Improving authentication and transparency of e-Voting system – Kosovo case

Blerim Rexha, Vehbi Neziri and Ramadan Dervishi

Abstract**—**Authentication and privacy are central issues for acceptance of any e-Voting system in particular and growth of e-Services in general. This paper aims to: (i) to analyze the appropriate architecture and propose new efficient architecture of electronic voting system in Kosovo, and (ii) to analyze the threat vectors and their avoidance in such system. The novelty of implemented solution is based on using dynamic queue list generated based on voters arrivals and identification at the polling station. The proposed architecture enables citizens to cast their vote in any polling station, in opposite to paper form voting where citizen is linked to his predefined polling station. The national election commission configures the smart card, as part of electronic voting infrastructure, to allow decryption of number of records that matches the number of voters in final country wide voting list. The communication between polling stations and central server is encrypted with server's public key stored in digital certificate and every casted vote is digitally signed by ballot box private key. The developed model is used to compare the costs and efficiency of e-Voting against the traditional paper based voting system in Kosovo.

Keywords**—** Digital Signature, Privacy, Security, Smart Cards, e-Voting, X.509 Digital Certificates.

I. Introduction

The right to elect and to be elected is nowadays considered one the fundamental rights of our modern society, which is exercised through a voting system, mainly in manual and paper form. After casting a ballot sheet into a ballot box, it mixes with other ballot sheets and it becomes anonym, no one can link it to a specific voter. Assuring voter's privacy is a fundamental instrument for protecting the freedom of voter's choice. It mitigates corruption and pressure because no one knows whether voters are saying the truth about cast ballots. Voter's privacy and tallying accuracy are central issues for the acceptance of any electronic voting system.

Kosovo from 1999 until today has organized several elections at both local and national level. Under the administration of United Nation Mission in Kosovo (UNMIK), Kosovo held municipal elections in year 2000 and 2002. The national elections were held in year 2001 and 2004. Also in November 17th, 2007 local elections were held for mayors and national elections for the Assembly of Kosovo. All these elections were managed by the international community and the Organization for Security and Cooperation in Europe (OSCE) as the main supervisory body.

Since declaring its independency in 2008, Kosovo has organized two elections in local and national level. These elections were organized by the Central Election Commission (CEC). The last national elections were held in December 2010. A huge debate about irregularities was raised by all political parties and civil society in Kosovo. "A high number of irregularities during the Kosovo Assembly elections have severely affected the trust in the democratic process in Kosovo. Breaching the secrecy of the vote by family and group voting was in many places the rule and not the exception" was one of many findings of European Union Election Expert Mission (EU EEM) to Kosovo report early this year [1]. Overton in "Stealing Democracy" concludes that "Voters do not elect politicians, but politicians choose voters by manipulating election rules". Further he asks: "What should we do to restore power to the people?" [2].

II. Paper based voting

A. Legal framework

Kosovo constitution article 45 defines that "Every citizen of the Republic of Kosovo who has reached the age of eighteen, even if on the day of elections, has the right to elect and be elected" and Kosovo is as one election zone. Further provisions are specified on Law on General Elections in the Republic of Kosovo No 03/L-073 and Law on Local Elections in the Republic of Kosovo No 03/L-072 [3]. Two very sensitive elements of the paper-based voting process during last elections in Kosovo were identified:

- Conditional voting, and
- Voting from abroad for expats.

Conditional voting provides an opportunity of voting for those voters who for various reasons, mostly technical in nature during the compilation of voter's lists are not part of the final voters list [4]. According to [4] conditional voting often is considered to have many shortcomings and usually delays declaring the final results of counting and presents a

Dr. techn. Blerim Rexha is associate professor at Department of Computer Engineering, Faculty of Electrical and Computer Engineering, University of Prishtina, 10000 Prishtina, Kosovo (e-mail: blerim.rexha@uni-pr.edu).

M. Sc. Vehbi Neziri is head of software development department at Kosovo Property Agency, Government of Kosovo, 10000 Prishtina, Kosovo (e-mail: vehbineziri@gmail.com).

M. Sc. Ramadan Dervishi is teaching assistant at AAB-Riinvest University in Prishtina and deputy head of Information Technology department of NLB Prishtina Bank, 10000 Prishtina, Kosovo (e-mail: dervishi@gmail.com).

significant potential to reduce confidence in the whole voting process. The drawback of this form of voting represents the possibility of the voting fraud in the counting centers. In the last parliamentary elections this form of voting has been used by over 26 thousand voters [5]. For expats Kosovo organizes the voting per post. However this form is very little used. In the last parliamentary elections only 1640 expats have made usage of this form of voting [6], even though the number of expats living outside the country is very high.

Kosovo current legal framework has no provisions for electronic voting, and it is clear that these laws must be amendment to support electronic voting. Developing a legal and regulatory framework for enabling electronic voting is presented in [7]. Estonian legal framework has been proposed as model since it is considered as most advanced in Europe that fulfills electronic voting requirements [8]. The Kosovo election legal framework consists of other administrative regulation enforced by Central Election Commission (CEC).

B. Voting procedures

By laws in place, Kosovo is as one election zone, divided in 746 polling stations with 2280 ballot boxes distributed over hole country. The CEC receives the voting list (VL) from National Civil Register (NCR) and prepares the voting lists for every polling station. As defined by CEC regulation voting procedure can summarized, as presented the UML schema in Fig. 1. Similar approach is presented in [9].

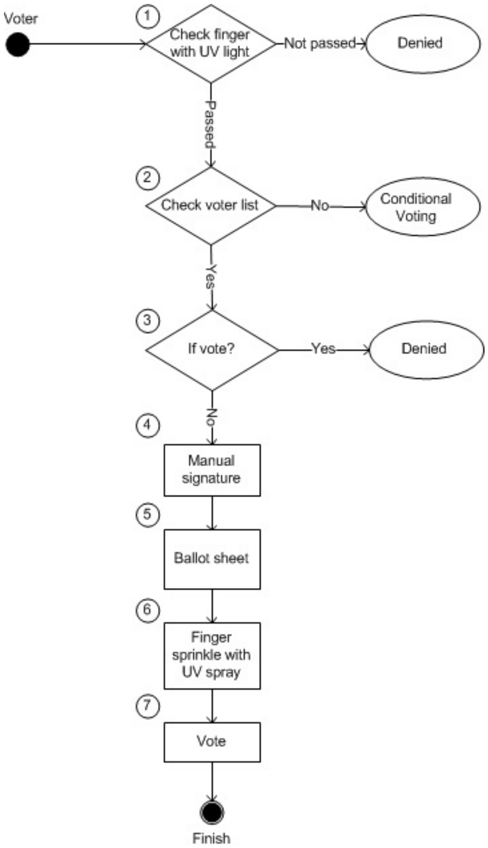


Fig. 1 Manual voting flow

As EU EEM cited in its report, during the last election there were many procedure violations starting from double voting, fraudulent and impersonation, i.e. voting unauthorized for third persons [1].

C. Threating vectors

The CEC provided each polling station with lists of all registered voters including pictures and alphanumeric ID information. Analyzing the flow presented in Fig. 1 in each step there are possibilities to breach the privacy and security. In step 1, as presented in Fig. 1, the voter finger is checked by administrative election staff with UV lighter if voter has already casted a vote in another polling station during the day. As it was cited by CEC expenditure report in many polling stations were malfunctioning of UV lighters reported [10]. The accuracy of the voters list was also on the main irregularities reported by EU EEM as consequence double voting was possible. In step 5, as presented in Fig. 1, there were cases reported where election administrative staff has given many ballot sheets to voter [1]. On Election Day, some polling stations opened slightly later. The delays were related to several problems pertaining to the sensitive materials used in the stations. In some cases the sensitive materials didn't arrive on time - either the sprays, polling papers or the lamps. A number of polling stations across the country were given non-working UV lights. This was either due to the low quality of the lamps or problems with the batteries [11].

III. E-VOTING SYSTEM

A. e-Voting forms

There is a wide variety of types of e-voting systems, ranging from the use of electronic equipment inside a polling station to the remote electronic systems where votes can be cast via the Internet or mobile devices such as mobile phones. Electronic voting system usually consists of three systems which can be referred to as subsystems, as presented in Fig. 2, which interact with each other so that as the overall system works the way that it was designed. Such approach is also given in [12]. These sub-systems can act independently in their own environments, but interact with each other because only together can perform and satisfy the common requirements arising from the management of elections in case of electronic voting.

E-Voting System
Election Administration System
Counting and Results System

Fig. 2 e-Voting sub-systems

B. e-Voting architecture

Traditional, paper form voting in Kosovo consists of 746 polling stations and 2280 ballot boxes. e-Voting architecture based on these facts is presented in [13]. The proposed architecture, as presented in Fig. 3, is most efficient one, as it requires:

- One (1) redundant Authentication and Registration Server,
- One (1) redundant Counting Server, and
- 2280 electronic ballot boxes

Until now the organization of parliamentary elections for the Assembly of Kosovo has been done with a single zone election model. The organization of elections for municipal assemblies and mayors belongs to the same model, i.e. the municipality is the one electoral unit within its territory. Architecture shown in Fig. 3 is designed as an online type architecture, which enables citizens to cast their vote in any polling station, in opposite to paper form voting where citizen is linked to his predefined polling station. This option will eliminate the abuses that have been spotted with conditional votes, which in 2010 Kosovo elections have been over 26.000 votes [5].

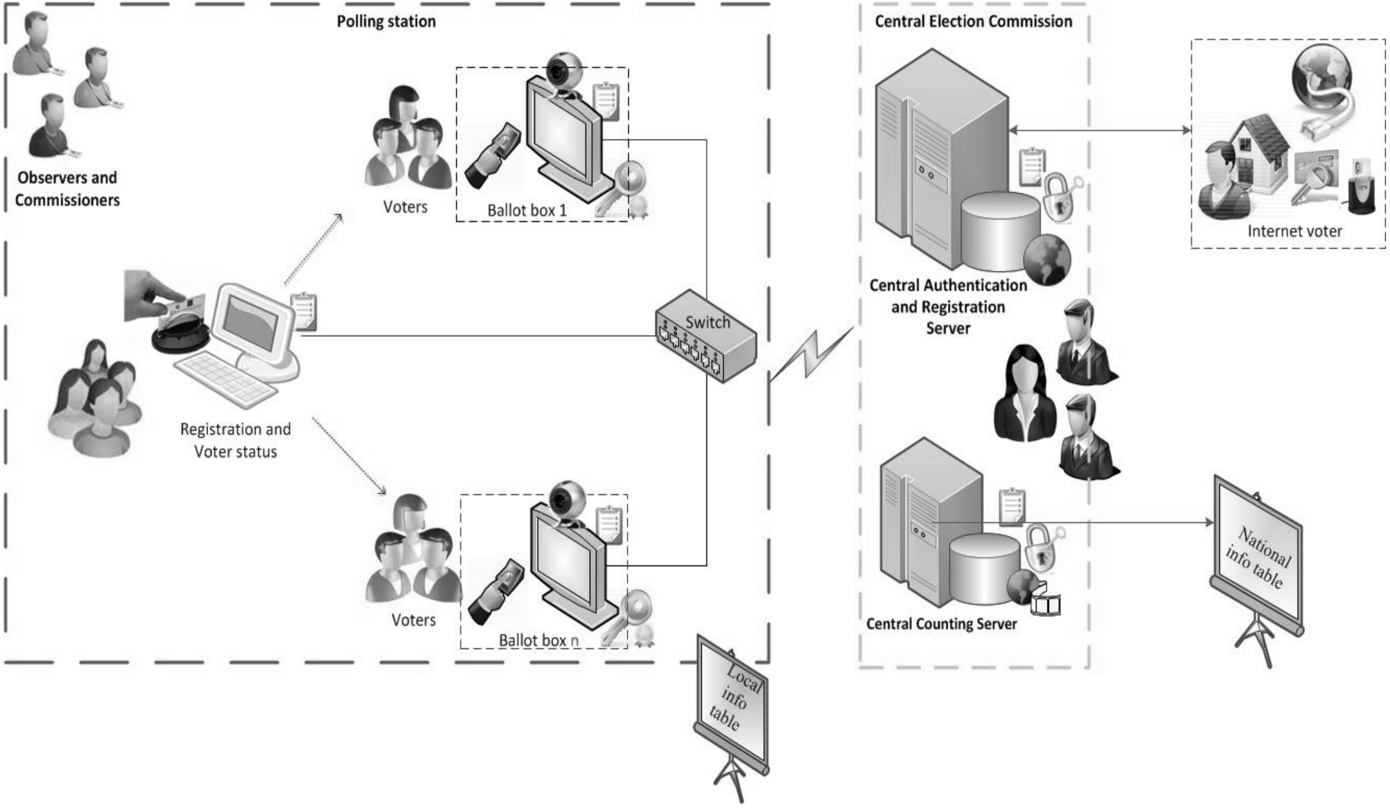

Polling station
Observers and Commissioners
Voters
Ballot box 1
Registration and Voter status
Switch
Voters
Ballot box n
Local info table
Central Election Commission
Central Authentication and Registration Server
Internet voter
Central Counting Server
National info table

Fig. 3 Online general e-Voting architecture

The Central Election Commission, as presented in Fig. 3, is composed of Central Authentication and Registration Server (ARS), Central Counting Server (CCS) and National Info Table, which serves as a medium for the announcement of results and statistics. CCS has a digital X. 509 certificate and its private key is stored in the smart card. The private key does not leave for any moment smart card and access to it is protected by a Personal Information Number (PIN). Public and private keys have size of 2048 bits. Hardware polling station consists of:

- One or more electronic ballot boxes as touch screens,
- One or more fingerprint scanner, connected to ballot box,
- One or more surveillance camera, connected to ballot box,
- One voter registration status computer,
- One barcode reader, connected to voter registration status computer, and
- Local information table.

C. Authentication and voters status

As presented in Fig. 3 every polling station has one voter registration status computer where voter's status is registered. This computer is the starting point where the voter will be notified when he enters the polling station. The voter registration status computer is equipped and connected with 2D barcode reader for reading ID cards, which contains various information about its owner. At this point also are accepted other documents which are allowed to vote, as determined by law.

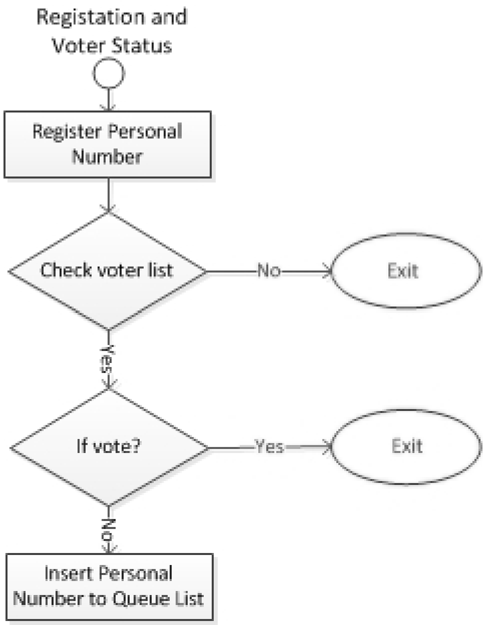


Fig. 4 Registration and Voter Status process

When the election officer scans the identity card, or record the ID number of voters, the system will verify if such person exists on the list of voters and check if that person has previously voted in any other polling station. This is shown schematically in Fig. 4.

If the person has not voted yet, the system will record the ID number in a dynamic queue list. This queue list will be used in next step when a voter scans his fingerprints. Once the voter has voted, the system will remove him from the dynamic queue list. This dynamic queue list is filled and emptied during the voting process based on voter's arrivals/leaving the polling station.

D. Authentication based on fingerprint matching

Fingerprints or finger scanning technology is very old method which uses the distinctive fingerprints features for identifying or verifying the identity of individuals. All fingerprints are unique models. A normal fingerprint pattern is made up of lines and spaces. These lines are called ridges while the spaces between the ridges are called Valleys [14].

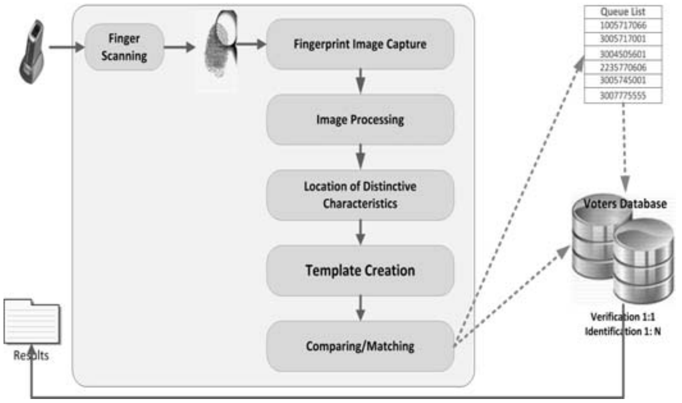


Fig. 5 Fingerprint matching process

The process of scanning and matching the traces of fingerprints is presented in Fig. 5. Once the voter appears at electronic ballot box, he puts his finger on the scanner for fingerprint scanning. The system will first take the trace of the finger image and then it will process the image by finding distinctive features. Based on these characteristics it will build template. Based on this template system will check for compliance with tracks that are on the voters dynamic queue list. If the dynamic queue list was missing the matching process would be compared against the whole national voters list, which in last parliamentary elections contained 1,632,276 voters [5]. In our proposed solution the comparison is done against the entries in dynamic queue list, which in average contains less than 40 entries. These 40 entries are in fact voters that are already identified by voter registration status computer and waiting to be authenticate by ballot box to cast their vote.

One could easily conclude that comparing the 1,632,276 and 40 the fingerprint matching performance is increased by more than 40,000 times!

Once the voter has cast his vote the ballot box will inform voter registration status computer to remove the specific voter from dynamic queue list. *It is worthy to stress out that using fingerprint matching technologies voters are not able to cast their vote twice*, as this is the case in traditional paper form voting and one of irregularities in 2010 parliamentary elections in Kosovo.

E. Assuring voters privacy

After successful authentication based on fingerprints, assuming as it was the case in Kosovo last elections, voter selects one political party and up to five candidates numbered from 1 to 110 among the selected party. The voter's data are presented Fig. 6.

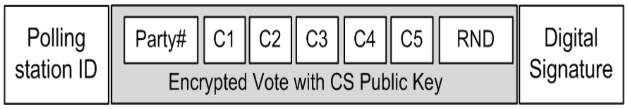


Fig. 6 Encrypted vote structure

Similar approach, selecting up to K out of L and using randomizers are proposed in [15] and [16]. For every casted vote the ballot box generates a random number, which is concatenated to voter's selection and makes the encrypted voters selection unique, as presented in Fig. 6. The casted vote is encrypted with public key of Central Counting Server (CCS) and is digitally signed by ballot box private key. The encrypted and digitally signed vote is stored into Central Authentication and Registration Server (CARS). The similar approach is presented in [17] and these voters' data are secure to be transmitted over insecure channel such as Internet. Nevertheless the communication between each ballot box and Central Authentication and Registration Server is encrypted using Central Authentication and Registration Server public key.

After closing the ballot boxes, the signed encrypted votes are checked against manipulation and unauthorized records insertion in CARS. In the second step the CARS separates:

(i) Voter ID,

(ii) Polling ID, and
(iii) Digital signature from voting record and transfers it to CCS.

To decrypt the arrived records the CCS needs the private key. Since the access to private key, needed for decryption, which is stored in smart card and is protected by PIN following schema is developed. This basic schema is presented in Fig. 7 and is independent from number of election commissioners. Every commissioner has the same weight in PIN knowledge process. The smart card final PIN is result of XOR operation over all commissioner's PIN, as presented in Fig. 7.

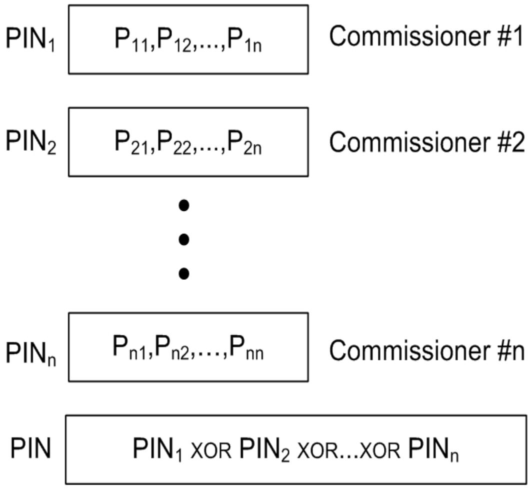

PIN_1
$P_{11},P_{12},\ldots,P_{1n}$
Commissioner #1
PIN_2
$P_{21},P_{22},\ldots,P_{2n}$
Commissioner #2
PIN_n
$P_{n1},P_{n2},\ldots,P_{nn}$
Commissioner #n
PIN
PIN_1 XOR PIN_2 XOR…XOR PIN_n

Fig. 7: XOR schema

The CEC initially configures the smart card with capability of decrypting number of records that matches the voting list, call it N. After closing the ballot boxes and before the counting begins all commissioners agree that on all polling station have voted M out N voters, where M ≤ N, a report received from national (central) info table. After entering smart card's PIN, the smart card is reconfigured to decrypt only M records, since only M voters have casted their vote. This feature is crucial for stopping double voting problem.

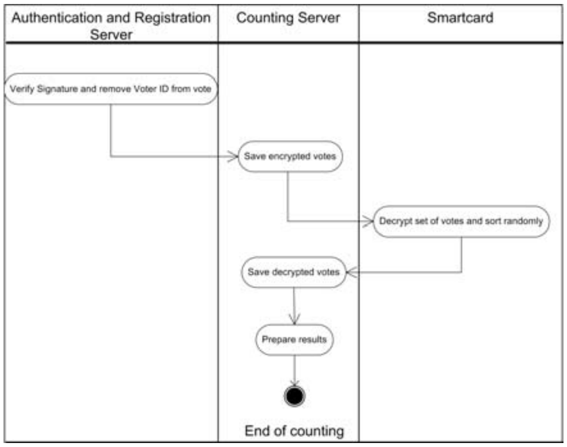

Authentication and Registration Server
Counting Server
Smartcard
Verify Signature and remove Voter ID from vote
Save encrypted votes
Decrypt set of votes and sort randomly
Save decrypted votes
Prepare results
End of counting

Fig. 8: Decryption flow

The Fig. 8 represents the decryption flow of voter's choice. Votes in CCS are ready to be decrypted using private key. The decryption process takes place in smart card, since its associated private key never leaves the smart card.

In order that the proposed model to be accepted by all involved parties the solution must be certified as trustworthy, i.e. it includes and reflects the voter's selection. The source code of all developed application must be opened for public audit. To increase voters privacy, every encrypted records is send to smart card for decryption. The decryption, as presented in Fig. 9, is done using private key stored in smart card.

The decrypted result, i.e. the plain text is stored randomly in array that can store M plain records in smart card, as presented in Fig. 9. Generating random number is one the oldest and basic functions build in a smart card [18]. The smart card used in a developed application has capacity of 72 Kbytes of EEPROM [19]. After this moment data are ready to be shown by national info table, which in our case is an ASP.NET application. The application was developed using C# programming language and the latest Microsoft .NET runtime environment. Microsoft Security classes have been used for encryption, decryption, creation and verification of the digital signature. For finger print matching is used Software Development Kit (SDK) of Neurotechnology.

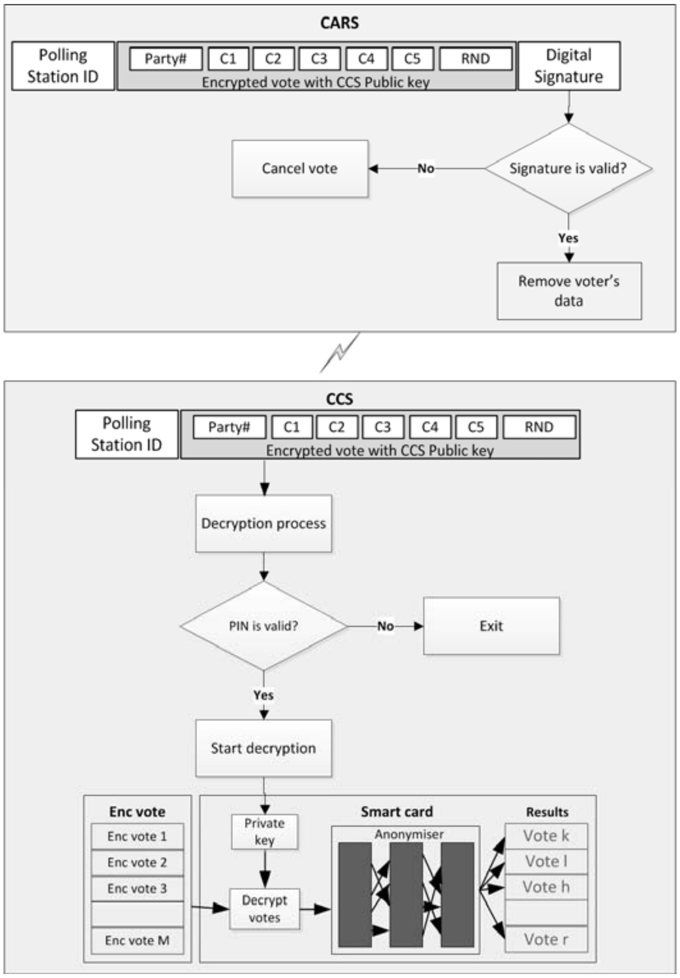


Fig. 9 Smart card as anonymiser

IV. AUDIT LOGS

Just as is the case with manual voting systems, e-voting systems have to able to be audited, i.e. it must be possible to examine the processes used to collect and count the votes and to re-count the votes in order to confirm the accuracy of the results. The greatest danger to e-voting systems is if external interference on systems is possible and can go undetected affecting the results of the voting [20]. This is why independent and extensive security monitoring, auditing, cross-checking and reporting needs to be a critical part of e-voting systems [20]. Trustworthiness of systems is not sufficient if a system functions only on the basis of analysis, methods and technology used by which one can theoretically proof its accuracy. For a system to be reliable it is not enough only implementation of security policies and trust in the safety analysis, but it should at any moment be able to be verified whether the system has worked as it was designed. To enable such verification it is proposed that in the system should be set an audit function which keeps track at any time of every data flow and system operations. If in a system it is possible that for every action to preserve the traces of it, than such system is regarded as a reliable system. If we rely on the systems of other countries that have implemented electronic voting systems, each of them has implemented the audit function.

Part of a system audit of a polling station consists of group log files in which events that occur in each component are recorded.

Group of log file consists of *Group* ***L1*** which is located on the component of registration of queue and voter's status. This group consists of three files:

(i) file Log_vote of voters who have the status "may vote",
(ii) file of voters who have status "voted", and
(iii) file of voters who have the status "not found in list of voters ".

These files have the structure ([*voter_id*], [*status*]).

Group ***KL*** is located at the components; ballot box and records the events that occur in this part. Consists of file_Log_KLn that registers the voting process which has the structure ([*voter_id*], [hash [ENC (*vote*)]).

Group **LSAR,** as presented in Fig. 10, consists of file to keep track of digital signature verification. File with the tracks of the structure *Log_ver_DS* valid signatures ([*voter_id*], [*hash* [ENC (*vote*)]), file with invalid signatures *Log_no_ver_DS* with, with the structure ([*id_votuesit*]) and file of the votes for counting *Log_vote_for_counting* with structure ([*voter_id*], hash (ENC ([*vote*])).

Group **LSNR** consists of file *Log_counted* with structure ([*ID*], [hash (ENC ([*vota*])]), where ID denotes a sequential number.

Verification of the accuracy of the system is done by the following actions:

Log_vote file should be equal $\sum_{i=1}^{m} Log\_KLi$ to without the hash [ENC (*vote*)] (1)

this verifies that in the ballot box have voted only authorized voters who were register from the component of queue list and voter's status.

- $\sum_{i=1}^{m} Log_{KLi}$ =Log_ver_DS (2)

This proves that the only votes that have come from the ballot box with digital signatures are verified.

- *Log_counted*(without [*ID*])= $\sum_{i=1}^{m} Log\_KLi$ without [*voter_id*] (3)

This proves that the votes are counted only have come from the ballot boxes.

By using equations (**1**), (**2**) and (**3**) can be verified that a vote is successfully processed from its initial point, voting point, until the final point, the point of counting votes. These equations make the system transparent, using the above rules the system of auditing electronic voting system is build. In every moment the Audit System can collect the log files stored on each part of the system as shown in Fig. 10.

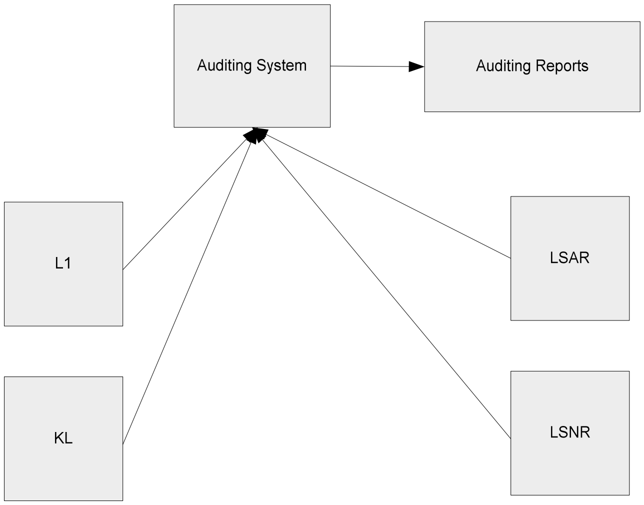


Fig. 10 Process of auditing system

After collecting log files from every part of system, the auditing system check this files using rules (1) (2) (3) and generates audit reports. If any of these rules (1) (2) (3) is not satisfied using log files, than the report is generated and the vote is canceled.

In proposed solution for Kosovo Case the auditing can be performed also using the photo of the voter. In proposed system every ballot box contains a camera, which takes a photo three times during the voting process: (i) when the voter put the finger on fingerprint scanner, (ii) when the voter starts to elect the candidates and (iii) when the voter vote. These pictures are saved with filename using the format like *[voter_id_yyyymmddhhmmsstt.jpg]*. National Civil Register contain also the photo of every voters, it is mandatory to take the photo during the registration process, when the citizens apply for ID Cards, using this resources the auditing can be made also comparing the photo taken in voting process and photo taken in registration process.

V. RISK ANALYSES

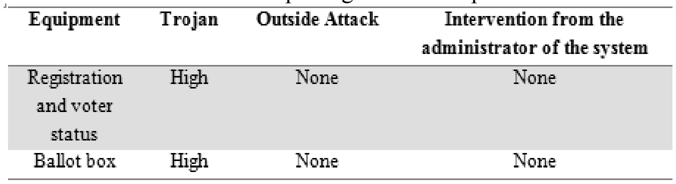
The system risk analysis is done based on the three main parts of the system:

- Client,
- Server and

- Intervention by the system's administrator.

The risk in the server part is the highest from the external attacks such as internet attacks. Risk of the highest level exists only at software type Trojan as presented in Tab. 1, which can be as infection in the case of installing devices through USB or other external media, in any of the equipment that installs a Trojan can cause deviation of the process and peek.

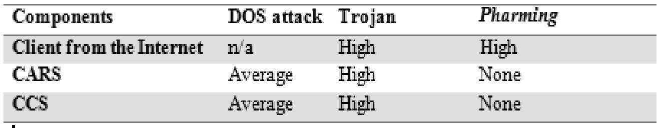
Tab. 1 Risks in polling station components



Equipment	Trojan	Outside Attack	Intervention from the administrator of the system
Registration and voter status	High	None	None
Ballot box	High	None	None

As far as the risk in the central part is concern, we are dealing with a greater risk in terms of attacks from outside, while in terms of Trojan type software risk is the same as that in the polling station. Once the central servers at a time when voting via the Internet will be online, there exists risk from Denial of Service (DOS) attacks as shown in Tab. 2; also it should be taken into account the risk on the client part, where this piece of architecture cannot be under the control and administration by the election staff.

Tab. 2 Risks in the core components



Components	DOS attack	Trojan	*Pharming*
Client from the Internet	n/a	High	High
CARS	Average	High	None
CCS	Average	High	None

If all these features are taken into account, the system must take a green light to proceed toward its implementation.

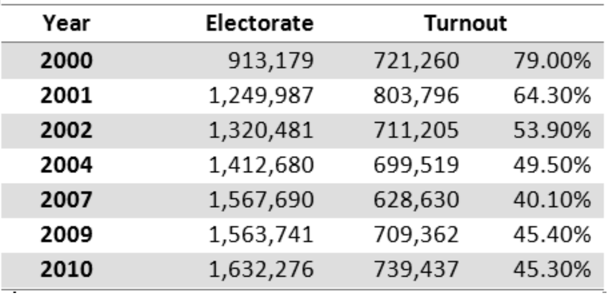
VI. Future Works

In the future in proposed system for Kosovo can be added more security features based on protecting system from Trojans on client side, also system can be modified to protect database from any unauthorized changes from viruses or even by system administrators. Protecting system from Trojans on client sides (voters from internet) and ballot boxes can be made using the method of VTS (Voter Token Security) that used in project named CodeVoting developed on University of Lisbon [21]. To protect system from unauthorized changes even from system administrators on servers side, can be implemented the technology that is used in Norway, the votes are saved on write once medium, this medium guaranties that the votes can't be changed from original data [22].

VII. Conclusions

According to officials in the CEC [6] the number of registered voters and turnout is presented in Tab. 3.

Tab. 3 Turnout statistics



Year	Electorate	Turnout	
2000	913,179	721,260	79.00%
2001	1,249,987	803,796	64.30%
2002	1,320,481	711,205	53.90%
2004	1,412,680	699,519	49.50%
2007	1,567,690	628,630	40.10%
2009	1,563,741	709,362	45.40%
2010	1,632,276	739,437	45.30%

Tab. 3 illustrations that voter turnout is in decline, so the implementation of e-voting can affect the increasing of voter turnout. The developed online architecture is cheaper than traditional paper voting. Comparing the Kosovo 2010 parliamentary election accumulative expenses, as reported in [6] and current IT market prices for proposed online architecture are presented in Fig. 11.

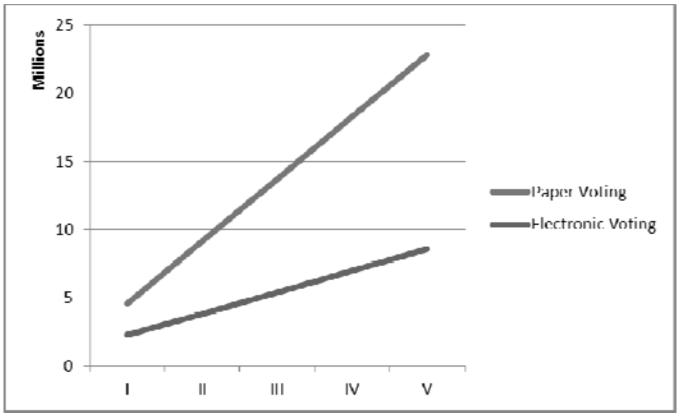


Fig. 11 e-Voting vs. paper voting cost

In Fig. 11 graphically is presented cumulative cost for paper voting and electronic voting for 5 years, as this is the depreciation time for technology used in Kosovo. In the first year the difference between paper voting and electronic voting costs is close to each other, but after the first election the depreciation of hardware in every year is 20% and the cost of electronic voting will be decreased compared to previous years. Based on the depreciation time, the investment for IT equipment should be done every 5 years and this increases the cost as presented in Fig. 12, but still is cheaper than traditional paper voting.

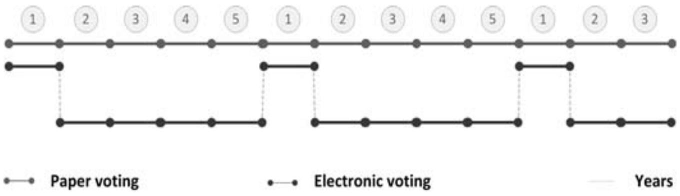


Fig. 12 e-Voting vs. paper voting cost

References

[1] ENEMO Election Observation Mission Kosovo Assembly Elections 2010 – Final Report, April 2011.

[2] Spencer Overton, Stealing Democracy: The new politics of voter suppression, 2007.

[3] Assembly of Republic of Kosovo, Laws, http://www.assembly-kosova.org/?cid=2,191, December 2011.

[4] Demokracia në Veprim, Ndryshimet e Pamjaftueshme në Legjislacionin Zgjedhor, "http://www.demokracianeveprim.org/publikime/Ndryshimet e Pamjaftueshme ne Legjislacionin Zgjedhor.pdf" Prishtinë 2010.

[5] Kosovo Central Election Commission, Statistikat e përgjithshme, Prishtinë, 2011.

[6] Kosovo Central Election Commission official web site, www.kqz-ks.com, Prishtinë, 2011.

[7] Axel Schmidt, Dennis Heinson, Lucie Langer, Zoi Opitz-Talidou, Philipp Richter, Melanie Volkamer, and Johannes Buchmann, Developing a Legal Framework for Remote Electronic Voting, Second International Conference Vote-ID, pp92-105, Luxembourg, September 7-8, 2009.

[8] The National Election Committee, E-Voting System, Tallin 2005

[9] Sharil Tumin and Sylvia Encheva, Web-based Election System for Small Scale to Medium Scale Academic Societies, Proceedings of the 9th WSEAS International Conference on DISTANCE LEARNING and WEB ENGINEERING, ISSN: 1790-2769, pp.48-53, Budapest, Hungary September 3-5, 2009

[10] Kosovo Central Election Commission, Raporti i shpenzimeve per zgjedhjet e parakohshme per Kuvendin e Kosoves 2010 (Election 2010 Expenditure Report), www.kqz-ks.org, 2011

[11] Kosovar Institute for Policy Research and Development, Kosovo National Elections 2010 - Overview and Trends, Prishtina, April 2011

[12] Ministry of Local Government and Regional Development (ErdoGroup), System Architecture: Overview, Interfaces and Deployment, Oslo, 2011.

[13] B. Rexha, R. Dervishi and V. Neziri "Increasing the trustworthiness of e-Voting systems using smart cards and digital certificates – Kosovo case 2011"- The 10th WSEAS International Conference on e-Activities (E-ACTIVITIES '11), Bina Nusantara University, Jakarta, Island of Java, Indonesia, December 1-3, 2011

[14] Edmund Spinella, Biometric Scanning Technologies: Finger, Facial and Retinal Scanning, SANS Institute, San Francisco, 2003.

[15] Claudia Garcya-Zamora, Francisco Rodriguez-Henriquez, Daniel Ortiz-Arroyo, "SELES: An e-Voting System for Medium Scale Online Elections," enc, pp.50-57, Sixth Mexican International Conference on Computer Science (ENC'05), 2005

[16] Martin Hirt, Receipt-Free K-out-of-L Voting Based on ElGamal Encryption, Towards Trustworthy Elections, LNC, Springer 2010

[17] B. Rexha, H. Lajqi and M. Limani. Implementing Data Security in Student Lifecycle Management System at the University of Prishtina. WSEAS Transactions on Information Science and Applications, ISSN: 1790-0832, vol. 7, pp. 965-974, July 2010.

[18] Wolgang Rankl and Wolfgang Efing. Handbuch der Chipkarten, Aufbau - Funktionweise Einsatz von Smart Cards. Carl Hanser Verlag Munchen Wien., ISBN = 3-446-21115-2, 1999.

[19] Infineon Technologies. Security & chip card ics, interface specification sicrypt secure token platform for public key cryptography version 2.1. http://www.sicrypt.com, June 2003.

[20] E-voting, Auditing of e-voting systems, http://aceproject.org/ace-en/focus/e-voting/e-voting-auditing

[21] Carlos Riberio and Paulo Ferreira Rui Joaquim, "Improving Remote Voting Security with CodeVoting,"

[22] M J Morshed Chowdhury. Comparison of e-voting schemes: Estonian and Norwegian solutions.