A Case study on PKI: SERVE

The University of Auckland

Cheung Ling Kelly Yu

cyu024@ec.auckland.ac.nz

26th October, 2004

Abstract

The paper is base on the case SERVE (Secure Electronic Registration and Voting Experiment) which is an online voting system. PKI (Public Key Infrastructure) system has been introduced to SERVE in order to protect communications and identification. There are discussions on some online attacks (which may affect SERVE) and their mechanism. The paper discusses the performance base on how PKI deploy in SERVE. Security analysis about the PKI is also available in this paper. And conclude with the comment about the overall look of the PKI system in the SERVE case.

1. Introduction

PKI (Public Key Infrastructure) is a system that deals with identification and encryption. There are many security protocols in today which design under the PKI system. PKI system's elements are private key and public key (they are asymmetric key pair). Private Key is keep by the owner and public key distributes to the other people (public). PKI system is asymmetric encryption system. Data encrypted with private key can only decrypted with public key on the other hand data encrypted with public key can only decrypted with private key. That is how the PKI system does identification on each others and encrypts data. Digital certificate is an identification technology that base on PKI system. SERVE (Secure Electronic Registration and Voting Experiment) is an internet voting system experiment in U.S. SERVE's aim is to let American absentees which have difficulty to vote within U.S to be able to vote though internet. This is an interesting project since if this experiment is successful the SERVE may be legal to be a voting system in U.S. Some of the PKI technologies have been used in SERVE [1].The following paper is going to discuss about Where is the PKI system deployed in SERVE and what is the security problems that according to the SERVE about PKI system. How the PKI perform when it deploy in the SERVE system.

2. PKI in SERVE

2.1 Overall view of the voting system

Since "SERVE is an internet- and PC based system" [1], there are information transfers between the server and clients though the internet. All the transfers are protecting by Security Socket Layer (SSL) protocol [1]. The following figure (figure 1) and paragraph is going to explain how the Security Socket Layer protocol going to protect the transfers from the voter's web browser to the central server.

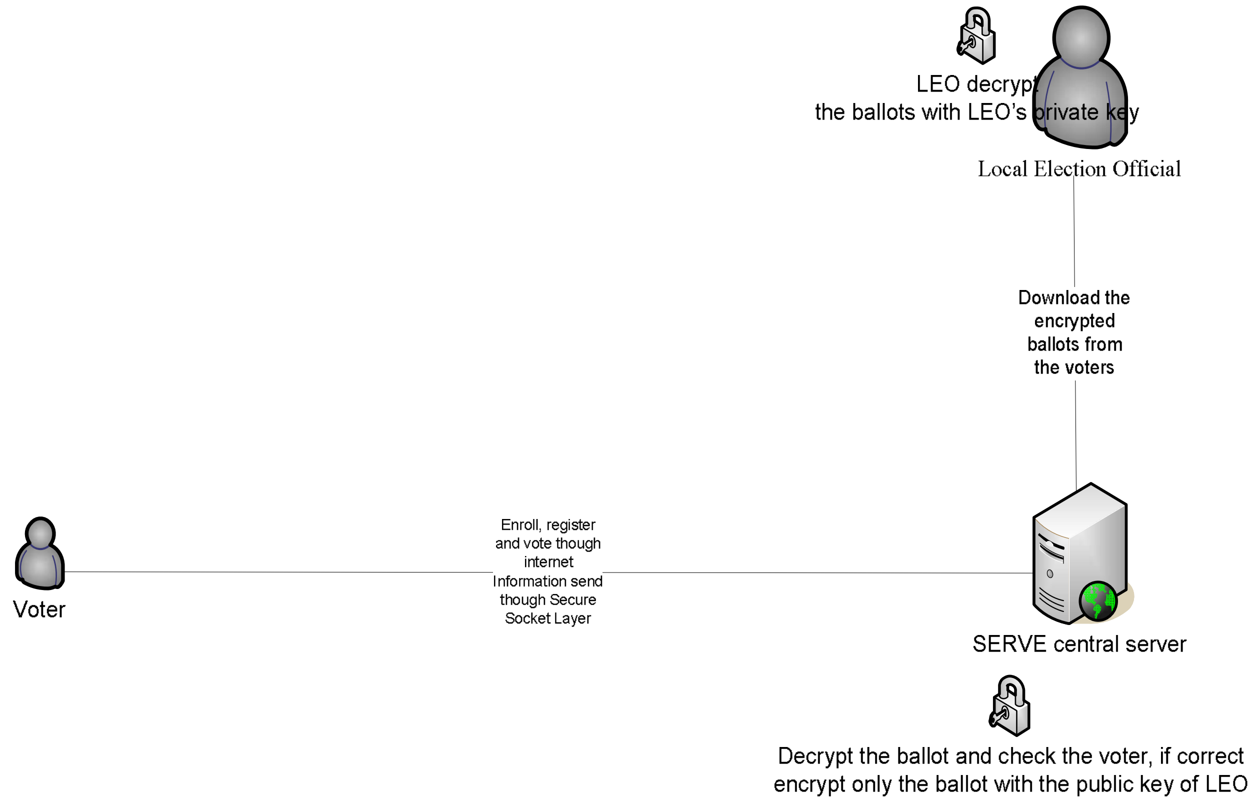

LEO decrypt the ballots with LEO's private key
Local Election Official
Download the encrypted ballots from the voters
Voter
Enroll, register and vote though internet Information send though Secure Socket Layer
SERVE central server
Decrypt the ballot and check the voter, if correct encrypt only the ballot with the public key of LEO

Figure 1: voting process

2.1.1 Connect to the server

At the beginning, voters will need to enroll to SERVE with the correct identification (e.g. military ID or citizenship and ID document face-to-face to a trust agent [1]). If the identification is correct, the enrollment process will be completed and SERVE can identify the voter.

2.1.2 The throw of the information

After the voters enrolled into the SERVE system and voters verified that is the correct SERVE central server. Voters should register to the central server to identify themselves. Then voters are eligible to vote [1]. The ballot information and the voter's identify information will send to the SERVE central server encrypted only SERVE central server can decrypt it. When it reaches the SERVE central server side SERVE central server will decrypt the information from the voter. After the information has been decrypted the SERVE central server will encrypt just the ballot with LEO's public key. The Local Election Official (LEO) will download the encrypted ballot and decrypt it with the LEO's private key.

2.2 Establish secure communication

2.2.1 Possible attack of the system.

The problem here is that how the voters can verify that is the correct SERVE central server rather than a fake central server. Attackers can confuse the voters and pretend themselves as the SERVE central server by spoofing or man in the middle attack. This can make the voters think they have voted but in fact they haven't [1]. Also how can the system avoid attackers in the middle read the message?

2.2.2 Deploy SSL in the system

The result of the vote can be affect by this kind of attacks. SERVE use SSL to protect the system [1]. In this case the SERVE central server will send its digital certificate to the voter's browser (see figure 2). The requirement of the SERVE is "The PC must run a Microsoft Windows operating system and either the Internet Explorer or Netscape web browser. [1]". Due to the browsers are only trusts the web server that its certificate is sign by a trust authority where it is in the trusted authority list [2], so in order for SERVE central server to be identify itself, it need to sign the certificate by an authority where it is in the trusted authority list of the web browsers or SERVE central server need to have some special approaches to let the voters able to recognize the certificate is from the

SERVE central server. If the SERVE central server's certificate's signer is in the trusted authority list of the web browser, the certificate will verify as trustable.

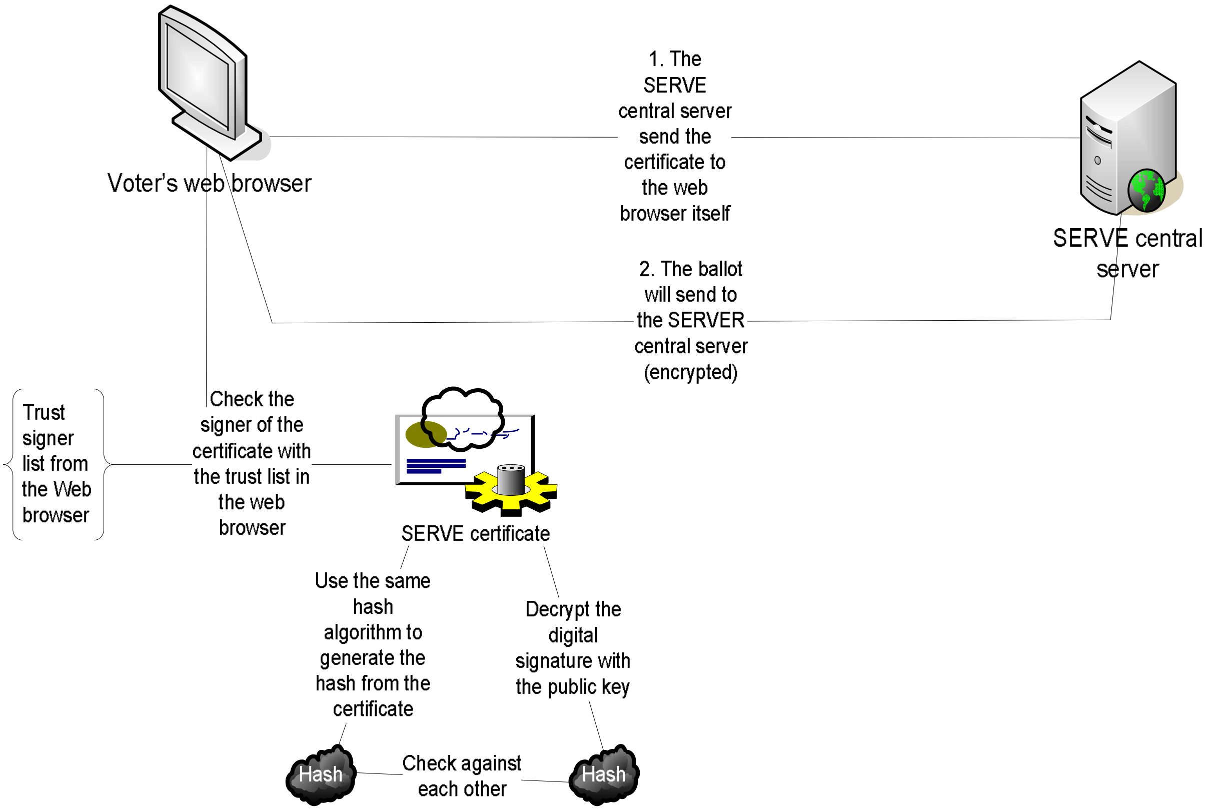
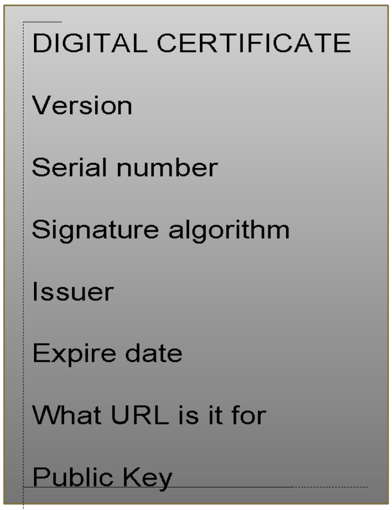

Voter's web browser
1. The SERVE central server send the certificate to the web browser itself
SERVE central server
2. The ballot will send to the SERVER central server (encrypted)
Trust signer list from the Web browser
Check the signer of the certificate with the trust list in the web browser
SERVE certificate
Use the same hash algorithm to generate the hash from the certificate
Decrypt the digital signature with the public key
Hash
Check against each other
Hash

Figure 2: SSL implementation between SERVE and Voter's browser.

2.2.3 Digital certificate (see figure 3)

Since the certificate is sent though internet, it is possible that attackers position himself/herself between the voter and the SERVE central server. The attackers can view and edit the certificate that send from the SERVE central server to confuse the voters. The way to protect this is from the certificate's digital signature. A hash is the output that computes the certificate by formulas or equations that is know as hash algorithm. The SERVE central server encrypts the hash (generated from the SERVE's certificate) by its private key. When the voter's web browser receives the certificate it will use the public key from the SERVE central server to decrypt the encrypted hash and compute the hash again from the certificate by the hash algorithm. Also as mentioned in the previous the digital certificate's signer have to be in the trusted authority list of the web browser in order to verify the SERVE central server. Therefore if the certificate's digital signature and public key have been modified, it will not be verify as SERVE central server according to the trusted authority list from the web browser. In this case if the two hashes are the same it means it is from the SERVE central server and it have not been modify by attackers in the middle. If the hashes are the same and the signer of the certificate is in the trusted authority list of the web browser. The web browser will then check the validity dates of the certificate (there is one field of the certificate state the expired date of the certificate see figure 3); if the certificate not expired. The web browser will then check the URL where the certificate downloaded from against the URL which is in the certificate identity information (there is field of the certificate state the URL information see figure 3). If the URLs are match and the certificate have not expired. It is the true SERVE central server.



DIGITAL CERTIFICATE

Version

Serial number

Signature algorithm

Issuer

Expire date

What URL is it for

Public Key

Figure 3: certificate look

3. Shortage of PKI in SERVE system

3.1 Potential vulnerability of the SERVE

Assume every user and staff (Certificate authority and internal officer) is good and not cheating the system. The communication of the SERVE system (the voters recognizes the SERVE central server by its digital certificate and send the ballot and registration information are encrypted before sent figure 1 and figure 2) is fine. Assume the encryption is strong enough the attackers which are in between the SERVE central server and voters are hard or costly to decrypt the message (it takes 3 million years to break the encryption when the key length is 1024 bits [2]). But this is not the real in today's word.

Those assumptions many not be always true. There are people do things they not suppose to do on the internet, for example attackers can play man in the middle attack and denial of service attack to the SERVE system [1].

3.1.1 Certificate revocation

In the SERVE central server need to revoke its certificate its not too hard and costly compare with revoke by CRL since the CRL's size get increase as more certificate get revokes [3] [4] (In the SERVE system ballots are protect under SSL and "The PC must run a Microsoft Windows operating system and either the Internet Explorer or Netscape web browser."[1], browsers are not check the certificates with the CRL it check the certificates with the trust list [2]). The SERVE central server just needs to revoke the old certificate and get a new one from the certificate authority [3]. When the voters connect to the SERVE central server a new certificate will send to the voters like figure 1. Voters will encrypt the ballots with the new public key from the SERVE central server. The old private key which has been comprised cannot decrypt the ballot which have encrypted by the new public key. But the problem is that the attackers can pretend as the SERVE central server and use the old certificate and private key. Also the attack can use the old private key to decrypt the old ballot if the attacker have act as man in the middle before and captured the encrypted ballot.

3.2 Attacks to the system

Although the SSL protocol is protecting the SERVE's communication between central server and voter's browser, but there are some problems with the communications in the SERVE case.

3.2.1 Man in the middle attack (see figure 4)

First, are all certificate authorities in the web browser's trust signers list trustable? One of the aims for SERVE is to help the Americans live in overseas to vote though the internet [1]. U.S is hard to know and effect what is happening inside those countries (oversea countries). For example, Country A's government can force the local ISP internet provider to block all connection to SERVE site. The ISP can also redirect all the people which go to the SERVE site to a site that looks similar to the real SERVE site (The fake site can have the same URL as the real SERVE central server since the ISP can work on it)and it is actually control by the Country A. In this situation as long as a certificate authority in the web browser trust list is helping country A and issue fake certificate to verify the fake SERVE site and the ISP changed the shown IP address of the fake site as the IP address of the real SERVE site to the real voters. In this case the voters will believe that they have already voted. Assume there is a careful voter he/she wants to check the vote stated (have he/she voted or not). He/she called someone in a safe internet environment (e.g. U.S) to check the vote form him/she. On the SERVE system it is only be able to check is a voter successfully voted or not by just register again then the SERVE will not allow the voter which have been voted to vote again, but cannot check who have the voter's vote [1]. Since the attacker have pretended the voter to vote (may be modified). The SERVE will show that it has been successfully voted.

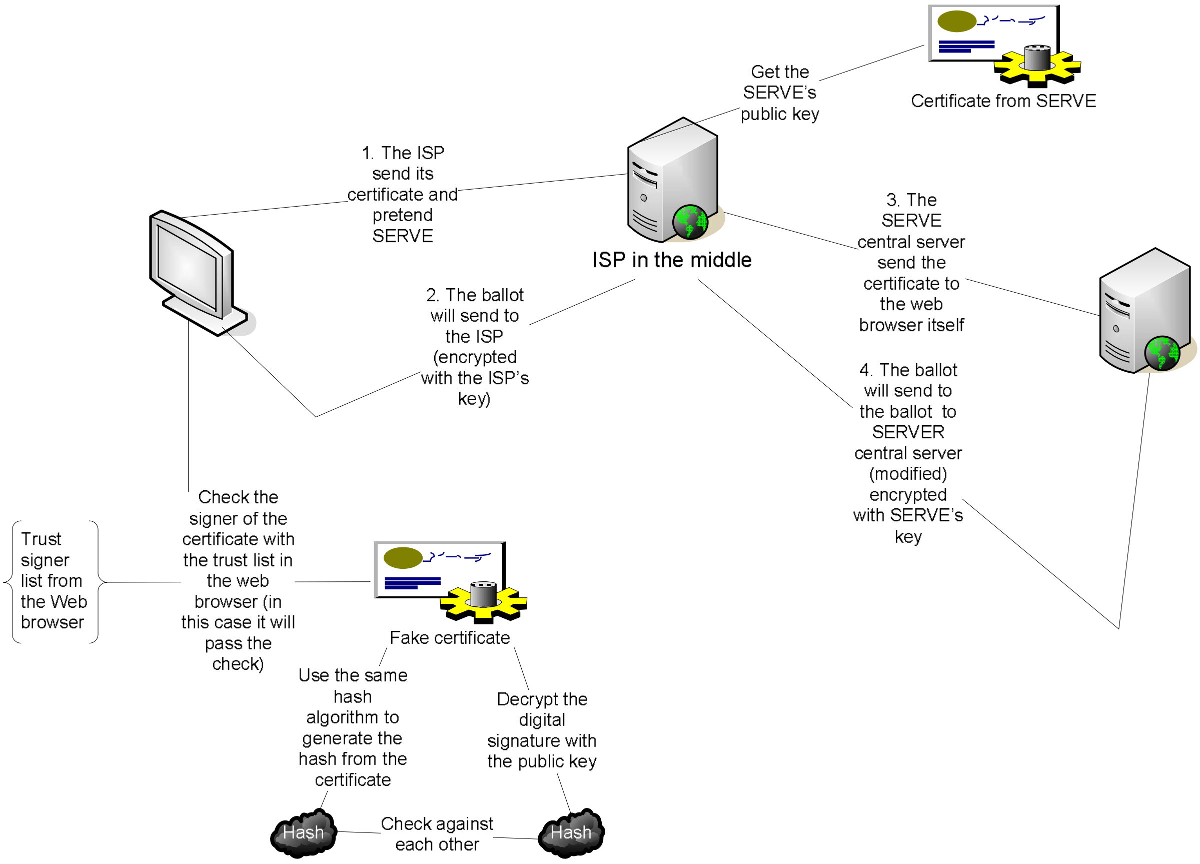

Get the SERVE's public key
Certificate from SERVE
1. The ISP send its certificate and pretend SERVE
ISP in the middle
3. The SERVE central server send the certificate to the web browser itself
2. The ballot will send to the ISP (encrypted with the ISP's key)
4. The ballot will send to the ballot to SERVER central server (modified) encrypted with SERVE's key
Check the signer of the certificate with the trust list in the web browser (in this case it will pass the check)
Trust signer list from the Web browser
Fake certificate
Use the same hash algorithm to generate the hash from the certificate
Decrypt the digital signature with the public key
Hash
Check against each other
Hash

Figure 4 example of country A

3.2.2 Denial of service attack

Denial of service attack is also a major shortage of the figure 1 as well [1]. SSL cannot prevent this kind of attack. In the SERVE case this kind of attack just trying to keep the SERVE central server too busy and cannot handle the correct operation. It is hard to identify which request of the certificate is from attackers. Although the system can set up some rules to restrict some IP address (which the system believe that this is from attackers) or not allow same IP address to frequently require for certificate (it cost the server's computation time). The attackers can first attack other computers in the world by some virus or Trojan horse software to form a "zombie network" [1]. This attack is not as hard as the previous example (country A). It does not require having full control of a large network but still can tremendously affect the performance of the system.

4. Security analysis

The following section is going to analysis the security performance of PKI in SERVE system.

4.1 Directory

4.1.1 Certificate authority (CA)

One of the problems which mentioned above is the certificate authority issue a certificate to the fake site. This come to the “which directory?” problem [3]. And in “Certificate Revocation and Certificate Update “[4] by Moni Naor and Kobbi Nissim give a definition of Certification Authority as “A trusted party (the CA should be trusted at least by the certificate acceptor), already having a certified public key, responsible for establishing and vouching for the authenticity of public keys, including the binding of public keys to users through certificates and certificate revocation.” [4] But in the SERVE system it mentioned in the man in the middle attack the attackers can “…fooling one of the certifying authorities, or simply purchasing a key. [1] “. Now the certificate authority is doing the correct things (technically), the certificate is really identifying the web server as the one this certificate is suppose to identify. The problem is that, the web server that a certificate authority is identifying may not be the web server that we are really wanted. In fact it may identify another web server but voters think that is the correct server. Also there are numbers of hard coded certificates in the browsers a user will not be notices unless they check the little lock at the bottom to see which certificate authority is signing this web server or check the list of the trust signer in the web browser. One of the interesting finding is that the users of the web browsers most of them do not know what is going on and just let the thing go [2]. And the certificate authority is running by company, a company’s aim is to maximize the profit .Therefore the certificate authorities may not be always trustable.

4.1.2 Certificate Revocation

Naor and Nissim mentioned that directories which stall the revocation information for certificate is not trustable. The directory may give wrong information to the users [4]. Peter Gutmann have mentioned the “which directory?” problem, since there is still no global distributed directory exist [3]. In SERVE “Which directory?” problem is not a serious problem. SSL have solve the “Which directory?” problem here as the voters is able to see where to get the certificate from and do not need to look for the directory and find the certificate of the SERVE server [3] [1]. But if the SERVE central server needs to revoke the certificate because the key have been compromise and the certificate is not yet expired. The old certificate may be use for a fake site since the private key has been compromise. In this situation how can the SERVE central server announce to all voters that the certificate has been revoked? It can either put the old certificate to the Certificate Revocation list (CRL put the revoked certificate's serial number. The certificate is sign by the certificate authority [2][3][4]) or notice all voters by email or some other notice method. To notice all voters may be very costly in terms of time and money. If SERVE chose the approach: to put the old certificate to the Certificate Revocation list, this comes to the "which directory?" problem (although the voter's web browser won't check the certificate with the CRL[2] but the voters can still be careful enough to check it by himself/herself if they can find the correct directory). The CRL have numbers of problems and disadvantages according to Peter Gutmann's papers and Gutmann strongly believe that CRL is a non-work approach. "That the use of CRLs violates the cardinal rule of data-driven programming which is that once you have emitted a datum you can't take it back.[3]" In Naor and Nissim's paper there is also mentioned some disadvantage to CRL, the only advantage that Naor and Nissim mention is the simplicity the scheme of CRL[4]. It is true that the CRL's mechanism is not designed very well, there are some problems that CRL is hard to solve, for example and the CRL is being update by the certificate authority to the directory with period. So that the time in between the period of upload the CRL is a flaw, since the server of the certificate need to wait until next period to let others know that its certificate have been revoke. Although this is the problem but if the CRL can update frequently enough this problem can still be minimize. Therefore as the frequency of the CRL update, the users can download a very up to date CRL therefore the freshness of the CRL is not a very big problem (but the cost of the certificate authority will increase and the internet's speed may not support [3]).

4.2 confidentiality integrity and availability (CIA)

4.2.1 Confidentiality

In the SERVE system, communications have been protected by SSL. People in between the SERVE and voter can only see some encrypted data and is unable to know what the meaning of the data, therefore the system have confidentiality. But the LEO is able to check the voter's vote [1] and if there are man in the middle attacks voters ballot may view by the attackers therefore the system loss the confidentiality.

4.2.2 Integrity

When the SERVE send its certificate to the voters in order to identify itself, the digital signature is encrypted and it is use to verify that the certificate have not be modified by anyone before it reach the voter's browser. In here we can see integrity since on one in the middle can modify the certificate. In the man in the middle attack example (country A) the voters vote can be modified therefore it loss integrity here.

4.2.3 Availability

In order to vote a voter has to first enroll to the SERVE and register. After these processes SERVE can recognize that this voter has been voted. So anyone who has voted the SERVE keeps a record somewhere. This shows the availability of the system. But the system can face the denial of service attack which can stop voters vote though the SERVE system therefore SERVE losses the availability under this attack.

Conclusion

The paper shows that the PKI system in the SERVE have numbers of weakness and cannot be solve recently. Although PKI system is working reasonable in commercial online systems [2] but online voting system and online commercial system is different [1]. On line voting system require more security and stable than online commercial system [1]. To build the SERVE security enough for legally use will be costly (bandwidth) and require good internal control (educate the voter deeply about the possible threats and what they need to be concern, certificate authorities and staff). In current technology there are restrictions to the system and the requirement of the system cannot be reach. Therefore even SSL (a protocol that use the PKI system and its use in the SERVE to protect the communication) is robust but it still cannot provide enough security to the SERVE system. In the future technology may be improve and the problems of the may be able to solve (the cost of SERVE to be security decrease and voter's education on the system be improve). But in the foreseeable future the SERVE system is still to danger to be legally used [1].

References:

[1] **D. Jefferson, A. Rubin, B. Simons, D. Wagner**, "*A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)*", 21 Jan 2004. Available: http://servesecurityreport.org/, February 2004.

[2] **Andrew Nash, William Duane, Celia Joseph, Derek Brink,** "*PKI implementing and managing E-Security*" RSA Press Published by Osborne/ McGraw-Hill, 2001

[3] **Gutmann,P**, "*PKI: it's not dead, just resting*" Published by IEEE, Computer , Volume: 35 , Issue: 8 , Aug. 2002

[4] **Naor, M.; Nissim, K.,** "*Certificate revocation and certificate update*" Selected Areas in Communications, IEEE Journal, Volume: 18, Issue: 4, April 2000