 100.000 are permanent migrants and over

[62] http://www.mtic.gov.md/en/csir-registru

[63] *Source: Calculations of the authors based on the source provided by CEC*

[64] Interview with Liuba Valcov and Dorin Toma, Bureau for Relations of Diaspora (01.04.2016, Chisinau)

[65] http://nexusnet.md/pic/uploaded/IASCI_CIVIS_Market_Analysis_Driving_Innovation_in_circular_migration.pdf

150.000 of Moldovans abroad are seasonal migrants. Main countries of destination for Moldovan migrants are the Russian Federation (approx. 450.000 Moldovan citizens[66], majority seasonal workers), Italy (over 300.000[67], including over 200.000 legal residents).

The General Directorate for Consular Affairs of the Ministry of Foreign Affairs and European Integration of the Republic of Moldova declared that according to the data collected by the Moldovan Consular Missions abroad, in 2014 there were over **587.000 Moldovan citizens residing abroad (See Annex II).** The following geographical distribution of Moldovan citizens (over 10.000) abroad could be mentioned:

1.	Italy	- 150021
2.	Russia	- 146924
3.	France	- 60000
4.	USA	- 39176
5.	Portugal	- 23000
6.	UK	- 20000
7.	Canada	- 12830
8.	Greece	- 18825
9.	Ukraine	- 17706
10.	Spain	- 16433
11.	Irland	- 15000
12.	Romania	- 11699
13.	Germany	- 11665
14.	Israel	- 11000

At the same time, according to the data of the CEC, during the last Parliamentary Elections (30th November 2014) **73.311[68]** citizens of the Republic of Moldova have participated in elections in a total of 95 polling stations opened abroad, which represents approx. **4,5% out of the total number of voters who participated in elections in 2014, or approx. 2.5% of the total number of eligible voters from the Republic of Moldova**.

If it were to compare the participation rate in the elections abroad, related to the number of Moldovans residing abroad (i.e. the information of the Consular Department of the MFAEI presented above), then one could conclude that the **majority of potential voters are residing in Italy, Russia, France, UK, Canada, USA, Spain, Portugal, Greece, Germany, Belgium, Turkey and Israel (13 countries)**. These countries may be included in the short-list of potential countries to take part in the piloting of the Internet Voting in 2018.

Detailed information about the geographical distribution of voters is presented below:

No.	Country	Polling Stations	Number of voters
1.	Italy	25	27.596
2.	Romania	11	10.454
3.	Russia	5	9.521
4.	France (including Monaco)	5	4.537
5.	UK	3	2.334
6.	USA	6	2.253
7.	Canada	3	2.032
8.	Portugal	5	2.088
9.	Spain	4	1.940
10.	Greece	2	1.735
11.	Germany	2	1.715

[66] http://pda.guvm.mvd.ru/about/activity/stats/Statistics/Svedenija_v_otnoshenii_inostrannih_grazh/item/5850/

[67] https://www.cliclavoro.gov.it/Barometro-Del-Lavoro/Documents/V_Rapporto_annuale_Migranti_2015.pdfmoldo

[68] http://cec.md/index.php?pag=news&id=1548&rid=12866&l=ro

12.	Ireland	1	1.467
13.	Belgium	1	1.163
14.	Turkey	2	932
15.	Israel	2	713
16.	Czech Republic	2	585
17.	Austria	1	407
18.	Switzerland	1	402
19.	Ukraine	2	308
20.	Netherlands	1	203
21.	Poland	1	178
22.	Bulgaria	1	154
23.	Hungary	1	117
24.	Sweden	1	109
25.	Belarus	1	107
26.	Latvia	1	62
27.	Estonia	1	60
28.	Azerbaijan	1	44
29.	Lithuania	1	42
30.	Qatar	1	32
31.	China	1	21
	Total	95	73.311

The estimated number of Moldovans residing abroad is cca. 700.000, whereas the effective number of voters abroad during the last Parliamentary Elections (2014) is 73.311. Consequently, only cca. 10% of voters abroad participated in previous general parliamentary elections.

At the same time, if it were to relate the general voters participation rate at the last Parliamentary Elections (2014) i.e. 57,28% to the total estimate of Moldovans residing abroad cca. 700.000, the number of potential voters abroad should increase from 73.311 to over **400.000 voters**. Thus, over 300.000 potential overseas voters are not able to vote due to the poor network/access to the polling stations abroad and lack of remote (Internet) voting.

The Online Survey of Moldovans living abroad

In this regard, in order to identify a demand for Internet Voting technologies, and better substantiate the figure mentioned above, the authors of this Study have conducted an on-line Survey among the Moldovan Diaspora representatives on the introduction of Internet Voting in Republic of Moldova[69].

The Survey was prepared and disseminated during 6 – 20 April 2016 on Google Forms by the UNDP consultants mainly via the social networks (Facebook and “Odnoklassniki”), with assistance from the Bureau for Relations with the Diaspora, Moldovan Government and UNDP Programme. The survey was addressed to Moldovan citizens living abroad and included 6 questions. In total, 914 answers where submitted to the questions of the Survey.

Key findings of the Survey were the following:

Previous participations at elections while abroad:

- 53% of the respondents indicated that they participated while abroad at the previous Parliamentary Elections.
- 37% indicated that they did not participate at the previous elections because the polling station was too far.
- 6,6% indicated that they did not participate for other reasons
- and only 3,1% of the respondents declared that they did not wish to participate in the elections.

[69] https://docs.google.com/forms/d/17BKhzCgJuOtpSDJQ4nD_0ccT2wXbuAaBtHClj-PZwOE/edit?usp=forms_home

Support for Internet Voting

- 92,8% declared their support to the introduction of Internet Voting, and 96,1% of supporters indicated that they would like to vote over Internet during the next elections.
- Geography of the Survey shows that the respondents who answered to the questions shall not be considered as a mapping of the Moldovans abroad, but rather an indicator of those citizens who are using more often the Internet and social networks.
- Almost 50% (456) indicated that at the moment they are residing in other countries than Italy, Russia, Romania, USA and Canada. Only 7 respondents mentioned that at the time of the Survey they were in Moldova.
- 15,2% (139) indicated that they are in Italy.
- 12,7% (116) in USA.
- 11,1% (101) in Canada.
- 9,5% (87) in Romania.
- and 1,6% (15) of the respondents indicated that they are in Russia

Generally, the majority of the Internet users and consequently of the Internet Voting supporters are aged between 25 and 45 years old (i.e. 71,2% or 651 respondents) and between 18 and 25 years old (i.e. 19,4% or 177). About 11% of the respondents indicated that they are older than 45 years.

The Survey has proved that the current voting system is not adequate for Moldovan citizens living abroad, and there is a sufficient demand for the remote voting solution which would facilitate voting for the expatriates.

The detailed results of the Survey are presented in the Annex I.

3.7. Internet use in Moldova (penetration rate)

According to the official data presented by the Ministry of Information Technology and Communications in 2015, 67% of the households in Moldova do have access to the Internet, 72% of users access the Internet at least once a day[70].

The penetration rate for the Internet service – (land ADSL, fiber) is 14,7% (over 525.000 households). At the same time, according to the recent report of the National Regulatory Agency for Electronic Communication and Information Technology the mobile telephone penetration rate is 121,8% (over 4,3 mln. users), while mobile data penetration rate is over 8,5% (with over 298,400 users)[71].

According to www.Internetlivestats.com there are 1,946.000 Internet users in Moldova, which represent over 50% of the population of the Republic of Moldova[72].

Government E-Services

According to the information provided by the E-Government Center, during the inception mission interviews, there are currently over 90.000 users of electronic signatures per year in Moldova, including over 55.000 users of Mobile signatures (SIM)[73], over 35.000 users of E-key (in particular legal persons and civil servants), over 200 users of E-ID cards.

Conclusion: *Moldova has a high penetration rate of internet and very good mobile coverage. Internet is accessible almost everywhere in the country. Mobile phones and computers can be found in the majority of households, being very popular among individuals.*

[70] http://www.mtic.gov.md/sites/default/files/staticdocuments/accesul_populatiei_la_tic2014.pdf
[71] http://en.anrceti.md/Internet_mobil_BL#fig5
[72] http://www.Internetlivestats.com/Internet-users/moldova/
[73] Moldcell (one of the 3 mobile operators) reported over 21.000 users of M-signatures.

3.8. Political acceptance

A supportive socio-political context significantly helps the introduction of Internet Voting as an alternative voting solution. The Socio-political context is sandwiched between the credible electoral process, which is on top, and the technical-organisational context, which is at the bottom of the Public Pyramid of Trust[74].

Trust in a solution that is technically weak can, however, be misleading. The weaknesses of the operational, technical or legal foundations could surface and may then discredit not only the Internet Voting option, but also possibly the entire electoral process, especially when the political stakes of an election are high. The complete cancellation of Internet Voting from a country's electoral framework may be the consequence, as it has happened in Germany or Netherlands.

Thus, a negative socio-political context creates serious risks, even if the technical and operational foundations of the Internet Voting solution are sound. A challenge in this regard is to make Internet Voting simple and understandable by a non-IT audience. Weak social and political support could hinder the implementation of a trusted Internet Voting Informational System, as political opponents will find reasons to undermine the trust in this advanced voting technology by pointing to some of its inherent weaknesses.

Introduction of new voting mechanisms requires changes in the legislation at the highest level. Therefore, wide and sustained political acceptance is needed. It is an essential must, as later changes in political spectrum of the government may render useless all the efforts and investments that were made. This has already happened in Norway in 2014, after two successful Internet Voting pilots of 2011 and 2013 – the new government has decided to stop trials without any solid reasons. Long-term support from the majority of political parties, distribution of rights and obligations, stable and long-term sources of financing, coordination of inter-office efforts are crucial.

During the mission of assessment of the Study, a series of meetings with Parliamentary political parties were conducted. In particular, meetings with the representatives of the Liberal Party, Liberal Democratic Party of Moldova, Socialists Party of the Republic of Moldova, Communist Party of the Republic of Moldova and Democratic Party of Moldova.

Parliamentary political parties expressed a general support for the introduction of the Internet Voting in Moldova. The main motivation that was mentioned in this regard was the creation of alternative voting solutions for the Moldovans living abroad, the young electorate (the participation rate of the youth in the previous Parliamentary Elections was less than 5%) and for those who usually do not vote in elections due to other agendas during the Sunday Election-Day. However, the majority of the political parties where rather reserved to predict the introduction of the Internet Voting in Moldova in the next 2-4 years, the main reasons in this regard being:

- Low rate of use of E-services by the general public;
- Low trust in the electoral process; concerns about the privacy and security of voting;
- The general perception about possible manipulation of the voting by attacking the Internet Voting Informational System, one of the examples mentioned by all representatives of the political parties was the problematic functioning of the SAISE/SRV during the previous Parliamentary Elections on the Election Day.

At least two representatives of the political parties have voiced challenges for the organisation of the Internet Voting for Moldovans living abroad, the geopolitical political contexts being outlined. A need for a phased approach in the introduction of the Internet Voting was underlined. Finally, all representatives of the political parties have expressed support for the piloting of the Internet Voting during the next ordinary Parliamentary Elections. Some also indicated that a preliminary piloting phase could be considered as well for the Elections of the President scheduled for 30 October 2016.

[74] Introducing Electronic Voting – Essential Considerations, IDEA (2011) http://www.eods.eu/library/IDEA.Introducing-Electronic-Voting-Essential-Considerations.pdf

Conclusion: *Parliamentary political parties expressed a general support for the introduction of the Internet Voting in Moldova. The main motivation that was mentioned in this regard was the creation of alternative voting solutions for the Moldovans living abroad, the young electorate (the participation rate of the youth in the previous Parliamentary Elections was less than 5%) and for those who usually do not vote in elections due to other agendas during the Sunday Election-Day. However, the majority of the political parties where rather reserved to predict the introduction of the Internet Voting in Moldova in the next 2-4 years. At the same time, all representatives of the political parties have expressed support for the piloting of the Internet Voting during the next ordinary Parliamentary Elections. Some also indicated that a preliminary piloting phase could be considered as well for the Elections of the President scheduled for 30 October 2016. A special attention shall be dedicated to the testing and piloting phases. Visibility and popularisation of the Internet Voting was also mentioned as being important.*

4. PROPOSITIONS OF THE STUDY

Moldova has all the basic preconditions for introducing Internet Voting in the near future:

1. Well- developed Internet infrastructure;
2. High degree of mobile network coverage;
3. Good degree of public ICT literacy;
4. Reliable voters list (SRV);
5. All polling stations are equipped with Internet – connected computers, and they are constantly online and communicating with SAISE.

Despite the fact that the absolute number of bearers of digital certificates for personal identification are still low, popularity of Mobile-ID is rising rapidly, and it is expected to continue to grow as more e-services will be offered by the government.

Thus, the authors of this Study present two main propositions:

- To create an official Internet Voting Information System (IVIS);
- To implement the IVIS Pilot version before the general Parliamentary Elections in 2018.

4.1. Internet Voting Information System

Analysis of the legal environment, demographic situation, ICT development, conducted during the assessment mission led to the conclusion to propose that an Internet Voting Information System (*hereinafter - IVIS, or Internet Voting Informational System*) be created under auspices of, owned and managed by the CEC as a Module of the SAISE based on the SRV.

The IVIS shall be used by CEC as an alternative voting channel during the national elections and referendums. The official implementation of the new IVIS module shall be performed after a lighter IVIS version will have been piloted before the next ordinary Parliamentary Elections in 2018.

At the same time, on the basis of IVIS, a separate E-Government Service could be considered in order to further popularise the Internet Voting in Moldova, which could be used for conducting secure and reliable citizen consultations for state and municipal institutions, as well as for political parties, large NGO's, university communities and other bodies, who require qualified, secure, reliable and transparent decision making processes.

4.1.1. Basic principles of Internet Voting Information System

IVIS shall retain all the requirements that are applicable for traditional elections.

The Internet Voting will have to keep all the traditional voting principles especially the secrecy of ballot. Secret ballot principle means that the Internet Voting Informational System must ensure that nobody, not even the system administrator can disclose someone's vote, i.e. disclose the voters' preference. Also, voters shouldn't have the means to demonstrate to someone else their choice of vote. The system shall not require to collect or provide evidence that could reveal the contents of the vote. *Secret* ballot principle does not mean that the voter must vote in an isolated environment.

4.1.2. An alternative method of voting

Internet Voting should be an auxiliary voting method. Normal paper voting ballot on Election Day, voting in diplomatic missions, ships, military units, in-patient medical facilities shall not be impacted.

4.1.3. Advanced voting

Internet Voting shall be conducted in a period prior to traditional paper ballot voting. It is up to a legislator to decide specific time of advanced voting.

Explanatory note: *Before the start of Internet Voting, the encryption key generation procedure needs to be carried out as well as other preparations for the opening of the electronic ballot box. At the end of advanced voting period the electronic ballot, the electronic box has to be closed and physically disconnected from the Internet.*

After the end of Internet Voting period there shall be a reasonable amount of time reserved to transport the information about those who have voted over the Internet to the SRV, to avoid multiple voting. No Internet Voting shall be possible on Election Day, when paper elections are being held. This is also necessary in order to avoid multiple voting.

4.1.4. Remote voting

Internet Voting should be accessible to all eligible voters that have the required technical means to prove their identity online. Eligible voters can cast their vote in any geographic area where Internet connection is available.

4.1.5. Last vote counts

The voter may vote on Internet for an unlimited number of times during the advanced voting period. All the ballots cast are recorded in an electronic ballot box. During the vote counting, only the last vote shall be included in the final tally. Voice cancellation rule must be discussed: IVIS may be configured to cancel a vote or to record a blank vote.

4.1.6. Voters list management

Equal suffrage is one of the key principles of democratic elections. Every voter is entitled to one vote in one election. All votes have equal legal effect[75]. This is in opposition to weighted voting, where vote values can depend on voters' wealth, age or other social status. This also means that the voting system has to be set up in such a way that it would be impossible that a voter's preference should be recorded more than once in one election. This should also be applicable to any electronic voting system, despite its configuration. Therefore, it is important to have a properly maintained list of eligible voters and an effective system to track whether a voter has voted electronically or by paper in his/her respected polling station and the vote is not recorded more than once.

4.1.7. Paper ballot priority

Paper ballot filed at the polling station on Election Day has the highest priority. If the voter has voted on Internet and in advance, his/her vote (votes) cast online have to be deleted from the electronic ballot box prior to vote counting.

4.1.8. Voter authentication

As mentioned herein, the user authentication function may be exercised by various methods, which could be either using digital certificates on voters' media (e.g. mobile signature, national electronic identity (E-ID cards), digital certificates), or using special login credentials which can be delivered to the voter by various means of communication – by post, by SMS, by e-mail or combined.

For the purposes of the Internet Voting in Moldova, it is advised to use several different methods of voter authentication, depending on the location of the voter:

- For the voters who wish to vote on Internet from the territory of the Republic of Moldova, it is compulsory to authenticate himself/herself through MPass service using mobile signature/national electronic identity (E-ID cards)/digital certificates.
- For the voters who wish to vote on Internet from abroad without prior registration, it is also required to use MPass service for authentication.
- For those who wish to vote on Internet from abroad, but do not possess a digital certificate, which could be used to authenticate himself/herself using MPass service, a special login credential delivery system should be setup.

Delivery of login credential for the expatriate citizens of Moldova

In case they do not possess the digital certificate which is accepted by the MPass service, Moldovan expatriate citizens should undergo the following procedure[76]:

[75] ECORM Art. 4.
[76] This method can be limited to certain countries, where postal service is considered to be reliable.

1. During the predefined period the person choosing to vote through Internet from abroad should log into a special registration website (or a dedicated subpage within a CEC website), where they should express their interest in voting through Internet in the particular elections of reference, while also providing their personal contact information: name, surname, personal code, passport number, birth date, valid email address, place of residence, mobile phone number;
2. After the required information is gathered and automatically checked with the SRV, a confirmation email is being sent to the voter's email address;
3. A pair of login passwords will be generated for the voter. First password will be sent in a secured envelope (e.g. like the envelope that is used to send bank PIN codes) to the voter's postal address in his/her country of residence. To avoid illegal organized voting, it is recommended to limit the number of voters that can register to vote from the same address.
4. During the voting over the Internet, the voter should log into the voting website and present his name, surname, personal code, passport number and the first part of the password received by mail. If the entered data matches the data handled by the IVIS, the second part of the password – the string of symbols and numbers - is then being sent to the voter's mobile phone and it should be entered manually by the voter into a special input field of the authentication website. If the second password is also entered correctly, the voter is forwarded to the voting website, where the process continues as if he/she was logged in using MPass service.
5. As an alternative, instead of mailing the password to the voter by post, a One Time Link can be sent to voters' email address. In this case it is desirable that the voter could declare his/her valid email address at the closest embassy/consulate of the Republic of Moldova.

4.2. Requirements for the Internet Voting Information System

The Internet Voting will have to comply with security requirements no weaker than those imposed on the highest level of state registers and state information systems.

The Internet Voting can be declared invalid if there are indications of breach of security in the voting system or the integrity of the electronic ballot box is compromised. The decision to declare Internet Voting invalid shall be made by the CEC, based on the auditors' findings. The decision on the impact on the overall election results shall be carried out.

IVIS can impose specific minimum requirements for hardware and software required to vote online. Such requirements are justified by the need to ensure the security of voting via Internet, but shouldn't be disproportionate as to not limit the availability of Internet Voting.

The following section describes the main requirements for an Internet Voting Information System of Moldova. There are two main components:

1. Functional requirements;
2. Non-Functional requirements.

In short, the following are the main requirements for using an Internet Voting Informational System in an electoral process:

- The IVIS should be trusted by all the stakeholders.
- The IVIS should be designed to be user-friendly.
- The IVIS should be designed to be accessible.
- The IVIS should be designed to be available.
- The IVIS should be designed to be scalable.
- The IVIS should be designed to be flexible.
- The IVIS be able to integrate with the country's existing electoral systems.

4.3. Functional requirements

4.3.1. Pre-election requirements

Pre-election information management

- The system must allow the implementation of any election process according to the Electoral Code of Republic of Moldova;
- The system must be able to automate the import of any election information extracted from the SAISE;
- The system must protect the integrity and authenticity of the election information used to configure the voting platform.

Voters list

- The system must be able to automate the import of information from the State Register of Voters;
- It is recommended that the system allow the use of various authentication methods for authenticating the voters when accessing the voting platform;
- The system must use voter's digital certificate and/or digital signature for protecting the votes before being cast;
- The system must provide a process for providing voters with digital certificates for casting their votes, which does not require voters to manually install digital certificates or smartcards in their voting terminals;
- It is desirable that the system include a process to help election managers to generate digital certificates in a secure manner, in the cases where public-key infrastructure is not available.

Role of the Central Election Commission

- The security of the overall voting process must be under the full control of the Central Electoral Commission;
- The system must allow the secure configuration in a way that a threshold of members is required to carry out the decryption and final tally/tabulation of votes, thus preventing a single member acting on his/her own;
- The system must require the presence of the CEC to certify any change on the election configuration;
- Any election information must be certified by the Central Electoral Commission by means of non-repudiation practices (e.g., digital signatures).

Pre-election audit procedures

- The election information used by the voting platform during the voting and counting process must be auditable in order to detect any manipulation attempt. Election information is understood as any information in electronic format that is used by the voting platform or independent auditors to verify the correct configuration of the election. That includes the contents of the electoral roll, the ballot templates, the election identification, the Central Electoral Commission members, etc.;
- Furthermore, the different software components of the voting platform must also be certified to detect any attempt of tampering. This must facilitate independent auditors and voters to check if the components used are the same as the ones audited;
- The system must check that the election information is certified by the CEC before starting the voting and counting processes;
- The system must allow the independent auditor(s) to check if the election information used by the voting platform has been properly certified by the CEC;
- It is recommended that the system check the integrity of the election configuration and that this configuration allow the correct operation of the system;
- Independent auditors must be able to audit and certify the application components used for

voting;

- Voters must be able to check the integrity and authenticity of any voting component executed in their voting terminal before using it (e.g., verification of the digital signature of a voting application);
- Any independent auditor must be able to certify the integrity and authenticity of the system components installed in the voting platform;
- Any action performed by an independent auditor must neither affect the voter's privacy nor the election's integrity.

4.3.2. Voting process requirements

Accessing the voting platform

- The access to the voting platform must not be restricted to a unique operating system and/or browser. All popular Operating Systems and browsers shall be supported;
- It is not recommended that Voters be required to manually install any specific election software or hardware on their voting terminals to access the voting process, with the exception of typical software used to access and work with the Internet i.e. Internet browser, Java/JavaScript, smartcard reader driver;
- Voters shall not be restricted to always use the same voting terminal to access the voting platform;
- Voters must be able to verify the authenticity of the voting platform that they are accessing;
- Voters must be able to allow the voting platform to perform compatibility and security requirement compliance tests on their hardware.

Identification and authentication of the voter

- The system must allow integration with all existing voter authentication mechanisms (MPass and others);
- The system must use voter digital certificates for digitally signed votes to be cast;
- The system must allow removing voters before and during the voting process (e.g. the voter's authentication mechanism has been compromised and it has to be blocked). If the removed voter has already cast a ballot, his vote must be tagged as invalid and ignored in the final tally.

Presentation of voting options

- The voting option must appear in a clear and understandable format, without being codified or requiring the use of a code book to reveal the real value of the options;
- Voters must be able to clearly distinguish between the different voting options;
- Voting options must support the use of all official languages used in Moldova.

Selection and confirmation of voting options

- The system should prevent and warn voters if they make involuntary errors that could invalidate their vote;
- The system should clearly distinguish the selected voting options from the non-selected ones;
- The system must allow voters to cast blank ballots, if allowed by the Electoral Code;
- It is to be decided if the system should allow voters to cast invalid ballots after having been warned and to requiring an explanation;
- The system must allow voters to verify their voting options before casting their vote;
- The system must provide the voter with the option of modifying his/her vote before casting it.

Casting the vote

- The system must protect the privacy and integrity of the cast vote, along with the voter's identity by cryptographic means (e.g., encryption and digital signature), which ensure that the vote cannot be falsified during its transportation or storage;

- The system must allow voters to cryptographically protect their votes on their voting terminal before casting it, instead of protecting the votes in the voting server;
- The cast votes must be protected against both external and internal attacks (e.g. system administrators);
- The system must use an adequate cryptographic voting scheme to protect the cast votes;
- The system must provide means for verifying that the contents of the protected (encrypted) vote can be recovered in the tallying stage.

Vote verifiability

- The system must provide voters with cast-as-intended functionality to allow them to individually check that the protected (encrypted) votes contain exactly the same selections that they made;
- The system must provide voters with recorded-as-cast functionality (e.g., voting receipt) to allow them to verify during the voting process that their cast votes are present (if accepted) in the ballot box stored by the voting server;
- The system must allow voters to verify using counted-as-cast functionality that their votes were received by the Central Electoral Commission at the end of the election, and therefore included in the final tally;
- Voters must be able to verify the authenticity of the voting server, any application executed in their voting terminals and any receipt generated to enable the verification of the results;
- If applicable, the system must allow voters to prove, beyond any doubt, that their vote was present during the final count;
- Any voter verification method must not facilitate coercion or vote buying practices;
- The voting server must be able to verify that protected (encrypted) cast votes contain valid voting options without unprotecting (decrypting) any cast votes. In the case that a received vote contains an invalid voting option, the system must reject that vote and notify the voter to vote again;
- The system must prevent all reattempts to attack the cast votes. This includes any attacks based on re-encryption.

Election monitoring

- The voting system must guarantee that the monitoring tools cannot compromise the voter's privacy and the election's accuracy.
- The voting system must provide monitoring tools that ensure the detection of any anomalies during the voting process.
- The voting system must provide monitoring tools that ensure that an anomalous log can be isolated from the rest of the logs without invalidating the whole set of log data.
- The system must ensure that the monitoring tools are tamper proof and guarantee non-repudiation of the recorded audit information.
- The voting system should provide monitoring tools that ensure the detection of any change of the certified system and application components installed on the voting platform.
- It is recommended that the voting system could provide monitoring tools based on system and application logs without requiring access to the voting platform components.
- It is recommended that the voting system could provide monitoring tools with an alert system that analyses system and application logs based on security threat patterns, allowing the analysis and investigation of possible incidents.

4.3.3. Counting and publication of results

Closing the voting process

- The system must automatically close the election at the time specified by the Central Electoral Commission during the election setup;
- Voters must not be allowed to access the system and cast their votes once the voting process has closed;
- The system should give voters who are in the process of casting their vote extra time to finish the process;
- The system must prevent internal or external attackers (including persons with privileged access rights to the system) from adding votes from voters that have not participated;
- The system must protect the integrity and authenticity of the digital ballot box (containing all the votes cast by the voters) after the voting process has been closed (e.g., digitally signing the ballot box);
- The system must require special privileges to perform specific actions like the export of the Ballot Box or the export of other election information.

Election Results collection

- The system must transfer the ballot boxes from the different voting servers to an isolated environment, where the votes are counted, without the use of a network connection;
- The authenticity and integrity of the collected ballot boxes must be verified before accepting them;
- The consolidation system must be able to check that all votes have been cast by eligible voters before being decrypted and counted;
- The ballot boxes must contain all the votes cast during the election process (i.e., if multiple Internet Voting is required, all the votes cast by the voters must be included in the collected ballot box);
- The consolidation process must allow collecting multiple ballot boxes from multiple channels i.e. Internet, meaning the electronic ballot boxes;
- In the case that multiple Internet Voting is required, the consolidation process must allow the selection of just one vote per voter to be counted, following the electoral rules established to define the vote with higher priority (I.e, the vote on paper ballot);
- The consolidation system shall never delete or destroy invalid or discarded votes, and must keep them in a separate location for any audit.

Decryption and tallying of the Ballot Boxes

- The decryption and tallying process must be carried out in an isolated environment;
- The decryption and tallying process can only be started by the CEC members;
- The decryption and tallying process must verify that all the votes contained in the ballot boxes are cast by eligible voters;
- The decryption and tallying process must prevent that multiple votes from the same voter are decrypted;
- The decryption and tallying process must ensure that it is impossible to correlate the order of the decrypted votes with the order they were cast and therefore, prevent any link between the decrypted votes and the voters (e.g., by using a Mixing process);
- The CEC must certify the list of decrypted votes (e.g. digitally sign it);
- The decryption and tallying process must guarantee that it is impossible to correlate any voter verification information (e.g., voting receipts) with the voting options selected within the ballot;
- The decryption and tallying processes must provide cryptographic proofs that the votes have not been manipulated during these processes. The cryptographic proofs should be universally verifiable by any authorized third party without compromising any sensitive

information (such as private cryptographic keys) which allows the correlation between the decrypted votes and the voters;

- The decryption process must provide cryptographic proofs that ensure that the decrypted votes' contents have not been manipulated by the decryption process, without disclosing any link between the decrypted votes and any voter.

Certifying and publishing the results

- The system must generate the results from the certified list of decrypted votes;
- The system must publish the results with the information that allows the voter to verify his/her vote was present in the counting process, without disclosing the contents of his/her vote;
- The system must be able to generate different election reports (e.g., turnout reports, preliminary results, results by electoral division).

Auditing the counting process

- The system must allow independent auditors to carry out parallel recounts from the certified list of decrypted votes.
- The system must allow independent auditors to check and certify the integrity and authenticity of the system components used for processing the ballot boxes.
- The system must allow independent auditors to verify in a public and transparent way, any cryptographic proofs generated by the decryption/counting process. This includes ensuring that decrypted votes have not been manipulated during this process, and that the contents of the decrypted votes are equal to the contents of the encrypted votes, without compromising voter privacy.
- The system must allow independent auditors to verify in a public and transparent way that the contents of each decrypted vote are equal to the contents of each encrypted vote, without compromising voter privacy.

4.3.4. Verification of the results

Verification of the results by the voter

- The system must generate a voting receipt that allows voters to verify that their vote reached the Central Electoral Commission and was present during the decryption and tallying process;
- This voting receipt must allow voters to file a valid claim in the case that they detect that their vote was not processed.

Independent audit of the Election

- The system must facilitate an exhaustive audit of the system by trusted third party auditors based on the stored election information and logs, allowing an analysis and investigation of possible incidents;
- The system must allow a full audit without compromising the election's integrity and voter's privacy;
- Auditors must be able to check the integrity and authenticity of the election information and logs to detect any manipulation attempt of such audit information;
- The system must allow auditors to verify that the decryption process behaved properly without having the private cryptographic keys used in the process (e.g. by means of zero knowledge proofs).

4.4. Non-functional requirements

4.4.1. Security

End-to-end security

- The system must protect the votes (e.g., encryption) on the voters' terminal before being sent to the voting server;

- The system must guarantee that only the Central Electoral Commission can decrypt the votes, after the election, ideally in an isolated environment (e.g., without being connected to any communication network);
- The system must be end-to-end verifiable, providing cryptographic proofs that ensure, beyond any doubt, the correctness of the operations executed by the voting platform components and the voting client (i.e., must provide cast-as-intended and counted-as-cast verifiability);
- The system shall not trust the vote casting device used by voters (i.e. zero trust vote casting device).

Voters' privacy

- The system must guarantee that votes are encrypted in a way that only the Central Electoral Commission can decrypt them;
- The system must guarantee that the key required to decrypt the votes is not available (i.e. does not exist) during the voting process until the Central Electoral Commission retrieves/reconstructs it;
- The system must guarantee that at least a pre-defined majority of Central Electoral Commission members are required in order to retrieve the election decryption key;
- The system must guarantee that it is impossible to correlate the order in which the votes were decrypted with the order in which they were cast;
- The system must guarantee that two different votes with exactly the same contents have different encryption formats;
- Any audit process supported by the system to verify the accuracy of the election must not compromise voters' privacy.

Voter's eligibility

- The system must guarantee that only eligible voters can access to the voting platform.
- Before accepting a cast vote, the system must verify the identity of the voter who cast the vote;
- The system must prevent a voter from casting more votes than the ones permitted (i.e. avoid double voting);
- The system must allow verifying, at any time during the election, that the Internet votes within the ballot box belong to the voter (receipts of the digital confirmation of the internet vote and an authenticated access to the IVIS website);
- The system must guarantee the non-repudiation of the cast votes;
- The system must not have any knowledge of the voters' credential required to protect the non-repudiation of the vote;
- The system must prevent the addition of bogus ballots in the ballot box from both external users and system administrators;
- The system must use unique digital certificates for authenticating voters;
- The system must use unique voter digital certificates for digitally signing the cast votes.

Secrecy of the Vote

- The system must guarantee that a cast ballot is secret in front of any third party, including system administrators and potential hackers that break through the conventional security measures protecting the voting platform;
- Votes must be encrypted on the voter's terminal before being cast;
- The system must prevent the decryption of the ballots before the election is closed to avoid leaking information on partial results;
- Any audit process supported by the system to verify the accuracy of the election must not compromise the vote's secrecy.

Integrity of the Vote

- The system must preserve during the whole electoral process the integrity of each individual cast vote;
- The system must allow checking the integrity of each individual vote stored in the ballot box;
- The vote's integrity is protected by the voter when casting his/her vote;
- The system must prevent any attempt to add blank ballots into the digital ballot box;
- Voters use their own digital certificates for protecting their votes by means of digital signatures.

Ballot Box accuracy

- The system must allow checking the integrity and the identity of the service that has managed the ballot box, before starting the decrypting and tallying process.
- The system must prevent the addition of blank votes from both external users and system administrators;
- The system, for audit purposes, must allow to accurately trace the processes that concluded with the casting and storage of a vote in a ballot box;
- The system must implement adequate measures for detecting any attempt to delete a vote from the ballot box;
- The system may have components segregated in different services, in such a way that each service checks the correct operation of the others, in order to guarantee the integrity of the Ballot Box and other election data;
- The system must publish information about the contents of the ballot box during and after the voting process to allow voters to check the presence of their votes in the ballot box, in an anonymous way.

Central Electoral Commission Role

- The system uses an N of M threshold scheme of Central Electoral Commission members for retrieving the key that allows the decryption of the votes;
- It must be impossible for an individual member or a number of members below the threshold, to retrieve the election decryption key;
- The system must support the use of tamper proof devices (e.g., PIN protected smartcards) for storing the information required by each Central Electoral Commission member in order to retrieve the election decryption key;
- The threshold scheme is based on secret sharing or similar scheme77;
- The decryption key never exists until it is reconstructed by the CEC members at the end of the election.

Verifiability of the voter

- The system must allow voters to verify if his/her vote was present during the decryption and tallying process, by means of a voting receipt;
- The voting receipt must preserve the vote's secrecy (i.e., the selected voting options should never be able to be deduced);
- The voting receipt verification process must allow the detection of manipulated or bogus receipts to prevent fraudulent claims by voters;
- The system must allow voters to verify if their votes are present in the ballot box after being cast;
- The system must allow voters to verify that their selections were stored in the system as intended (e.g., by means of return codes);

[77] http://www.christophedavid.org/w/c/w.php/Calculators/ShamirSecretSharing

- The system must provide a cast-as-intended verification method independent from the voting client software (e.g., using alternative channels).

Prevention of coercion and vote selling

- The system must generate cryptographic verification proofs (e.g. voting receipts) that do not allow voters to prove who they had voted for to a third party;
- The system must prevent anybody, even privileged managers or auditors, from correlating votes with voters;
- The process that breaks the correlation of votes with voters should be universally verifiable, generating cryptographic proofs that do not manipulate the results and without having to compromise the private cryptographic keys used in the process (e.g. by means of zero knowledge proofs [In cryptography, a zero-knowledge proof or zero-knowledge protocol is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true, without conveying any information apart from the fact that the statement is indeed true);
- Cryptographic proofs generated by the system to allow voters to verify that their selections were stored in the system as intended, shall never facilitate voter coercion or vote selling practices. Additional measures, such as multiple voting, may be put in place in order to prevent this.

Independent auditability

- The system must allow auditors to retrace any election processes, in a meaningful manner, without compromising the election privacy or accuracy;
- The system logs and election information generated during the election must allow a meaningful audit of the election without requiring that auditors have access to any private keys, or assuming the role of any privileged actor;
- The system must implement adequate cryptographic practices for verifying the accuracy and integrity of the log information to be used during the audit;
- The system must allow any independent auditor to check and certify the integrity of the application components at any time during the election;
- It is recommended that the voting system provide monitoring tools that ensure the detection of any changes of the certified system and application components installed on the voting platform;
- It is recommended that the voting system provide monitoring tools based on system and application logs without requiring access to the voting platform components;
- It is recommended that the voting system provide an alert system using system and application logs based on the analysis of security threat patterns, allowing the analysis and investigation of possible incidents;
- It is recommended that the voting system provide monitoring tools that allow checking the integrity of the system components against a baseline fingerprint;
- The decryption and tallying processes must provide cryptographic proofs that the votes have not been manipulated during these processes. The cryptographic proofs should be verifiable by any authorized third party without compromising any sensitive information, which would allow the correlation between the decrypted votes and the voters.

Service availability

- The system must be scalable without having to stop the service;
- The system must be fault tolerant;
- The system must implement practices that mitigate the implementation of denial of service attacks.

4.4.2. Usability and accessibility

Usability

- The system should provide a user-friendly voter interface, so that the voting process is intuitive and no previous training for using this voting channel is necessary;
- The voter should not be required to install any specific digital certificate on their vote casting device;
- The system must support the use of the main Internet browsers and operating systems;
- The system must include easy-to-understand instructions for voters;
- The system must warn voters if, during the voting process, they make a selection that could invalidate their vote (e.g., under voting, over voting, etc.);
- Voters must select their voting options by directly selecting the candidate instead of using a code or an indirect selection method.

Accessibility

- The system must support the use of multiple languages without compromising the voter's privacy;
- The system must be compliant with WGAI accessibility standards78.

4.4.3. Scalability and flexibility

- The system must allow the addition of new components without having to stop the service.
- The system should be able to run elections for thousands to millions of voters in an easy and cost-efficient way.
- The system must support all the characteristics of the corresponding country's electoral process.
- The system must be customizable in several features, such as look and feel, language, help and information pages, etc. following the electoral authorities' requirements.
- The system must support several mechanisms for authenticating voters. These mechanisms should be able to work in parallel, so that the participation rate can be maximized.
- System management tools must be customizable to tailor the electoral authorities' requirements, such as the capability to access the participation rate in real time, to audit the system, or to cancel/revoke certain votes following the agreed procedures.

4.4.4. Standards compliant

Election standards

- The system must support the requirements of the Electoral Code of Moldova and the associated regulations;
- The system must be compliant with the Council of Europe election standards;
- The system must be compliant with the Election Markup Language (EML)79.

Cryptographic standards

- Any cryptographic algorithm used in the system must be based on open standards.

4.4.5. Source code of the software

There are mixed views on open-sourcing the software due to the advantages and disadvantages of doing so. On the one hand if the code is open source then it gives any would-be hacker full knowledge of how the software works, which might allow them to construct malware specific to that voting

[78] https://www.w3.org/standards/webdesign/accessibility
[79] http://docs.oasis-open.org/election/eml/v7.0/eml-v7.0.html

system. On the other hand making the code open source means it can be reviewed by a wide audience and give voters greater re-assurance that the software is fit to purpose.

Sharing the source code of the election software is a good way to raise the awareness and trust and understanding of educated (IT-literate) people for the respective election software. However it is not a guarantee that the software is secure and prone to any errors. It just makes it easier for third parties to detect. Generally open source is a democratic idea so it should be inherent to elections to be run with as much open source software as possible. But it is also clear that maybe not everything can be provided openly[80].

Others consider it as a good practice to publish code with a license restricting its use to code inspection or testing, providing transparency to the Internet Voting process. It is worth understanding that code publication does not provide a guarantee of the security of the system. In the case that only a few reviewers participate, it may be difficult to find any weakness without a systematised methodology and organisation for the code review. There are many examples of systems whose code has been publicly available for years, before any weakness has been found such as in OpenSSL. For this reason it is more important for a voting system to be end-to-end verifiable rather than open source. With end-to-end verifiability the verification of the election integrity is independent of the software as it’s based on a mathematical proof. Due to this property of Software Independence, should an attacker exploit any bug in the system, the end-to-end verifiability properties will allow detection of the attack - thus preventing this from compromising the integrity of the election.

It is widely accepted that publishing source code does not ensure that software contains no bugs. In addition to this, if a bug is detected, there is no surety that the finder will not maliciously exploit it.

Finally, publishing the source code does not guarantee that the same source code is used in the real system. This leads to a requirement for additional audit measures to be implemented that will demand direct access to the voting system by additional staff, adding further risks of malicious access.

Whilst source code publishing does provide transparency it falls short in providing other security attributes such as being mathematically provable or ensuring that the source code is the same as that used in an election. It is recommended to focus on demanding end-to-end verifiability, as it is a more reliable way to audit and gain confidence in the system.

4.5. Internet Voting Pilot 2018

Prior to official implementation of the IVIS for voting in politically binding elections, a pilot of a fully functional version of IVIS shall be performed before the Parliamentary Elections in Moldova in 2018 (hereinafter IVIS Pilot).

During the assessment mission of this Study, security was one of the most common concerns among interviewed respondents. Can an Internet Voting Informational System be attacked?; can manipulation of the results take place? To answer these questions, one first needs a working Internet Voting Informational System to measure and evaluate upon. For that purpose, we propose to develop a fully functional Internet Voting Informational System and put it under a series of tests, including actual voting, but without legal consequences, i.e. to conduct a pilot Internet Voting and perform technical, operational and functional audit of the Internet Voting Informational System.

Therefore, it is proposed that a fully functional IVIS shall be presented to the general public as well as experts and auditors to test before its actual use in legally binding political elections. Thus, the IVIS Pilot would have some limitations and/or restrictions, if relevant legislation would not be changed by the time of conduction the Pilot:

1. Participation in the IVIS Pilot should be limited only to those voters who possess the digital certificates which could be used for personal authentication using MPass service;
2. The voting results would have no legal effect; Instead, the results of the Pilot shall be used for evaluation purposes, to identify weak points in the system and fix them, if any;

[80] Krimmer R. A guide to secure #onlinevoting in elections. // Webroots democracy. Page 56.

3. The list of candidates may not be the same as in actual elections.

However, the IVIS Pilot should have all the functional, operational and security features as if it was used for legally binding elections:

1. Only eligible voters could vote;
2. The ballot is encrypted on voters' device, signed with voters' digital signature (or special dedicated certificate);
3. The voter could vote multiple times and only the last vote would be included in the final tally;
4. The voter could receive a confirmation that his/her vote was cast-as-intended;
5. The voter could perform a recorded-as-cast verification;
6. The auditors and independent observers could perform a universal verification and counted-as-recorded verification;
7. The source code of the Pilot software shall be available for review and testing to every auditor under condition that all detected flaws would be reported to the management body first, prior to publication of such information.

Elaborated plan of the execution of the IVIS Pilot is described in the Section 5.2" Roadmap for conducting an IVIS Pilot in 2018" of this Study.

4.6. Cost-benefit analysis of the introduction of Internet Voting Information System

As the scope of this Study requires presentation of cost-benefit analysis of the introduction of Internet Voting, it is important to stress that this is a relatively complex task which depends on a number of hard-to-predict factors.

Democratic election and referendum processes are essential in modern democracy, and therefore they cannot be valuated as business cases. However, some estimation can be made based on the experience of other countries:

Main direct benefits of introducing the Internet Voting:

- Increased voters' participation;
- Better voting accessibility;
- Reduced number of errors in elections;
- Increased election transparency.

It is a common belief that the participation rate directly correlates with the legitimacy of the government elected. Thus, increased election participation is a value by itself. There is no reliable data which could indicate how introduction of Internet Voting is affecting election turnout, but it is obvious, that there is a potential of growth of participation through introduction of a new voting channel.

Universal suffrage is one of the main principles of any democratic election. However, this principle is only applicable in full extent for those who are able to come to the polling station and make their choices in private. Those who have movement difficulties or those who cannot express their will without external help are subjected to certain limitations of their voting rights. Therefore, Internet Voting is a good solution that can help people with disabilities to exercise their political rights better. This benefit could not be measured in hard currency.

Usually, election observation is limited to physical observation of one individual polling station per observer. If a political party, NGO or international organization organizes election observation, country-wide election observation becomes a very complex and costly task in terms of money, time and human resources. Introduction of the Internet Voting with all necessary transparency features makes elections observation an easy task. Counted-as-recorded verifiability and universal verifiability enables trained observers and independent auditors to check the integrity of the entire online election process without deploying a large amount of observers.

Traditional observation methods are limited to physical presence of the observer at the polling place during voting and ballot counting processes. The quality of the observations largely depends on the skills, patience and attention of the individual observers. Moreover, the only instrument available is a right to request to recount of the ballots or a right to submit a formal protest about other violations of electoral procedures. It is practically impossible to detect such things as carousel voting. On the other hand, the Internet Voting Informational System allows checking the integrity of election process from the very start to the very end. Modern election technologies enable both EMB's and elections observers and auditors to check if the election data was modified without compromising the secrecy of the data itself.

Some indirect benefits of Internet Voting can be indicated:

1. Increased demand and use of e-government services;
2. Improved public trust in digital services;
3. Improvement of country's' international image.

For the time of this Study, the level of use of government e-services in Moldova is very low, in comparison to other European countries, despite Moldova's good position in the Internet penetration and mobile coverage rates. Introduction of Internet Voting may increase public trust in e-services.

Since the first attempts to introduce Internet Voting around the world at the beginning of the 21st century, only Estonia is currently using Internet Voting for national Parliamentary Election and other nation – wide elections. Other countries are using Internet Voting on local (municipal) or regional level. Introduction of Internet Voting in Moldova could have a huge positive international impact on the image of the country as the second country in the world and the first country outside the EU to introduce remote Internet Voting on a national level.

4.6.1. Potential costs of implementation of Internet Voting

As Internet Voting solutions are not off-the-shelf products, it is very hard to predict the actual cost of the system at this stage of the Study. The cost of building such system depends on a wide variety of factors, which include:

1. Voting protocol selected;
2. Hardware required;
3. Software licenses and custom development costs;
4. Complexity of the solution, necessary integration with existing information systems;
5. Voter authentication methods;
6. Personnel training, etc.

To identify the actual potential costs of such system, a separate Request for a Quotation shall be sent out to all the major vendors worldwide. Depending on the features, complexity, level of security, project management and logistics involved, the project could cost from 400 000 up to 2 000 000 Euros.

4.6.2. Potential cost savings analysis

Another aspect of cost-benefit analysis of this Study is potential long-term savings in election management, if participation rate of Internet voters reaches significant levels. The idea behind this analysis is that if the number of Internet voters increase, the number of traditional voters would decrease, assuming the overall turnout remains the same. In this case, the demand of polling places in the areas with high population density (e.g. capitol city) would decrease, therefore less human resources and premises would be required, and in consequence logistic expenses would be reduced. The following analysis explains the logics behind this thesis:

Initial data

Number of eligible voters – 2,800,827

Voters that have participated in the last election (within Moldova) – 1,576,091

Number or polling stations opened in Moldova – 2,073

Total elections participation rate - 57,28%

Number of eligible voters in Chisinau – 618,842

Number of voters participated in election in Chisinau – 464,296

Number of polling stations in Chisinau – 309

Polling stations abroad - 95

Estimate number of eligible voters abroad – 700.000 persons

Potential number of voters abroad who would have liked to participate in elections, but where not able due to the long distance to the polling station or other objective reasons – cca. 400.000 persons

Actual number of voters abroad – 73,311 (2014)

Elections abroad participation rate (2014):

2,5% out of the total number of eligible voters from the Republic of Moldova (=73,31*100/2,800,827)

4,5% out of the total number of voters who participated in elections in 2014 (=73,31*100/1,576,091)

Participation rate of the voters abroad who participated in elections related to the total number of potential voters abroad – cca. 10% (=700,000/73,311)

Total Budget[81] spent for the Parliamentary Elections (30 October 2014) - 35,287,300 MDL – approx. 1,781,287 EUR**[82]**:

1. Budget spent by CEC – 7,939,500 MDL – 400,782 EUR
2. Budget spent by the District Electoral Councils and the Precinct Electoral Bureaus – 27,347,800 – 1,380,504 EUR
3. Estimate Budget of elections abroad: 868,015 EUR

Cost-benefit analysis for voters abroad

Average cost per polling station (in Moldova): cca. 666 EUR per polling station (=1,781,287/2,073)

Estimate cost per polling station abroad[83] - cca. 9,137 EUR per polling station abroad (=868,015/95)

Total cost of the vote: cca. 1,17 EUR per Vote (=1,781,287/1,576,091)

Estimate cost of vote abroad: 11,8 EUR per Vote abroad (=868,015/73,311)

- If participation rate of the vote abroad would increase to 140.000 or cca. 20% of the estimated number of Moldovans abroad the cost per vote abroad would be: cca. 6,2 EUR/Vote (=868,015/140,000)
- If participation rate of the vote abroad would increase to 210.000 or cca. 30% of the estimated number of Moldovans abroad the cost per vote abroad would be: cca. 4,1 EUR/vote (=868,015/210,000)
- If participation rate of the vote abroad would increase to 280.000 or cca. 40% of the estimated number of Moldovans abroad the cost per vote abroad would be: cca. 3,1 EUR/vote (=868,015/280,000)
- If participation rate of the vote abroad would increase to 350.000 or cca. 50% of the estimated number of Moldovans abroad the cost per vote abroad would be: cca. 2,4 EUR/vote (=868,015/350,000)
- If participation rate of the vote abroad would increase to 410.000 or cca. 58 % (average participation rate in elections in Moldova) of the estimated number of Moldovans abroad the cost per vote abroad would be: cca. 2,11 EUR/vote (=868,015/410,000)

[81] CEC Report of activity (2015), http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=358313

[82] 1 EUR – 19.81 MDL (NBM exchange rate october 2014)

[83] Average to organize elections abroad in one country is 28.000 EUR. Elections organized in 31 countries abroad in 95 polling stations=Cost 9137 EUR/polling stationhttp://www.e-democracy.md/files/votarea-peste-hotare-2010.pdf

Cost-benefit analysis for Chisinau

Presuming the fact that distance to the polling station is not an issue in Chisinau and assuming that the voters could easily travel extra within the capital city, the following calculations can be made:

Cost of election management in Chisinau = 309 x 666 EUR = 205 794 EUR per elections.

If participation rate via Internet would be **20%**, we can expect savings in election management by 40 000 EUR. If participation rate via Internet would be **30%**, we can expect savings in election management by 60 000 EUR.

Conclusions on cost benefit-analysis

The Introduction of Internet Voting:

1. Would increase participation among Moldovan citizens living abroad;
2. Would reduce the "cost per voter" rate for voters living abroad;
3. Could reduce the number of required polling stations in largely populated areas;
4. Would increase accessibility to vote among people with disabilities and those with limited mobility;
5. May give positive effects in terms of public trust in the public sector and government e-services;
6. May raise worldwide knowledge of the Republic of Moldova as a modern and technologically mature state.

4.7. Internet Voting – related risk management

Implementation of Internet Voting Informational System may inevitably encounter a series of risks and threats, which should be mitigated accordingly. The risks may rise in all stages of implementation: planning, installation and operation. The risk mitigation/management policies shall be applied as the ones applicable to other high-level state information systems.

Together with other common risks, such as Denial-of-Service attacks, human error factors, lack of common security measures, Internet Voting has a special set of risks and related countermeasures, which we shall present in this section.

4.7.1. Would it be possible to break voter's secrecy?

No! Files, which contain voters' choice (digital ballots) shall be encrypted on the voters' device using advanced asymmetric cryptography techniques before being digitally signed by voters' certificate. The digital ballot contains only the information about voters' preference, but not about the voters' identity. The encrypted digital ballot is subsequently signed by the special digital certificate, issued by the IVIS, thus creating a "digital double envelope", which is sent to the Internet Voting server (Digital Ballot Box).

Because of the fact that the private election key, which is needed to decrypt the votes, is inaccessible during the voting period, it is technically impossible to decrypt the contents of the digital ballot while they are stored in the Digital Ballot Box. This requirement shall be fulfilled by ensuring the following:

1. The pair of keys needed for ballot encryption and decryption is performed in an isolated environment;
2. The private key is disassembled using secret sharing schemes and put away so is it inaccessible until the designated time;
3. The public key is transported to the Internet Voting Informational System so it can be used for encrypting the votes.

After the elections, the Digital Ballot Box is being prepared for ballot counting:

1. All multiple votes cast by the voters have to be discarded, except the last one;
2. If the voter has voted on the Election Day at the polling station, all his/her votes have to be removed from the Digital Ballot Box.

Afterwards, all the “digital double envelopes” in the Digital Ballot Box are first anonymized, i.e. the digital signatures, attached to the encrypted ballots, are removed. Then all anonymized ballots have to be transferred to the Mixing server, where they have to undergo a procedure, similar to shaking a paper ballot box, meaning that no correlation between a ballot and the voter is left. Anonymizing and mixing shall be conducted in such a way that the integrity of the votes is preserved.

Only after proper anonymizing and mixing, encrypted votes can be transferred to the decryption server. The decryption procedure is conducted in the isolated environment, where a private election key is reconstructed by a qualified majority of the members of Central Electoral Commission.

Therefore, there is no moment in the entire process, where it is possible to deduce the voter’s identity.

4.7.2. Is it possible to manipulate election results when using Internet Voting?

No! As the ballot shall be filled and encrypted on the voters’ device (terminal) and then digitally signed using digital certificate, issued by the IVIS, any change to the contents of the digital ballot during transmission would be immediately detected, as the integrity of “Digital Double Envelope” would be breached.

When the Digital Double Envelope reached the Digital Ballot Box: (1) a series of one-way mathematical operations has to be performed to generate a unique Return Code, which says nothing about the contents of the vote nor the voter, nor the time of casting the vote; (2) the Return Code is then digitally signed by the digital signature of the IVIS and sent back to the voter, thus the voter can check the validity of the Return Code; (3) the corresponding record has to be made to the Log Journal of the Internet Voting server in such a way that any breach of the integrity of the data in the Digital Ballot Box cannot remain undetected.

Any potential outside interference with the Digital Ballot Box should trigger an alarm in the Internet Voting Informational System.

When a voter receives the Return Code, there shall be a service which provides the voter with tools to check if his/her Return Code is valid, i.e. a ballot is present in the Digital Ballot Box. If the same voter, during the same election, votes again for the same candidate (party), the Internet Voting Informational System should return the same Return Code. Therefore, the voter is sure that his/her vote is recorded – as – cast.

The same principles as described herein apply to check if only valid votes are being transferred to the Mixing Server, and, subsequently, if only votes cast by eligible voters were properly decrypted and counted.

Therefore, verifiability measures ensure that any interference with the Internet Voting Informational System will not remain undetected.

4.7.3. Is it possible to install malware into the voter’s device which could show to the voter that his/her vote corresponds to his/her choice, but the actual vote is different?

Every voter before voting over the Internet has to be explicitly warned to make sure he/she is using virus/malware free computer. For that, the voter has to use a legally obtained and updated operating system and other software and have a proper anti-virus installed.

Besides that, after voting for a party of his/her choice, the voter can repeat the voting procedure from a different computer. If the Return Codes would not match, this would mean that at least one of the computers is compromised.

The same applies to the software, hardware and procedures of the Internet Voting Informational System itself to avoid even the smallest security risks as ones described in the *Security Analysis of the Estonian Internet Voting Informational System*[84] by J. Alex Halderman.

[84] https://jhalderm.com/pub/papers/ivoting-ccs14.pdf

As with the issue of the voting secrecy, described herein, the voter himself/herself bears responsibility of the security of his/her internet communication device. However, the Internet Voting Informational System shall provide the voter with all necessary tools to assist him/her to check the security of the device on which the voter is planning to make his or her vote.

4.7.4. Would it be easier to buy votes if voters will be able to vote online from their homes or work?

Vote buying is a criminal offence in all countries, including Moldova. Most of the opponents of Internet Voting are indicating vote buying as a potential threat to democracy as it would make easier for potential political criminals to apply pressure to the voters to vote over the internet in a way necessary to the coercer. It would be irresponsible and naïve to deny the existence of such threat, which seems obvious, but, on the other hand, successful cases of Internet Voting in the world do not show any signs of increased vote buying.

Multiple voting when only last vote counts, as described herein, is considered an effective measure against vote buying or other peer pressure. A voter can vote as many times as he/she desires during the advanced voting period. If the voter feels that his/her voting secrecy or privacy was compromised or illegally affected, he/she can re-vote whenever comfortable during the advanced voting period.

As mentioned previously, every cast vote generates a Return Code. In case of multiple voting, all Return Codes have to be valid during the entire life cycle of the Internet Voting Informational System. Since all the Return Codes are valid, the coercer is unable to verify, if the vote cast under pressure is the last one, i.e., the one that is counter. Moreover, the voter shall be able to denounce the fact that his/her voting secrecy or privacy was compromised, so all ballots cast in his/her name can be removed.

The voter should also be able to override his/her vote cast by Internet, by arriving at the polling station on the Election Day. In this case, his/her Internet vote(s) should be removed from the Digital Ballot Box before the voter is allowed to vote by paper ballot.

Vote buying or other kinds of peer-pressure is not directly related to Internet Voting, although this risk can be mitigated by allowing multiple voting with only the last vote counting.

5. PRELIMINARY ROADMAP FOR INTRODUCING INTERNET VOTING INFORMATION SYSTEM (IVIS)

In this section of the Study we present the preliminary Implementation Roadmap. Following the methodology set at the beginning of this Study, the Roadmap will include the Plan of Actions together with the four quarters of the Readiness Matrix: legal, technical, social and political aspects.

5.1. Roadmap for the official implementation of IVIS in Elections

First, a long-standing political decision shall be made via broad political acceptance of all major political parties. This is essential because the introduction of Internet Voting will inevitably lead to significant expenses in terms of funds, time and human labour. And the return of this investment is a long-term one.

1. Amendments to the Electoral Code

The following amendments to the Electoral Code shall be made:

- A series of new concepts shall be introduced: *advanced voting*, *Internet Voting*, *multiple voting*, and other;
- A new section of Electoral Code shall be drafted and approved. This section could be called “Internet Voting”. It should set forth the main principles and procedures of Internet Voting;
- Configuration of Internet Voting: advanced voting period (e.g. number of days, start and end hours, etc.), whether Internet Voting Electoral Council shall be introduced, number of members of the CEC needed to re-construct the private election key;
- Voter authentication rules shall be described in details. In particular, the remote registration/authentication protocol for those voters without digital IDs;
- Provisions regarding observation and auditing shall be included;
- Legal grounds for declaring Internet Voting as invalid.

Subsequent decisions of the CEC shall be drafted.

2. Amendments to the Law on Personal Data Protection

The procedure of voters’ registration with consequential delivery of login credentials as described in the Section 2.5 of this Study, may be in contradiction to the provisions of the Law on Personal Data Protection, in particular, with the provisions that require the voter to give his or her written consent.

3. Internet Voting Information System

The Internet Voting Information System shall be set up. A Steering Committee should be established to coordinate preparation, establishment, piloting and official implementation of IVIS. This Committee shall be comprised of the members of the CEC, CEC Secretariat, Ministry of Information Technology and Communications, State Enterprise „Center for Special Telecommunications” (CTS), State Enterprise “Registru”, international development partners (ex. UNDP), and other relevant bodies.

The Steering Committee should approve a Plan of Actions, which should include:

1. To coordinate the preparation of the Terms of Reference, procurement, test, pilot and implementation of the IVIS;
2. To endorse the draft amendments to the legal framework in order to prepare the full scale implementation of the IVIS;
3. To endorse the Draft CEC decision on Establishment, Piloting and Implementation of the IVIS;
4. To draft The Statute of the IVIS, technical regulation documents, IVIS security regulation documents;
5. To draft the technical documentation.

The Plan of Actions shall be harmonized with the Plan of Actions of the IVIS Pilot (described herein).

4. *Public Procurement*

After necessary preparations are being done and the necessary legislation is in place, the international tender shall be announced for purchasing the required software and hardware. The public procurement procedure can take up to 6 months' time, taking into account the complexity of the project.

The terms set forth in the Request for Proposal shall not exceed 6 months for delivery. The service provider shall deliver reliable and efficient software, which complies with all modern requirements of an Internet Voting Informational System described herein. The Internet Voting solution must be compatible with all existing methods of authentication of the voter, as well as those, which will be created for the purpose of this project. The service provider shall also deliver training of the election management personnel, provide necessary means for the informational campaign for the voters, provide operational and warranty support for the designated period. A separate public tender shall be executed to purchase consultancy and audit services, both for overseeing the project implementation and conducting the audit of the result delivered by the provider of Internet Voting technology.

5. *Preliminary timetable of the official IVIS Implementation Roadmap*

The following timetable explains the roles of various stakeholders in the first 12 months of the Implementation Roadmap.

Institution	Time (months)											
	1	2	3	4	5	6	7	8	9	10	11	12
CEC	Prepare draft legislation							Approve subsequent CEC decisions		Start of the implementation of the Project		
Parliament				Initiate and approve amendments to the Electoral Code and Law on Personal Data Protection								
Government								Approve subsequent government decisions				
Steering committee	Support the drafting of the required legislation, coordinate the actions,											

5.2. Roadmap for conducting an IVIS Pilot in 2018

The non-binding IVIS Pilot shall be conducted prior to the Parliament Elections in 2018. The elections may be organised at the earliest in October-November 2018, thus, the Pilot shall be conducted at least one month before the Election Day (i.e. in September, 2018).

The IVIS Pilot should offer all technical, operational and security features, as if it were used for legally binding elections, except the legal validity of the results is not checked. This is an important requirement both to test the security and reliability of the Internet Voting Informational System, and to gather valuable feedback from experts and general society.

The time needed to prepare the IVIS Pilot should not be less than 18 months; therefore the decision to initiate the Pilot shall be made no later than the III quarter of 2016.

1. *Legal framework*

The Pilot voting shall be conducted using the legal grounds of the Provisions of Law No. 101. Hence this is a non-binding Pilot, no changes to the Electoral Code are necessary at this stage.

The Plan of Actions of the Pilot voting shall be approved by the CEC to outline all necessary steps to prepare and conduct the Pilot. The Plan of Actions shall include the following components:

- General description of the Pilot;
- The task to set up a Steering Committee;
- General description of Technical Specifications for the Pilot;
- Assignment to the respective authorities and officers to prepare the necessary legal documents;
- Timetable of the Pilot.

2. *Steering Committee*

A Steering Committee mentioned in p. 5.1 will ensure the implementation of the Pilot IVIS. The task of the Committee shall be the coordination of the implementation of the Plan of Actions.

The CEC shall develop on the basis of the IVIS functional requirements proposed above in the Study a ToR for the development of the IVIS Pilot module as part of the SAISE. These requirements shall be made in compliance with the main functional and operational principles set forth in the General Description of the Pilot.

3. *Organizational aspects*

A new SAISE module shall be added for the purposes of the Pilot. The technical, operational and security documents shall be drafted for the purposes of the Pilot. These documents must comply with the requirements set forth in the General description of the Pilot. Experts from the CEC, MITC, and academic society as well as international experts with necessary qualification an expertise shall part in drafting these documents.

4. *Funding of the Pilot*

The investment plan has to be outlined to allocate required funding for the Pilot. The investment Plan has to provide information on potential sources of funding: whether it's national budget, international donors', public-private partnership or combined.

Depending on the size and complexity of the IVIS Pilot, it could cost around 200 000 – 500 000 EUR.

5. *Public procurement*

With the Technical Specifications ready, a public procurement can be performed in order to purchase the necessary hardware and software to conduct the Pilot. Public procurement can take up to 6 months' time, taking into account the complexity of the project.

The terms set forth in the Request for Proposal shall not exceed 6 months for delivery.

Separate public tender shall be executed to purchase consultancy and audit services, both for overseeing the project implementation and conducting the audit of the result delivered by the provider of Internet Voting technology.

6. *Public Relations and social awareness*

Elections are a very sensitive topic in the society. Every change in the electoral system is expected to receive a lot of attention from the society and political groups. Therefore, it is very important to be well prepared to inform the society about the proposed changes and to have well prepared answers and explanations for common questions and concerns. Thus, the following actions are suggested:

- CEC, eventually with help from a selected/contracted public relations agency, shall prepare and conduct a Public Relations Plan to reach necessary awareness level among general public.
- A dedicated website has to be created with a direct link from a CEC main webpage, where all relevant information about the Pilot is to be published. A special friendly logo has to be created for the purposes of the Pilot.
- A series of educational videos shall be prepared and made available on social networks to explain what the Internet Voting is, how it works and what its benefits are. Also, the common myths have to be explained.
- Printed educational materials have to be prepared with detailed explanation about the Pilot.

- A series of round table discussions have to be aired on national television, where members of the CEC, The Steering Committee, political parties, and non-governmental organizations could present and discuss the conduction and the benefits of the Pilot.
- Lottery may be organized in order to increase participation. Mobile phones, tablets or laptops can be offered at such lottery.

7. Conducting of the Pilot

With the Steering Committee, Plan of Actions and Public Relations Plan in place, the conduction of the IVIS Pilot project can proceed.

For a successful implementation of the Pilot, it is advised to select a group of volunteers with various social backgrounds. The group of Volunteers shall be comprised of 500-1000 persons, representing both residents of Moldova and Moldovan citizens living abroad (in particular aiming at eventually up to 10 top countries of residence of Moldovan voters living abroad[85]).

The selected volunteers should receive special training, so that they not only participate in the Pilot, but also participate in fine-tuning the functionality of the Pilot, as well as providing feedback about the conduction of the Pilot. These volunteers shall be provided with digital certificates at the expense of the CEC, so that they can reliably identify themselves online.

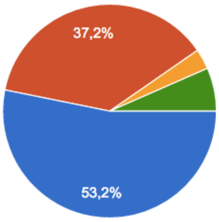
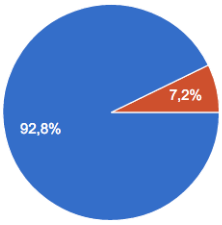
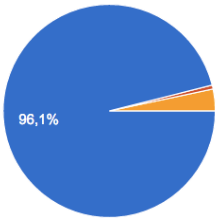
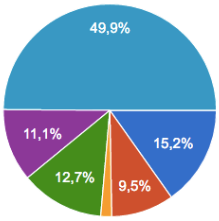
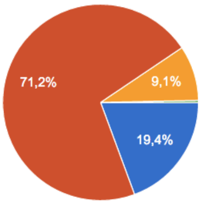
8. Feedback collection

After the completion of the IVIS Pilot, feedback from the participants shall be collected and a Report shall be created and presented to the Steering Committee of the IVIS, so that any knowledge gained during the Pilot can be used in the official implementation of IVIS.

[85] Italy, Russia, France, Canada, Portugal, Spain, Israel, Greece, UK, USA

6. ANNEXES

6.1. Annex I. Detailed report of the Expatriate Survey

Questionnaire for expatriates	Total 914 answers	Graphics
Do you vote in national elections in Moldova, while living abroad? Yes No, because my polling station is too far away No, because I don't want to vote Other	**912 Answers** 485 339 28 60	
Do you support the introduction of Internet Voting in Moldova? Yes (skip to q3) No (skip to q4)	**914 Answers** 848 66	
If Internet Voting would be introduced, would you use it for voting in national elections in Moldova? Yes No Maybe	**846 Answers** 813 5 28	
Which country do you currently live in? Italy Romania Russian Federation United States of America Canada Other (France, Spain, Portugal, Israel, etc.)	**914 Answers** 139 87 15 116 101 456	
What is your age? 18-25 26-45 46-65 66+	**914 Answers** 177 651 83 3	

6.2. Annex II. Information by the General Directorate for Consular Affairs of the MFAEI of the Republic of Moldova[86]

n/o	Country	Number of citizens
1	Austria	1682
2	Azerbaidjan	35
3	Belgium	1299
4	Luxemburg	49
5	Belarus	3465
6	Bulgaria	3372
7	Bosnia and Herzegovina	64
8	FYROM Macedonia	11
9	Albania	21
10	**Canada**	**12830**
11	Czech Republic	5415
12	China	100
13	**Germany**	**11665**
14	Danmark	260
15	Swizerland	650
16	**Greece**	**18825**
17	Estonia	128
18	Egypt	65
19	**France**	**60000**
20	**Italy**	**150021**
21	**Israel**	**11000**
22	Latvia	255
23	Lithuania	670
24	Lebanon	825
25	Poland	876
26	**Portugal**	**23000**
27	**Romania**	**11699**
28	**Russia**	**146924**
29	Qatar	70
30	Oman	6
31	**UK**	**20000**
32	**Irland**	**15000**
33	Turkey	5538
34	Holand	170
35	**Spain**	**16433**
36	**USA**	**39176**
37	Sweeden	273
38	Slovakia	88
39	Slovenia	299
40	Croatia	37
41	**Ukraine**	**17706**
42	Hungary	238
43	Finland	136
44	Norway	256
	TOTAL	**587.632**

[86] The information is collected by the Moldovan Consular Mission abroad.

6.3. Annex III. List of the interviewed persons during the Study

The experts have met the following subjects:

- Mr. Iurie Ciocan, Chairman of the CEC;
- Mr. Iurie Turcanu, Executive Director, E-Government Center;
- Key Experts from the Special Telecommunications Center;
- Mr. Ștefan Creangă, Chairman of the Standing Committee for budget, economy and finance, Parliament RM;
- Ms. Violeta Agrici, Head of General Directorate Consular Affairs, MFAEI;
- Mr. Vladimir Cebotari, Minister of Justice;
- Officials from CEC Elections Management Division, Legal division and IT department;
- Mr. Vitalie Tarlev, Deputy Minister, Ministry of Information Technologies and Communications and REGISTRU;
- Ms. Liuba Valcov and Dorin Toma, Senior officials of the Bureau for Relations with Diaspora, Government of Moldova;
- Mr. Alexandru Tănase, Chairman of the Constitutional Court;
- Mr. Pavel Postică, Programme Director „Promo-LEX";
- Ms. Irina Strajescu, Head of Communication Department, Moldcell;
- Ms. Maria Postoico, Member of Communist Party of the Republic of Moldova;
- Mrs. Raisa Apolschii, Chairwoman of the Standing Legal Committee for appointments and immunities, Parliament RM;
- Mr. Mihai Ghimpu, Chairman of the Liberal Party of Moldova, and members of the LP parliamentary fraction;
- Ms. Ion Cosuleanu, E-Voting expert;
- Mr. Simion Rerzioglo, Migration and Development Coordinator, IOM Moldova;
- Ms. Liliana Palihovici, Vice-Speaker of the Parliament, member of Liberal Democratic Party of Moldova;
- Ms. Sergiu Sîrbu, member of the Democratic Party of Moldova;
- Mr. Vasile Bolea, member of the Socialists Party of Moldova;
- Mr. Sergiu Panaghiu, Word Bank office in Moldova;
- Mr. Nicolae Lungu, Head of the Legal Department of the National Center for Data Protection.