Analytical survey

Modern programs of developing eGovernment

Sergiy V. Martynenko, Ph.D. in physico-mathematical degree.

Annotation

This article sheds light on modern programs of developing e-government in EC aimed at e-government rearrangement in Ukraine. It gives information on the most important developing directions, namely such EC programs as: “e-Passport”, “e-Customs”, and “e-Voting”. Question on providing security information of e-government development in these programs are examined.

1. Introduction

Results of the European Council in Lisbon (March 2000) established a new strategic aim for European Community: within the decade to make economics the most competitive, dynamic and intellectual that will be able to support economic growth with better and bigger working places, and higher social unity. Having this as an aim, EC considers necessary to develop the programs of “e-Customs” (EC Resolution of 05.12.2003 “On creating a simple and paperless environment for customs and trade”, 2003/C 305/01).

Electronic Passport program may be considered as an independent program, which is required by International Civil Aviation Organisation and is approved by EC Council Resolution №2252/2004 of 13.12.2004. At the same time this program can also be considered as a part of some other programs because it can provide with the means of the person electronic identification that may be used by other programs.

“E-voting» program is proceeding by developed E-government program. E-government program proposes public serves, but Internet gives abilities to wide the citizens’ participation in management via electronic voting, that shown the integral indicator of e-government development, as a pointer of E-Democracy level. E-Democracy programs wants to take the second priority in the area of electronic public serves to citizens.

All programs, which we considered before, are the parts of unique “E-government” program. They use the same resources, standards, and data ets. Particularly, “Electronic custom” program has to use technical base realization of “E-government”, provides compatibility (occasion to make data exchange) with any State institutions (administrations) or agencies, involving in movement of goods limiting by each states.

2. Program of e-Passport

2.1. The basis of program

ICAO (International Civil Aviation Organisation)starts to define the specifications and worldwide Standards for machine readable Passports projects in 1968.It means that electronic passports have biometric attributes of owners (photo, finger-prints, and so on).

The implementation of the ICAO Standard is designed to “minimize delays in border crossing formalities and to safeguard international civil aviation operation against acts of unlawful interference,” according to Dr. Assad Kotaite, President of the Council of ICAO.

On July 11, 2005, ICAO formally adopted the machine readable passport specifications, developed collaboratively by it and the International Standards Organization (ISO), as the worldwide standard for Passports. The formal adoption also embraces the specifications governing issuance of the new high security, biometric-enabled version of the standardized Passport or "ePassport" as it has become known. In adopting the specifications as the worldwide standard, all 188 member countries of ICAO have agreed to issue their passports including the new ePassport version in conformance with the Standard by no later than April 1, 2010 – although several more immediate deadlines will result in over 40 countries implementing the ePassport before the end of October 2006.

Including:

-The European Union has mandated that all 25 member states have fully-compliant ePassports containing a facial biometric in place by the end of September ,2006(this plan has not been realized yet)

- The United States is in the process of testing ePassports for its citizens and expects to begin issuing them in 2006.

Known as the “ICAO Blueprint”, the ePassport specifications mandate:

1. Face as the primary, mandatory biometric; with iris or fingerprint as optional, secondary biometrics.
2. A contactless, integrated circuit chip incorporated into the ePassport as the storage medium;
3. A globally interoperable logical data structure for programming the chip; and
4. A modified public key infrastructure (PKI) scheme to secure the data recorded in the chip.

Department Homeland Security demands to citizens’ passports in countries that have rights without visa entry on territory of America:

- since 26June, 2005 citizens from these countries, which have arrived to the USA, must show machine-readable travel document;

-since 26 October 2006 travel document must consist of owner digiphoto, microchip that saves biometric information from corresponding passport page in the memory and other biometric information.

It was the 7th seminar of the international Porvoo Group, which was established in conjunction with the EU eEurope project, in Iceland. Around 80 representatives from 18 European countries, Japan and USA as well as representatives from the European Commission and the United Nations 2005 discussed the situation with regard to interoperable European electronic identity and electronic services and the development projects in participating countries, as well as to exchange information about ongoing projects.

Particularly, there formed three major electronic identity policy objectives:

- general wide spread usage of PKI (Public Key Infrastructure) certificates;
- an open and standardised market providing certificates and related services ;
- full benefits of EU- and international standards, thus aiming for interoperability with administrations of other countries.

According to standards of European Community and confirmed by Council Decision (Council Regulation (EC) on standards for security features and biometrics in passports and travel documents issued by Member States, Official Journal L 385, 29/12/2004 P. 0001 – 0006.)

2.2. Condition of e-passport program in EC

According to demands of European Commission, Directorate-General Justice, Freedom and Security the facial recognition in ePassports becomes mandatory by August 2006.

England. There are plenty of initiatives in the electronic identity field particularly around driver licensing. Plans for national ID cards were delayed because of the recent general election, but a bill to introduce them is expected to become law at the end of 2005, with implementation during 2008–2009. The ID cards will be based on passports, and biometrics will remain a key component.

Belgium. In Belgium, after a pilot project, electronic ID cards were introduced to the population as a whole beginning in September 2004. The intention is to replace the current paper cards with electronic ones by the end of 2009 – carrying an ID card is obligatory. A Public Key Infrastructure, i.e., PKI-supported signing mechanism, is present for e-transaction services.

Belgium is the first country worldwide to complete its roll out of ICAO-compliant electronic passports (ePassports). Since January 30, 2005 all new passports issued contain contactless chip technology. In total, 150,000 ePassports have been produced.

Belgian Passport receiving “the world’s most secure passport” award from Interpol in 2003. The latest development includes an online website www.diplomatie.be/passweb on which the status of a Belgian passport can be verified. This website is linked to a centralized electronic database of stolen and lost passports that is accessible by every authority or even private person. All consultations of these files are properly logged. Belgium has a very severe privacy legislation. Moreover, every citizen can see online who looked into his or her file, and if need be file a complaint. The responsible CA organisation is Certipost, a semi-private organisation.

Estonia. Estonia has used electronic ID cards since 2002, and carrying an ID card is obligatory. The national ID cards are issued by the Citizenship and Migration Board. Over 100 services can be used with this card. A second chip containing biometrics, facial image and fingerprint, complying with the ICAO (the International Civil Aviation Organisation) recommendations, will be added to the card. . The Estonian UES initiative is currently being examined by Belgium and Finland.

Iceland. In Iceland the aim is to issue the first biometric passports in October 2005. The certificate policy of the Government of Iceland is based on the European standard ETSI TS 102 042, and the Danish OCES certificate policy

Italy. In March 2005, Italy approved a national law according to which it will become mandatory to issue citizens an identity card only in the electronic version, when citizens apply, beginning on January 1st, 2006. The usage of biometrics (one fingerprint, along with the bearer’s photo) in the cards is envisioned. The ultimate objective of the Italian government in introducing electronic identity is to safeguard the rights of citizens; the privacy of citizens'.In 2005 Italy agreed national law, according to which is obligatory to make electronic version of identity card. Citizens will use them since January 1, 2006. Provided the usage of biometrics (one fingerprint with photo of owner) and that is the highest task of Italian government about entering of electronic identity card – protection of citizens; data confidentiality of citizens.

Lithuania. Lithuania is currently preparing the introduction of new, non-biometric passports prepared the entry of new non-biometrics passport (produced 1mln.passports).

Poland. Poland has put a hold on biometric travel documents until 2007 due to funding problems.

The Netherlands from February 2005 a six-month ePassport trial took place in six Dutch municipalities, where in total 14,700 ePassports were issued. Issuance of the new passport will start in the autumn of 2006.

Germany
Of the various card projects that the Federal Government is responsible for, currently the main priority is the ePassport. Roll-out of the ICAO-based ePassport with facial recognition is intended to begin in November 2005. Additionally, the German Federal Government launched an eCard initiative some months ago. The goal of this initiative is the definition and implementation of a common platform for all upcoming smart cards in Germany, including those that Federal Government ministries will be responsible for (e.g. health patient card, civil servant cards, job card, upcoming electronic ID card) and private offerings in the field of banking cards, with respect to the signed "e-signature alliance". The upcoming electronic ID card is intended to be introduced in 2007. The intended usage of the eCard will be both private and public, mostly for access to eGovernment services.

Norway. From 1975 the banks in Norway have established joint systems for bank identification cards. Net-banking has become very popular, and the banks are developing a common inter-bank electronic identity system.

Slovakia. The Slovak government has announced plans to start issuing biometric passports by 1 September 2006.

Finland. The issuance of electronic ID cards was begun in 1999. The card contains a citizen certificate issued by the Population Register Centre, which is at the moment the only issuer of quality certificates in Finland. The ID card is not obligatory Electronic signature is already in use. There are over 50 services that use the card, including the Tax Administration, insurance companies, the Social Insurance Institution, Electronic Forms Finland service and The Finnish Defence Forces. The list of services is available at www.etu-klubi.fi.

For mutual recognition of electronic ID cards, Finland entered into a cooperation agreement with Estonia in 2003. The introduction of the biometric ID cards is envisioned in Finland during 2007–2008. In Finland the Ministry of the Interior is in charge of the Biometrics project. The aim is to start the issuance of ePassports in spring 2006.

France. The objective of the French administration remains the convergence with the German specifications to enable a degree of interoperability for both platforms, which constitute the basis of the future standard for the European Citizen Card. A decision is to be made concerning whether or not the electronic ID cards will be mandatory in France or remain optional as they are today. Electronic signature is already in use in France for some applications, but is not yet implemented on a large scale or for electronic identity purposes.

Sweden. The goal of the government is to give the citizens 24-hour-a-day, 7-day-a-week "one-stop-e-services" with the use of a standardised electronic identity. The infrastructure can also be used by private companies. At the moment, the responsible

CA organisations are Swedish banks and the telecommunications operator TeliaSonera. E-passport is not obligatory.

Examples of electronic services which are presently accessible to holders based on acceptance of electronic identity include Swedish Tax Agency services, calculation of a person's retirement pension, registration of a new address, permission to start a lorry, taxi or other vehicle corporation, renewal of bank loans, and a large number of local government electronic services. The Swedish Farmers Supply and Crop Marketing Association will also use electronic identity for contracts between the farmers and the association.In October 2005 the police will begin issuing a national electronic ID card, which will be both an official ID document and a Sweden passport.

3. E-Customs programme

EC normative documents about the building system of **eCustoms** are;

- decision (№ 253/2003/EC) of the European Parliament and of the Council of 11February 2003 adopting an action programme for customs in the Community (Customs 2007);

- EC Council Resolution about creation a simple and paperless environment for Customs and Trade of 5 December 2003 (2003/C 305/01);

- Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee a simple and paperless environment for Customs and Trade of 24.07.2003, COM(2003) 452 final, 2003/0167 (COD);

- Project "Draft e-Customs vision statement and multi-annual strategic plan" of European Commission TAXDU/477/2004 of 20.10.2004;

- Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee and Regional Committee e-government role for European future 26.9.2003, COM(2003) 567 final.

The matter of e-Customs programme is in EC Resolution of Committee from 5 December 2003, particularly: "globalization and liberalization of trade, the increased volume of trade and the growth of e-commerce and wide usage of information technology thrown down new challenges to Customs administration.So Customs administration have to operate in the most effective and friendly e-services for providing European competitiveness".

According to e-Custom project from 20.10.2004 the Commission and the Member States will aim at achieving by 2008 that tasks;

- electronic data exchange between customs offices is possible throughout the Community where required for any customs procedure or any other purpose (e.g. pre-arrival declaration);

- an importer can lodge his summary and/ or customs declaration in electronic form from his premises, irrespective of the Member State in which the goods are entering into the Community;

- an exporter can lodge his export declaration in electronic form form from his premises, irrespective of the Member State from which the goods are leaving the Community;

- the collection and the repayment/ remission of import duties will, in principles, be handled by the customs office responsible for the place where the importer/ exporter is established and keeps his customs records;

- selects of goods for customs controls at border and inland customs offices is based on risk analysis using international, Community and national criteria, the Community criteria being electronically exchanged between the Member States;

- Authorized Economic Operators (AEO), including customs agents, can, at their request, operate throughout the Community on the basis of a single authorization granted according to Community- wide established criteria; this includes the use of facilitations, a common reference for operators and common quality standards, as well as the existence of a common AEO database accessible by customs offices throughout the Community;

- traders have access to an information portal and a single electronic access point for import and export transactions, irrespective of the Member State in which the transaction starts or ends, and even if the transaction involves agencies other than customs (single window, one-stop-shops).

The multi-annual strategic plane on e-Customs has been broken down for State Members in the following categories (by years).

1. Legal changes and simplification **(2003-2007)**;
2. Operation convergence **(2003-2005)**;
3. Computerization of customs processes (**2004-2009)**.

EC "Electronic custom" plan program includes the creation of projects computerize systems for State Members (by years):

- Automated Export System (AES) **(2003-2007);**
- Automated Import System (AIS) **(2004-2009);**
- Exchange of risk information **(2004-2007)**;
- AEO database(s) (2005-2009).

Within the range of each state need to do;

-interoperability between customs administrations and other administrations or agencies involved in customs transactions within the same MS **(2004-2007)**

Working stages of ES common system:

- common customs information portal for trades (2004-2010);
- single electronic access point for transactions **(2004-2010).**

Concerning to technical realization of program marked documents need the following:

- Communication from the Commission COM (2003) 452 (p.4.1.8.*Electronic signature, electronic documents, electronic archiving*) noted that the use of information technology poses the crucial problem of the authenticity and soundless of data exchanged which exchanged and saved by electronic way. By using electronic signatures it is possible to authenticate the person signing an electronic document.

- Member States who have not yet implemented Directive 1999/93/EC on electronic signature should proceed with the implementation and so on. That's why Member States should be a specific provision in the Community Customs Code explicitly recognizing the legal value of an electronic signature and document for customs purposes, independently from the state of implementation in the different Member States; but to guarantee the compatibility of electronic signature usage.

- according to EC Resolution of 05.12.2003 "On creating a simple and paperless environment for customs and trade", (2003/C 305/01), need to "to examine in corporation with Commission, common decisions that let the certification and commendation of digital signature, independently of State Member, in which is based economic operator".

- technical basic realization of "E-Custom" program is the exception of EC State Members obligations regarding to e-Europe, particular E-Government.

The realization of eCustoms program in EC, though pilot project of Export Control System, was started in 2003, in which to take participation 12 from 25 State Members (Belgium, German, Italy, Spain, Sweden, United Kingdom, Czech Republic, Denmark, Portugal, the Netherlands, Australia, Poland).

4. eVoting program

4.1. Program basis

The Parliamentary Assembly of EC is lighted selective questions, particular many reports of the Venice Commission Europe Council – "European Commission for Democracy through Law - Venice Commission"that was devoted to the problems of e-enabled voting (e-mail and electronic votings) according to the Standards Committee. This report was agreed by the Council of 12-13 March 2004.

Some countries have already used e-voting or are preparing to do this, underlining the advantages that e-voting is represented. Commission warmed about the necessity to use special security procedures for minimising the risk of fraud.

Commission has determined 5 principles that reflecting base of European democracy and are suitable for voting companies and referendums:

- *Universal voting right:* all human beings have the right to vote and to support any candidate on the elections (on certain conditions e.g. age and nationality).
- *Equal voting right:* each voter has the same number of votes.
- *Freedom of voting right*: voter has the right to form and to express own wishes in any form, without any compulsion or authority.
- *Secrecy of voting right:* voter has the right to choose secretly the candidate and to protect own opinion.
- *Direct voting right:* the choice (balloting) that has done the voter determined the electee face.

As a result of this, Commission recommended the following:

- E-voting may be used if the system secure/protected (can withstand planned/deliberate attack) and reliable (can function on their own, irrespective of any shortcomings in the hardware, software, supplies and so on.
- E-voting system must be clear, in other words to give the abilities for checking its functioning. This system also must be open, in the view of methods and decisions which are used.
- Electors must be able to obtain confirmation of their votes and correct them, when want to do this, respecting secret suffrage.
- In order to facilitate 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.
- Commission concluded that the observance of pointed conditions, electronic voting compatible with "the Code of Good Practice in Electoral Matters" 2002 European Commission for Democracy through Law - Venice Commission.

Consequently, the acceptability of e-voting systems are determined by legal, procedural and technical standards that are taken part in voting process and provided marking demands.

4.2. E-voting security

For providing e-voting security system was developed standards - VSS (Voluntary Voting Systems Standards) in the USA. These standards were developed specifically

for computer-assisted punchcard, optical scan, and DRE (direct-recording electronic) voting systems. They include a chapter on security (volume 1, section 6), which was substantially expanded in the updated version (Federal Election Commission, Voting Systems Performance *and Test Standards, 30 April 2002* http://www.fec.gov/pages/vssfinal/vss.html).

Along with standards, a voluntary testing and certification program was developed and administered though the National Association State Election Directors (NASED).In this program, an independent test authority (ITA, Independent Test Authority) chosen by NASED tests voting system and certifies those that comply with the VSS. Testing is done of both hardware and software, and the tested software and related documentation is kept in escrow by the ITA.If questions arise about whether the software used in an election has been tampered with, that code can be compared to the escrowed version that saves.

HAVA (Help America Vote Act 2002) creates a new mechanism for the development of voluntary voting system standards. It creates the Election Assistance Commission (EAC) to replace the FEC's Office (Federal Election Commission) of Election Administration and establishes three bodies under the EAC. (EAC was created in 1990):

- 110-member Standards Board consisting of state and local election officials;
- 37-member Board of Advisors representing relevant government agencies and associations and fields of science and technology;
- 15-member Technical Guidelines Development Committee chaired by the Director of National Institute of Standards and Technology (NIST).

This last committee is charged with making recommendations for voluntary standards (called guidelines in the Act HAVA), to be reviewed by the two boards and the EAC.

HAVA also requires the EAC to provide for testing, certification, and decertification of voting system and for NIST to be involved in the selection and monitoring of testing laboratories. The EAC is also required to perform a study of issues and challenges – including the potential for fraud – associated with electronic voting.

4.3. E-voting experience

Kazakhstan

The first step was in September, 2000. According to president degree was been created State Governmental working group that consist of 18 people and want to insert variations and additions to the legislation. In 2003 was planned to finance e-voting in budget.

In 2004 was bought equipment on 3000 districts and was conducted the trainings of operators. In April 2004 was accepted the changes to the law about elections (the 10^{th} section); introduced an addition to the administrative code about responsibility over breaking system.

Estonia

E-voting via the internet was on the local elections in Tallinn, in the end of 2005, as a preparation to the parliamentary election in on-line form in 2007.Like most other European countries, Estonia has digital signature legislation, yet unlike many of the other, it also has legislation covering digital certificates for identification cards (presence from 2002).

Also this card has machine-readable cod and microchip (as an additional feature of its security), has data vision on the card and two digital certificates too that are for

checking the face of cards owner and for presenting of digital signatures. Possible that in the future will be realized the integration of identity cards and the banker cards, as others cards for special purposes. By the end of 2004 was issued 500,000 ID-cards.

Consequently, the average Estonia thus has access to two separate digital certificates, based on standardized platforms, which the government supports through the provision of free software tools to businesses and citizens to enable their use. Widespread deployment of trusted digital identities has allowed the use of ID cards in a number of transactions, including with the country's famously e-ready banks. In addition to helping to create one of the world's most developed e-banking markets (95% of banking transactions are estimated to take place though digital channels), Estonia's government plans to leverage familiarity with ID cards in order to implement its e-democracy programme in 2005.

Estonia is the first country of Central Europe, where e-voting is accepted by national legislation. Tallinn pilot projects are the part of on-line voting estonian project, that have been started in August 2003.

On-line system is based on Public Key Infrastructure that let to realize the security indification of citizens with the usage of digital signatures and electronic ID-cards. Country has 1mln citizens that have electronic cards (most of them are the potential voters).

USA

Different types of punched card machines for voting are used many decades in the USA. But the best replacement for old technique is (as a rule) electronic "black box", in more progressive form touch liquid crystal display-screen and registration smart-card of voter.Two american and private companies Diebold and ESS (Election Systems Software) control 80% of market that are produced such equipment and it cost 5000$.
The holding of e-election brings to light on specified problems in the USA. One of these problems is impossibility of voter to check own choice. The availability of problem with new technique is in reports of a congressman Rash Holt from New Jersey State:
"can you image the election day in 2004. You came to the election district and entered your voice though a touchscreen of new voting machine. The screen said that your voice accepted. But when left the cabin, you ask yourself:" Is the machine fixed my voice in a right way? And the fact is that you can not check this information." On realization of electronic technologies, in present time, the USA voter has not got any ability to be sure that his voice was transmitted though a touchscreen and was given to candidate A, and was not prescribe to candidate B.

The second important problem is the problem of security. As said David Dill, the professor of informatics in Stanford University, "all that is said about the present machine is not true because machines are certificated on federal and state levels, but very difficult to get direct information about certificate process". At the same time, on pretext of commercial secret is all information about interior arrangement of technique.
Do not desire with a secret around e-voting machine, Bev Haris, the journalist and the public activist, works under this situation with her friends very long. Consequently was written a book «Black Box Voting: Vote Tampering in 21st Century." Elon House, 2003 (www.blackboxvoting.org).In this book, on the base of the conversation with the concrete event participants was shown, particular, as named "certification" of electronic machine was as a clear farce with open lie (see: www.scoop.co.nz/mason/features/?s=usacoup).

India

Indian voting machine or EVM (Electronic Voting Machine) is developed equipment in 1989–90 that consist of two unites - control unit and balloting unit.

Balloting unit has a list of candidates. Near each candidate is a buttom of voice registration. After the pressing of it, the entering mechanism blocks other candidates. And fixed voice is registered in storage cell of suitable candidate. Control unit has functions of common supporting process, gives total numbers of citizens, sealings of results when the procedure has finished and final results of election have announced.

On the basis of security, electronic machines are not connected with any nets or central data base. Voting results are fixed by members of regional election commission. Electronic machine for voting does not need any operation system because of simple construction. All codes of security are in microscheme and this system is very steady for attack (hacking). In the view of indian EVM computer security this variant is a typical “black box”. All information security is based on secrecy and complicacy of physical access to the code. Familiar to know that an access to the security on basis of a conception of “black box” is unreliable, because gives wider area for fraudsters.

In India 2001 political opposition strongly delivered against EVM that is issued by state organizations and is under control of “party authority”. Regardless of producer assurance and election commission about “machine steady to the hacking”, on the concrete example was shown the following. Microscheme code is scanned and chip can be change on the reprogram. As a result this modification machine does everything as might be but in the end is taken off from all storage cells definite part of voices and is added them to the another candidate. Consequently is guaranteed the victory and is safed the same number of voters.

Brazil-USA

As informed an official representer of Diebold Election Systems, company represents the ability of “paper print” generation to the USA customers without any problems, when they have necessity of it. And more Diebold export supplies have already provided in own machines the abilities of typing control ballot-papers. Particularly, from 300 000 machines for voting that was sold to Brazil, was equipped with control printer on “Mercury method” (in protected box behind glass is painted a ticket that the voter voice is accounted and is in control archive). This technique was examined during brazilian parliament election, practically in October 2002 (www.spectrum.ieee.org/WEBONLY/publicfeature/oct02/evot.html). About similar equipment development for own touchscreen is announced ESS firm, that is a competitor of Diebold.

Australia

By visual demonstration, Australia shows the process of election modernization in reality. In 1998, in this country was a discomfiture with traditional ballot-papers, when two candidates gathered practically equal number of voices. Under such conditions of estimate, they can not find the winner. As a result, the government makes a decision about EVACS development, the system of e-voting and counting of votes (www.elections.act.gov.au/EVACS.html). The creation process of it was open. The government announced a competition with well-known members and judges. The final result was given to the third side to examine it – BMM International, the audit software firm. Consequently all EVACS program supply was written in open source code and in the form of zip file; accessible for everyone on government site.

The majority of Australians also supports the introduction of some form of electronic voting, a study of 1,000 voters by Australian Electoral Commission (AEC) revealed. People most likely to support e-voting lie in the 25 to 34 age group, have an income in excess of A$80,000 (near 53,000$) with Internet access at home and familiarity with online payment solutions.

Switzerland

In Switzerland was referendum with the usage of e-voting in September 2004. More then 2700 from 22000 voters came to vote in on-line mode in the Geneva suburb. Before this, e-voting was used on the local election in Switzerland. On average 90% of swiss voters prefer the traditional e-voting methods. During the referendum was using the program supply of compatible develop with HP and firm Wisekey, those specialize in the area of IT- security. To all voters were given cards with ability to vote in three different ways. Card consisted of 16- significant personal indicator and 4- significant security code. Voters can invite a special web-side, enter a personal code and receive the ballot-paper for voting that was realized by the way of filling, entering the security code and receiving the ballot-paper.

Korea.

Korea will be the first country in Asia to introduce an electronic voting system and for all political elections, starting in 2005. The new voting system will begin on a trial basis from 2004, when the government allows local citizens to vote on its major policies, according to the Korea Herald. Also, up to 85 percent of government services will be available via the Internet, an increase from the current 15 percent. A one-stop service will be available on the Web to help with online company registration. A national distribution information network will be created by the government to keep track of imports and exports, customs, and rail and land transport by 2007. Also, the government will digitise all of its paperwork by 2005 and create a database of major public documents by 2006, to increase efficiency and reduce costs, said the report. Other parts of Asia have also launched pilot projects in e-voting, including Japan, Taiwan and Hong Kong. In June 2002, residents of Niimi, about 500 kilometres (310 miles) southwest of Tokyo, became the first city in Japan to use e-voting. More than 15,000 people registered their choices by pressing their fingers on the screens of voting machines, according to a report by news agency the Associated Press.

5. Conclusion.

The main questions of marked programs are a question of security supply and unification of technical standards, question of legislation. For success development of program is necessary, as minimum:

1). To confirm a technical standards list for each program. At the same time we need to consider that programs must be compatible with corresponding european and international programs, therefore is based on european and international technical standards.

2).To make ukranian legislation as EC has, according to: a) remote (electronic) voting; b) e-passport. State Members must clarify in Custom Code the legislation status of e-signature and e-document for custom, independent of realization condition in different State Members; ***but guaranteed a compatibility of e-signature usage.***

3).In the matter of saving resources, need to "connect" the e-Government program with e-Custom, e-Passport and e-Voting programs and to make unique conception and that is compatible with strategic plans of development.

4). To make or to interest independent (not state) testing center. As in Ukraine is impossible to give direct information about the certification process of security information system; as for this process is responsible a state authority, and for those programs, as e-Voting must be attract independent certificate centres (testing).