Increasing the Trustworthiness of e-Voting Systems Using Smart Cards and Digital Certificates – Kosovo Case

BLERIM REXHA
RAMADAN DERVISHI
VEHBI NEZIRI
Faculty of Electrical and Computer Engineering
University of Prishtina
Kodra e Diellit pn., 10000 Prishtina
KOSOVO
blerim.rexha@uni-pr.edu dervishi@gmail.com vehbineziri@gmail.com
http://www.uni-pr.edu

Abstract: - In this paper is presented a novel solution for the implementation of an electronic voting system using smart cards and digital certificates. The novelty of implemented solution is based on using smart card as secure processing and anonymizer device and constraining their processing capability to a certain number of voting records, which is equal to the final number of voters that voted at specific polling station. The national election commission configures each smart card, as part of polling station infrastructure, to allow decryption of number of records that matches the number of voters in voting list. For security reasons, polling station certificate and its associated private key are stored in a smart card. The access to private key is protected by a personal identification number, which is XOR-ed based on number of commissioners at the polling station. The developed model is used to compare the costs and efficiency of e-Voting against the traditional paper based voting system in Kosovo.

Key-Words: - Digital Signature, Privacy, Security, Smart Cards, Voting, X.509 Digital Certificates

1 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.

Since declaring its independency in 2008, Kosovo has organized two elections in local and national level. 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].

2 Paper Based Voting

2.1 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 [2]. These laws have 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 is presented in [3]. Estonian legal framework has been proposed as model since it is considered as most advanced in Europe that fulfills electronic voting requirements [4]. The Kosovo election legal framework consists of other administrative regulation enforced by Central Election Commission (CEC).

2.2 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 (NRC) 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 [5]

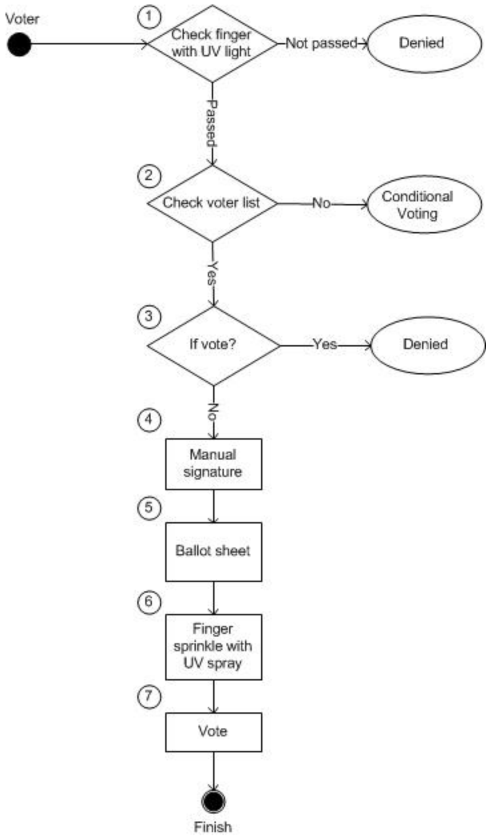

Fig. 1: Manual voting flow

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].

2.3 Privacy and security breaches

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. As it was cited by CEC expenditure report in many polling stations were malfunctioning of UV lighters reported [6]. 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].

3 e-Voting System

Issues rose above, which are not observed in Kosovo only, but in many countries, require a new approach to voting system that fulfills the privacy and accuracy of voters. For Kosovo case the main objective was to develop a system that reflects traditional voting process and it does not require a high computer literacy.

3.1 e-Voting architecture

Traditional, paper form voting consists of 746 polling stations and 2280 ballot boxes and architecture proposed in this paper is based on these facts. General architecture of e-Voting system is presented in Fig. 2.

The polling station consists of Authentication and Registration Server (ARS) and Counting Server (CS) which are connected with ballot boxes and registration and voter status computer. The voting procedures are same as presented in Fig. 1. In order to assure voters privacy there was deployed a governmental Public Key Infrastructure, as proposed in [7], which is responsible to issue digital X.509 certificates to citizens, servers and other devices.

The Kosovo Civil Registry (KCR) holds all citizens data including finger print data. Finger print data are recorded during issuing of the national ID card. The proposed model uses these finger print data for citizen authentication. Each polling station receives from CEC the respective voting list, which contains also the finger print data. The CS has a X.509 digital certificate and its associated private key is generated and stored in smart card. The CS public and private keys have the size of 2048 bit. This private key never leaves the smart card and access to it is protected by Personal Identification Number (PIN).

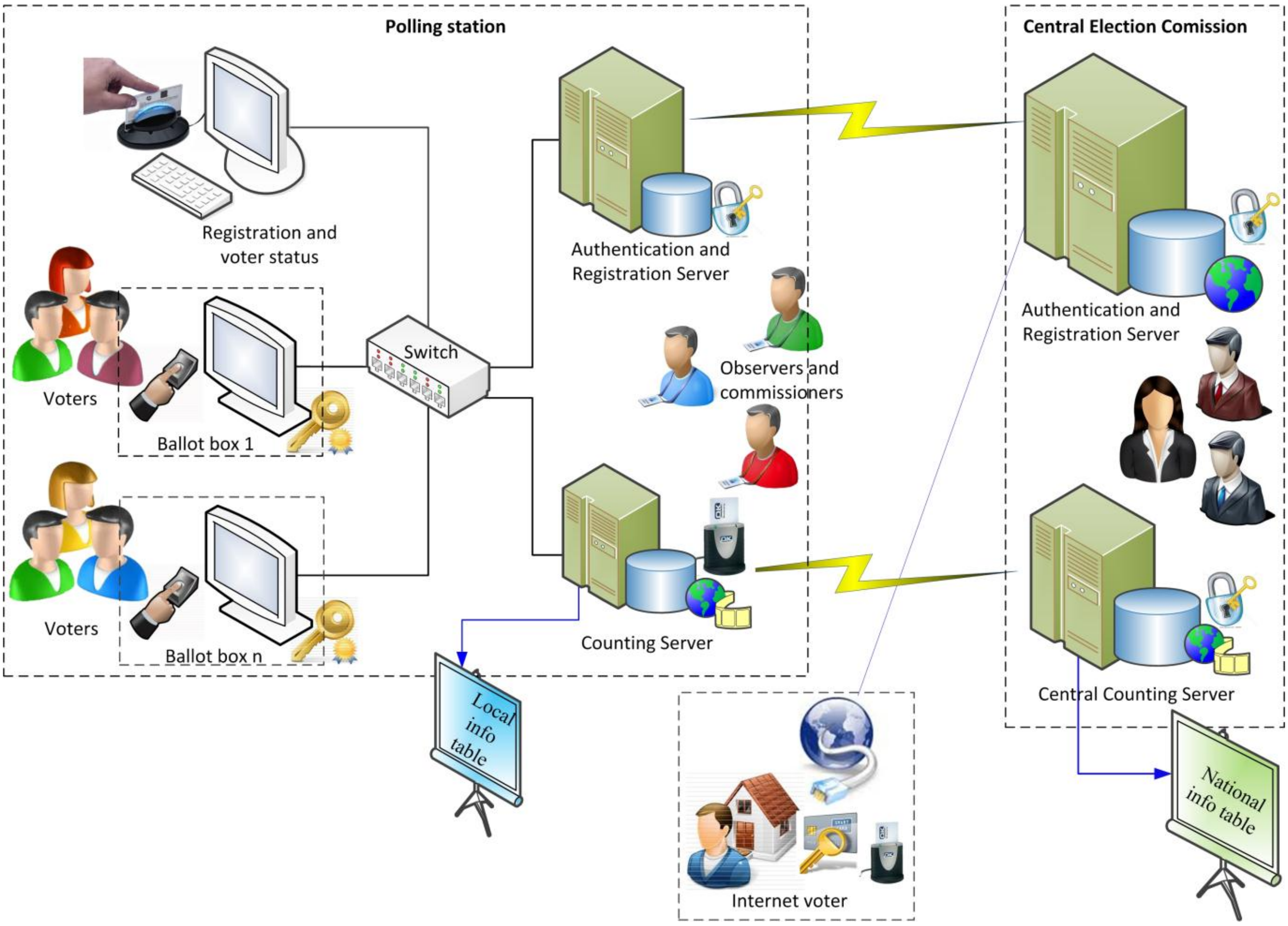
Polling station
Central Election Comission
Registration and voter status
Authentication and Registration Server
Voters
Ballot box 1
Switch
Observers and commissioners
Voters
Ballot box n
Counting Server
Local info table
Internet voter
Authentication and Registration Server
Central Counting Server
National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

Fig. 2: General architecture of e-Voting system

The local info table shows the voting results, as required by CEC administrative regulations and also gives general information about local election process. The Central Authentication and registration Server (CARS) has also a digital X.509 certificate and its associated private key stored in its system store. This digital certificate allows Secure Socket layer (SSL) encryption of casted ballot sheet for home voters via Internet. Central Counting Server (CCS) is connected with all polling stations and receives the results from them.

3.2 Assuring privacy

After successful verification using existing ID card voter proceeds to ballot box where is required to scan its finger print. Voter's scanned finger print is compared with existing finger print set in voting list of polling station. 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 as presented Fig. 3. Similar approach, selecting up to K out of L and using randomizers are proposed in [8], [9]. 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. 3. The casted vote is encrypted with public key of CS and is digitally signed by ballot box private key. The encrypted and signed vote is stored into ARS.

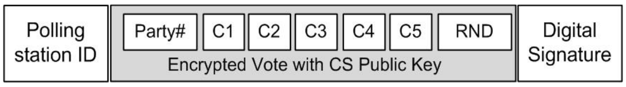

Fig. 3: Encrypted vote structure

After closing the ballot boxes, the signed encrypted votes are checked against manipulation and unauthorized records insertion in ARS. In the second step the ARS separates: (i) Voter ID, (ii) Polling ID, and (iii) Digital signature from voting record and transfers it to CS. To decrypt the arrived records the CS 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. 4 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. 4.

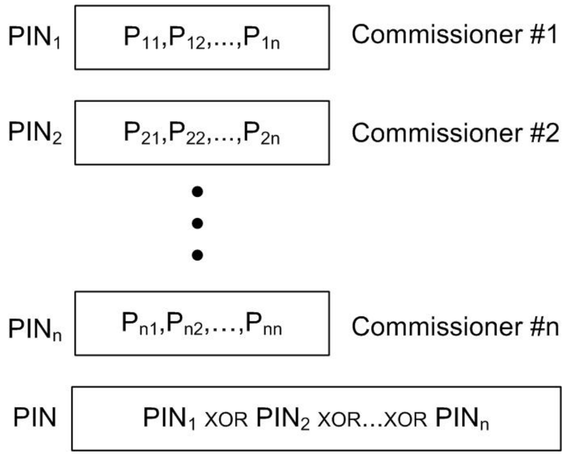
PIN_1
$P_{11}, P_{12}, \ldots, P_{1n}$
Commissioner #1
PIN_2
$P_{21}, P_{22}, \ldots, P_{2n}$
Commissioner #2
PIN_n
$P_{n1}, P_{n2}, \ldots, P_{nn}$
Commissioner #n
PIN
PIN_1 XOR PIN_2 XOR…XOR PIN_n

Fig. 4: XOR schema

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

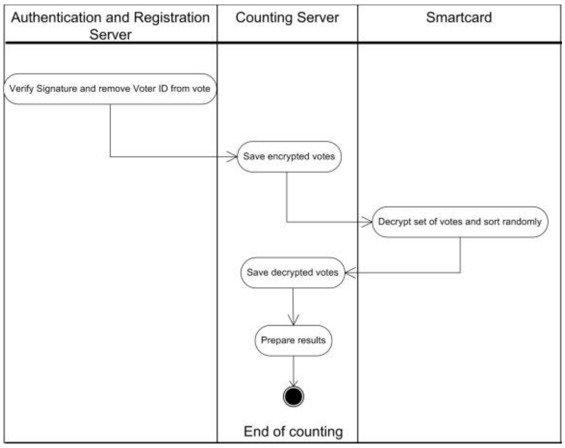
Authentication and Registration Server
Counting Server
Smartcard
Verify Signature and remove Voter ID from vote
Save encrypted votes
Decrypt set of votes and sort randomly
Save decrypted votes
Prepare results
End of counting

Fig. 5: Decryption flow

The Fig. 5 represents the decryption flow of voter's choice. Votes in CS 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.

3.3 Increasing trustworthiness

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. 6, is done using private key stored in smart card.

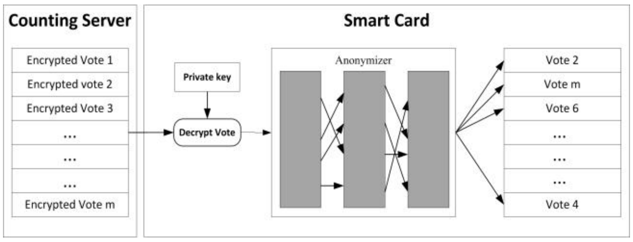

Fig. 6: Smart card as anonymizer

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. 6. Generating random number is one the oldest and basic functions build in a smart card [10]. The smart card used in a developed application has capacity of 72 Kbytes of EEPROM [11]. After the smart card decrypts the M records the private key is deleted and any later verification and decryption of votes is not any more possible. The decrypted polling station results, in their path to CCS, are encrypted with CCS public key and digitally signed by CS private key. The CCS is configured to receive election results only from authorized polling stations CS. The arrived data are checked against data integrity to avoid man in the middle attack and are decrypted with CCS private key. 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 [12]. For finger print matching is used Software Development Kit (SDK) of Neurotechnology.

4 Conclusion

The developed architecture is the most expensive one, since it foresees for every polling station two redundant ARS, even in cases where these servers have to store few hundreds of records. Comparing the Kosovo 2010 parliamentary election expenses reported in [6] and current IT market prices for proposed architecture are presented in Fig. 7.

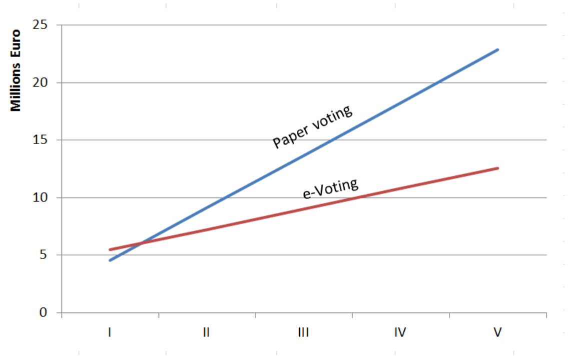

Fig. 7: e-Voting vs. paper voting cost

As cited in [1] the last national elections in Kosovo took more than two months, similar behaviors were noticed in region. Assuming that a polling station in average has 2000 voters, in Table 1 are presented estimated results of paper voting vs. measured results of e-Voting. E-Voting counting completes in 861 seconds.

Table 1: Counting efficiency in seconds

Description	Paper voting	e-Voting
Decryption	0 [s]	840 [s]
Counting and results	10,800 [s]	21[s]
Total time	10,800 [s]	861[s]

On the national level, these 746 polling stations data are summarized at the CCS and final election results can be displayed less than 900 seconds, thus the final result in total time can be published less than 30 minutes.

References:

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

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

[3] 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

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

[5] 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

[6] 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

[7] Blerim Rexha, Ehat Qerimi, Valon Raça and Haxhi Lajqi, Building governmental Certification Authority using OpenSSL, FLOSSK, Prishtina 2009

[8] 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

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

[10] 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.

[11] 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.

[12] Mattew MacDonald and Erik Johansson. C# Data Security Practical .NET Cryptography Handbook. Wrox Press Ltd. UK, ISBN = 1-86100-801-5, 2003.