

# Safeguarding the 2010 Elections with Digital Signatures

Pablo Manalastas, PhD  
Department of Information Systems & Computer Science  
Ateneo de Manila University, Katipunan Avenue, Quezon City 1108  
**Email:** <pmanalastas@ateneo.edu>, <pmanalastas@acm.org>

April 2009

President GMA has just signed the 11.4 billion peso supplemental budget that will enable the full computerization of the May 10, 2010 national and local elections. The Commission on Elections (Comelec), in turn, has published the terms of reference or “*Request for Proposal 2010 Elections Automation Project*” (RFP) which will guide the vendors in their bids to supply computer and communications equipment, election software, training of Comelec personnel, and management of the entire election process. The amount of 11.4 billion pesos is not a small amount of money, and is probably the biggest budget for an IT project ever undertaken in the entire IT history of the Philippines. Why the important players like computer-IT companies, communications companies, software houses, government IT agencies, the academe, and local computer organizations, were not consulted in the design of this all-important IT project is incomprehensible. Even more incomprehensible is why an IT person was not appointed to the Comelec at a time when the Comelec needed an IT expert among its commissioners.

All preparations have been made, no matter how inadequate, and Comelec will push through with fully computerized 2010 elections. All that we can do is be vigilant and make sure that Comelec does not squander its humongous budget.

## Computerized 2010 Elections: Voting & Counting at the Precincts

Section III-3 of the RFP specifies how voting will be done using the Precinct-Count Optical Scan (PCOS) voting machines. “*One PCOS unit shall be installed in the polling place for voting purposes. Five established precincts shall be clustered to use one PCOS unit. The voter shall indicate his vote by marking the space provided on the ballot opposite the name of his candidate of choice.*” If you do not vote for any candidate for a position or if you vote for less than the required number for the position (called under-vote), that is allowed, and only choices made will be counted. If you vote for more candidates than permitted for a position (called over-vote), your votes for that position shall not be counted. If you vote for the exact number of candidates for a position, your vote will be counted. “*The voter shall feed his voted ballot personally into the PCOS unit.*”

Putting the PCOS voting machines in the precinct area, and allowing the voter to feed his ballot personally into the PCOS unit gives the voter the confidence that his vote will be counted. However, the RFP should have included the provision: “*When the voter personally feeds his ballot into the PCOS unit, a hooded LCD display terminal shall show to the voter the names of the candidates that he voted for, in order to show the voter a summary of his votes, and to give assurance that his votes are **correctly** counted by the PCOS. The purpose of the hood is to make his votes visible to the voter alone, thereby providing secrecy of his vote*” However, the RFP does not include this provision, and is a serious omission in the RFP.

Section III-4 of the RFP specifies the counting, consolidation, and generation of the (clustered) precinct election return (ER): “*After the close of polls, the Board of Election Inspectors (BEI) shall execute a closing-of-polls function in the PCOS unit to indicate that the counting and consolidation*

*application may be executed automatically by the system. Immediately after the precinct results consolidation, the system shall automatically generate and print the ER, in eight (8) copies, in the format specified by the Comelec. The BEI shall physically sign and affix their thumbprints on all copies and on all pages of the ER. The BEI shall post one (1) copy of the ER in the polling place, and shall announce the results of the voting in the (clustered) precinct by reading from another copy of the ER. The BEI shall digitally sign and encrypt the internal copy of the ER (computer softcopy of the ER in the hard disk filesystem of the PCOS unit). The BEI shall execute a function in the (PCOS) system to electronically transmit (the computer softcopy of) the ER, together with the precinct statistical report and the PCOS unit's audit log report to the following destinations: city/municipal Board of Canvassers (BOC), provincial BOC, national BOCs of Comelec and Congress, dominant majority party, accredited citizen's arm, and KBP, and central (Comelec) server.”*

These provisions in the RFP are the most controversial provisions, and details of many of these provisions have to be elucidated by the Comelec. The digital signing of the ER by the BEI and electronic transmission are specified here because these are required by the Amended Automated Election System (AES) Law, RA 9369. Furthermore the law specifies that the digitally signed electronically transmitted precinct ER shall be the basis of canvassing of votes, not the printed hardcopy of the precinct ER. The requirement of digital signing of the ER by the BEI has prerequisite infrastructures based on public key cryptography. Let me explain public key cryptography and how it is related to digital signatures.

### **Uses of Public Key Cryptography**

Public key cryptography (PKC) is used for two purposes.

First, PKC is used by individuals to *digitally sign* computer documents (files). Paper documents can be signed with pen and ink; computer files can not, and so the E-Commerce Act (RA 8792) has prescribed a way for computers files to have numerical data added to the end of the file (suffix data) that is legally acceptable as a signature. If an individual signs a paper document with pen and ink, scans the document to produce an Adobe Acrobat image file (PDF file) of the paper document, then the resulting PDF image file does not constitute a digital signature. Digital signatures are not at all related to handwritten signatures, but instead are numerical data added on to the end of computer files, and are based on PKC as their mathematical and legal justification. Details of the digital signature process will be explained below.

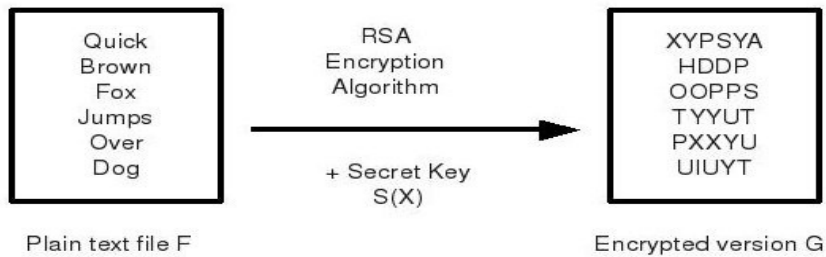
Second, PKC is used to *encrypt* computer files that can be *decrypted* only by the intended recipient. Simply put, to *encrypt* a computer file is to make difficult mathematical transformations of the file to make it unreadable. Similarly, to *decrypt* an encrypted file is to convert the file to the original readable form. Details of encryption/decryption based on PKC will be explained below.

### **PKC: Secret Keys & Public Keys**

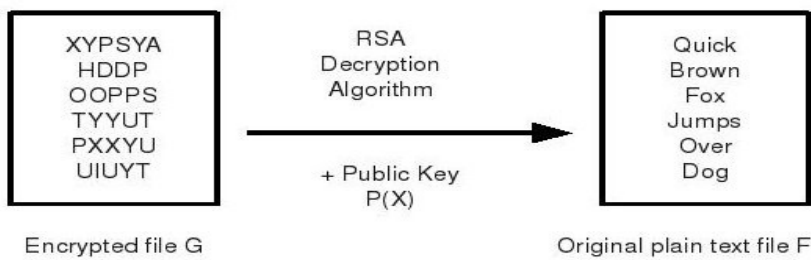
A person X who needs to send or receive confidential files in encrypted form has to generate two sets of numbers, a secret key S(X) and public key P(X), using a computer program called SSL, which stands for Secure Sockets Layer. The SSL program is built into most browsers like Internet Explorer or Firefox, so most computers already have the SSL program. These two keys S(X) and P(X) work in pairs, if one key is used to encrypt, the other key is needed to decrypt. The SSL program can generate a great number of secret key – public key pairs, so that in general no two persons using the SSL program will have the same secret key – public key pairs.

## Person X Uses Own Secret Key S(X) to Encrypt Files for Others

Person X can use his secret key S(X) to encrypt a plain text file F that he wants to send to another person Y. Encrypting file F produces file G which he sends to Y.

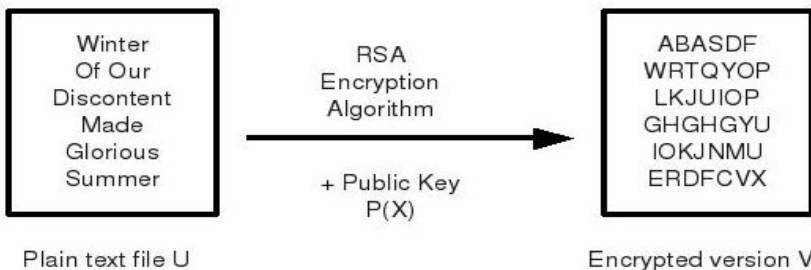


Upon receiving the encrypted file G, Y can decrypt the file G using the public key P(X) of person X, to get back the plain text file F.



## Other People Can Use X's Public Key P(X) to Encrypt Files for X

For the reverse communication, person Y can use the public key P(X) of X to encrypt a plain text file U that he wants to send to X. Encrypting file U gives file V, which Y sends to X.



Upon receiving file V, X can decrypt the file using his secret key S(X). Decrypting file V gives back the original plain text file U.



## Confidentiality of Secret Key

Legally, the secret and public keys are personal properties of the person who generated them using the SSL program. In particular, person X's secret key S(X) is confidential personal data that X has to keep secret, much like his banking PIN or his Swiss bank account number. The person X's public key P(X), on the other hand, has to be publicized to the whole world so that anybody who wants to

send him encrypted files can do so.

The secret key  $S(X)$  and the public key  $P(X)$  are mathematically generated using complicated prime number computations, so that even if  $P(X)$  is known to everyone, it will take years for anyone to compute the value of  $S(X)$  from  $P(X)$  using today's very fast computers.

A system that uses secret keys and public keys is called a Public Key Cryptosystem (PKC). The PKC described here conforms to the requirements of the E-Commerce Law (RA 8792) for legally acceptable electronic digital signatures, and to the requirements of the Amended AES Law (RA 9369) for digital signatures on the softcopy ER. We describe digital signatures below.

### **Digital Certificates and Certificate Authorities**

In a community where every person  $X$  has his own secret key  $S(X)$  and his own public key  $P(X)$ , a person whose real name is Juan Reyes can claim that he is Pablo Santos with public key  $P(\text{PabloSantos})$ . Now everyone can send encrypted files to Pablo Santos using public key  $P(\text{PabloSantos})$ , but in reality, it is Juan Reyes who is receiving the files and decrypting them correctly. Such misrepresentation, or assumption of another person's identity, can arise. To prevent such misuse of public keys, we need a trusted authority who will certify that the person Pablo Santos with public key  $P(\text{PabloSantos})$  has presented to the trusted authority, documentary evidence that he is really Pablo Santos, and not some other person, so that you can trust that public key  $P(\text{PabloSantos})$  truly belongs to the real Pablo Santos. A person needs to prove his identity to the trusted authority, before the trusted authority can certify to the community that public key  $P(\text{PabloSantos})$  really belongs to Pablo Santos. Pablo Santos needs to present documentary evidence like GSIS/SSS picture ID, a valid passport, company ID card with picture, and other documentation. The trusted authority who will certify that Pablo Santos presented documentary evidence that he is actually Pablo Santos and that public key  $P(\text{PabloSantos})$  belongs to him, that trusted authority is called a *certificate authority*, or *CA* for short. After satisfactory documentary proof of identity, the CA can then issue to Pablo Santos a *digital certificate* (a computer file) with the name Pablo Santos, the public key  $P(\text{PabloSantos})$ , and a statement that public key  $P(\text{PabloSantos})$  belongs to Pablo Santos. The digital certificate of Pablo Santos is not exactly like this, but this serves as a reasonable description for the layman of what a digital certificate is. The CA also publishes the public key of Pablo Santos on its website so that anyone can download Pablo Santos's public key. Actually the CA publishes all the public keys of all people that the CA has certified. Pablo Santos, by himself, can send by email his digital certificate to all his friends and associates.

### **Computerized 2010 Elections: Digital Signature on the Precinct ER**

Here we describe a working model for a digital signature scheme for the 2010 elections.

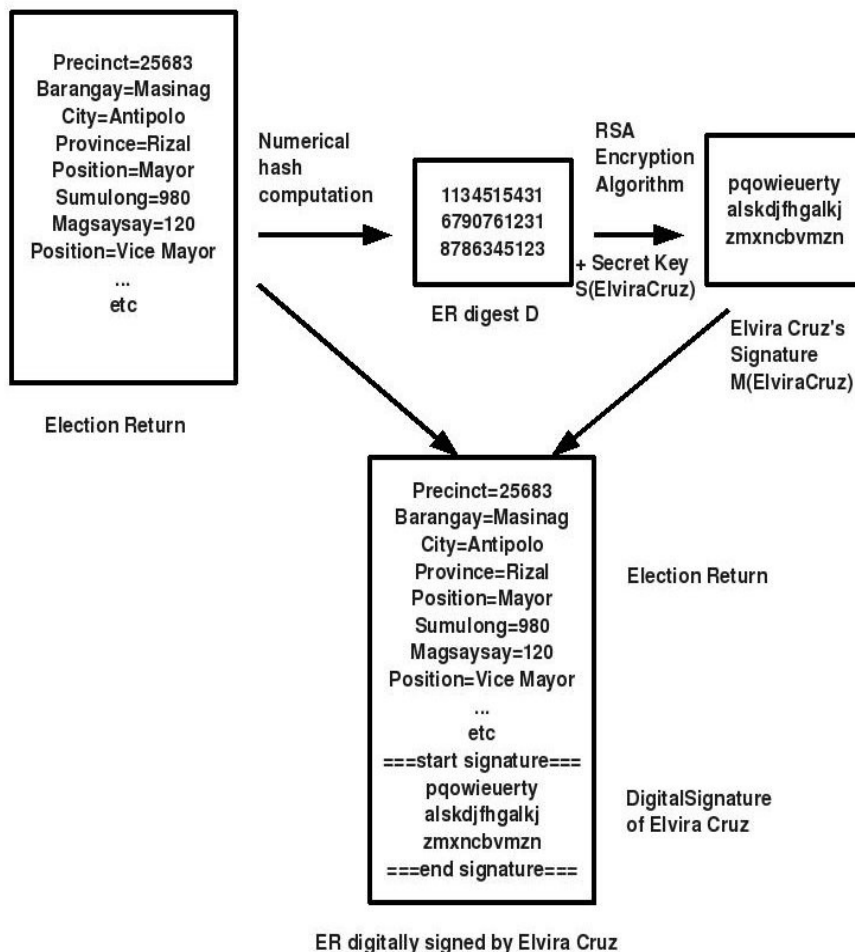
Let us say Elvira Cruz, a public school teacher is assigned as BEI personnel for Precinct 25683-25687 in Barangay Masinag, Antipolo City, Rizal Province. Elvira Cruz has her secret key  $S(\text{ElviraCruz})$  and digital certificate containing public key  $P(\text{ElviraCruz})$  in a smart card tied to an ID necklace that she wears around her neck. The smart card and ID necklace were bought by Comelec and given to her to be used for saving a copy of her secret key and digital certificate. Her digital certificate was issued by Comodo, a certificate authority that issues free certificates that are used for encrypting email. Elvira Cruz, like all the other public school teachers who are serving during the 2010 elections as BEI personnel, has already sent her digital certificate to Comelec via email, and so Comelec has a database of more than 160,000 digital certificates of public school

teachers serving as BEI personnel, and the digital certificates of the accredited precinct watchers and party representatives. These database contains the certified public keys of all signatories to the softcopy precinct ER, and is accessible to all the municipal BOC, provincial BOC, Comelec BOC, Congressional BOC, Namfrel, KBP, etc.

At the end of the voting period on election day, 2010, the Comelec RFP specifies:

*“After the close of polls, the Board of Election Inspectors (BEI) shall execute a closing-of-polls function in the PCOS unit to indicate that the counting and consolidation application may be executed automatically by the system. ... The BEI shall digitally sign and encrypt the internal copy of the ER (computer softcopy of the ER in the hard disk filesystem of the PCOS unit).”*

The PCOS program will count and consolidate all the votes for each candidate in the precinct, from the ballots that have been fed into the PCOS unit by the voters themselves, and the PCOS program will generate a softcopy ER file. From the generated softcopy ER file, the PCOS program will compute a numerical value called an *ER digest*. The ER digest, which we designate as D, has the property that if the ER contents are changed in any way (say by dagdag-bawas) then the ER digest D will also change. The PCOS program will now prompt Elvira Cruz to insert her smart card into the smart card reader, Elvira Cruz types in her passphrase or PIN to allow the PCOS program to read Elvira Cruz's secret key, S(ElviraCruz), from the smart card. The PCOS program will now encrypt the ER digest D with Elvira Cruz's secret key, and convert the encrypted ER digest into printable form M. Finally M will be appended to the end of the softcopy ER file. This softcopy ER file with M appended to the end of file (where M is the ER digest D encrypted with Elvira Cruz's secret key S and converted to printable form), is called the *digitally signed ER*. The appendix data M is called Elvira Cruz's *digital signature*.



Each signatory X to the softcopy ER will convert the ER digest D using his secret key S(X) to a digital signature appendix data M(X). The file that will be transmitted by the PCOS program is

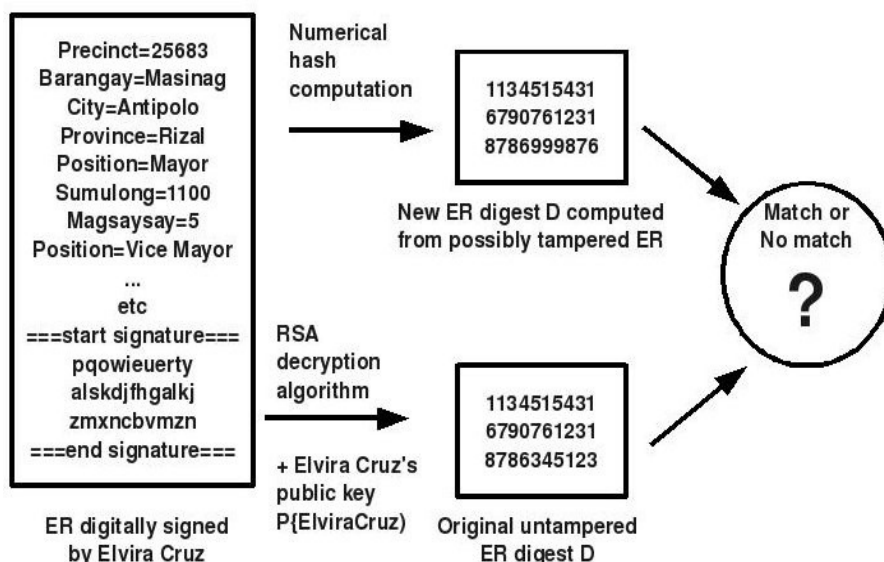
**Softcopy ER file format:** (softcopy ER) + M(X1) + M(X2) + ... + M(Xk)

where the Ms are the digital signature appendix data of all the BEI personnel, the watchers, and the party representatives.

For purposes of preserving verifiability of correctness of precinct results, this softcopy ER file format must be preserved even after successful transmission and verification of correctness in the destination computers. The signatures must be kept intact at the bottom of each of the 80000 softcopy ER files that Comelec will receive and store in its central database. At each canvassing stage (municipal, provincial, Comelec national, Congressional), the signatures need to be verified in order to prove that the ER's and COC's are not tampered with.

### Verification of Non-Tampering of ER

If the softcopy ER file is changed in any way, for example by dagdag-bawas, then the new ER digest E computed after the dagdag-bawas, will be different from the ER digest D computed before the dagdag-bawas. Now the original ER digest D was prevented from tampering by being encrypted with the secret keys S(X1), S(X2), ..., S(Xk) of each signatory, to produce the appendix data signatures M(X1), M(X2), ..., M(Xk). The original ER digest D can be retrieved from these appendix data by decrypting them using the public keys P(X1), P(X2), ..., P(Xk) of the signatories that are available from the Comelec database. Thus the original untampered ER digest D can be computed back from the signatures. If the ER digest computed from the softcopy ER file is the same as the original ER digest D as decrypted from the signatures using the signatories's public keys, then the softcopy ER file is not tampered and so can be used in further canvassing. If the two values do not match, then the softcopy ER file has been tampered with.



In case tampering has been proved by the above computation, then Comelec must order a retransmission of the original untampered digitally signed softcopy ER file from the PCOS machine. This retransmission can be done at computer communications speeds and should take only seconds.

## **Advantages of Digitally Signed Softcopy ER**

The Amended AES Law, RA 9369, specifically states that the digitally signed electronically transmitted softcopy ER file shall be the basis of canvassing at the municipal, provincial, Comelec, and congressional levels. This provision was placed in the law for several very important reasons.

First, the digitally signed softcopy ER file, is already in computer-readable format, and so there is no need to retype the precinct ER into the canvassing computers. There will be no data transcription errors.

Second, as mentioned above it is possible to confirm that the softcopy ER file is either tampered or untampered. If the ER file is proved to be tampered, then retransmission of the original untampered ER file can be ordered by Comelec, and retransmission can be carried out quickly at computer communications speeds.

Third, the identity of the BEI signatories of the softcopy ER file can be quickly established (in a few seconds) from the digital signatures, and the responsibility for the authenticity of the softcopy ER file can be quickly assigned to the correct people. Contrast this with paper and pen ER results, where either the signature on paper or the name on paper of the BEI personnel could be difficult to read, or may in fact be forged.

Fourth, it takes only minutes to electronically transmit and process 80,000 softcopy ER files from the local precincts via the Internet using commercial carriers (Globe, Smart, Sun, etc) to a central server in the National Comelec offices. But it may take months to transmit by human courier and process by hand 250,000 paper ER results. This gives the advantage that an election protest at the national level will take only minutes to resolve, as compared to the present manual system which may take years to resolve.

## **Is Comelec Ready to Implement Digital Signatures on the Softcopy ER?**

A reading of the Comelec RFP does not give any indication of Comelec's ability to implement a legally valid digital signature system for BEI personnel. The budget presented by Comelec to the Senate on February 2009 does not include the cost of digital certificates for BEI personnel, or the cost of purchase of media (smart cards, USB sticks, CDrom) to store the personal private keys and digital certificates of each BEI personnel. An interview with a Comelec commissioner reveals that the Comelec might actually depend on the vendor who will get the computerization contract to implement the vendor's version of a digital signature system.

An interview with three of the vendors by this author further reveals that for reasons of efficiency and lack of time, the winning vendor will issue digital certificates to unnamed precinct personnel for each of the 80,000 clustered precincts. That is, a secret key  $S(X)$  and a public key  $P(X)$  will be generated for each person  $X$  who will man each of the 80,000 clustered precincts, where  $X$  will not be identified by name, but by position in the precinct. For example, on election day, the vendor will issue for precinct number 25683 in Barangay Masinag, Antipolo City, Rizal Province, a secret key  $S()$  and public key  $P()$  to the following personnel: BEI-1, BEI-2, WATCHER-1, WATCHER-2, PARTYREP-1, PARTYREP-2, etc. So public school teacher Elvira Cruz assigned as BEI-1 to precinct 25683 will not generate her own secret key  $S(\text{ElviraCruz})$  and her own public key  $P(\text{ElviraCruz})$ , but will instead be given a secret key  $S(\text{BEI-1})$  and a public key  $P(\text{BEI-1})$  that has been previously generated for her by the vendor. The vendor of course knows Elvira Cruz's secret key  $S(\text{BEI-1})$ , since the vendor generated this for her. But Elvira Cruz's secret key is her private

personal confidential data that is her obligation to keep secret and unknown to everyone but her. Any participation of the vendor in the preparation of digital certificates (secret keys and public keys) for for BEI personnel, precinct watchers, and party representatives, will be illegal and immoral.

Also, there will be too little time for the vendors to secure proper digital certification for each of the more than 160000 BEI personnel who will be signatories in the 80000 softcopy precinct election returns, since the final list of teachers that Comelec will deputize for election duty will not be available until very near election time. This list will not even be final, since there will be last-minute changes in assignments when teachers get sick or give some other reasonable excuse for absence. But as I mentioned above, any participation of the vendor in the preparation of personal digital certificates for BEI personnel is illegal and immoral. This is the job of the BEI personnel himself, possibly with the help of Comelec.

The public school teachers can apply for personal digital certificates with existing certificate authorities like Verisign, Thawte, Entrust, etc., but the teacher can not afford the cost of certification, and there will not be enough time to submit documentary proof of identity, since these agencies are based abroad.

The E-Commerce Office of the Department of Trade and Industry (ECO-DTI), in cooperation with the Commission on Information and Communications Technology (CICT) and the Korean Office of International Cooperation (KOICO), is working to establish a National Public Key Infrastructure, which will be a national certificate authority. Unfortunately, the National PKI will not yet be up and operational by election day, 2010.

So I propose here a temporary process for digital certification of teachers in preparation for the May 10, 2010 elections, that will be completed in time, and with minimal cost for Comelec.

### **Proposal for Digital Certification of BEI Personnel**

For purposes of Comelec duty, each teacher who may be deputized as BEI personnel, even if he has never been deputized before, will secure an email address from Yahoo, Gmail, etc. The email address must be the full teacher's name with an optional numeric suffix. For example, Elvira Cruz should get the email address elviracruz@yahoo.com, elvira.cruz@yahoo.com, elvira\_cruz@yahoo.com, or elviracruz123@yahoo.com, whichever address is available or not yet taken by another Elvira Cruz. The important thing is that Elvira Cruz must have her full name (with an optional numeric suffix) as her email address. She must not use an email address like beautifulgirl@yahoo.com that does not give any indication of her true name. Also, she must do this as soon as possible, long before the May 2010 elections.

Let us say that Elvira Cruz finally got the email address elviracruz123@gmail.com. Next she must apply for a free email certificate from one of the certificate authorities (CA) that give out free email certificates. There are several such, and here are a few:

[http://www.comodo.com/products/certificate\\_services/email\\_certificate.html](http://www.comodo.com/products/certificate_services/email_certificate.html)

<http://www.thawte.com/secure-email/personal-email-certificates/>

The email certificate that these CA's will issue to Elvira Cruz will certify that the email address elviracruz123@gmail.com exists and that public key on the certificate belongs to that email address. It will not certify that the public key belongs to Elvira Cruz, because Elvira Cruz has not given to the CA documentary proof of her identity. This email certificate will normally be given for free,

and will be available very quickly, almost immediately after the application of the teacher is received online by the CA. Nevertheless, Elvira Cruz must apply for email certificate a little after May 10, 2009, since the email certificate will be valid for a year, so it will be good during the May 10, 2010 elections. Upon receiving her email certificate, usually via email, Elvira must store this certificate in the private certificate store of her browser. This certificate store can be accessed by clicking in the Firefox main menu, on Edit → Preferences → Advanced → Encryption → View Certificates → [Certificate Manager] Your Certificates. While in the [Your Certificates] tab, Elvira should save her email certificate to an external file on disk or in a USB memory stick. The external file should be named *elvira\_cruz\_email\_certificate.pk12*, which is a file in PKCS12 format for digital signatures,

The next step is to attach to this email certificate (given to *elviracruz123@gmail.com*) the identity of Elvira Cruz, such that the attachment of identity will be acceptable to Comelec, and to the entire Filipino nation, who must accept that the digital signature on the softcopy ER file is truly the digital signature of the real Elvira Cruz, public school teacher and deputized BEI personnel for Precinct 25683-25687 in Barangay Masinag, Antipolo City, Rizal Province. The fastest and most trivial way to do this is for Elvira Cruz, on receiving her deputization papers from Comelec, (1) to put her handwritten signature on the deputization paper, (2) scan this signed deputization paper to produce a PDF file, (3) email this PDF file to Comelec using her email address *elviracruz123@gmail.com*, and (4) digitally sign this email to Comelec. This four-step procedure will accomplish three things. (a) It will tell the Comelec that Elvira Cruz is accepting her appointment as BEI personnel, (b) It will confirm to Comelec that Elvira Cruz is using the email address *elviracruz123@gmail.com*, (c) the email that is digitally signed by *elviracruz123* will provide Comelec with a copy of the public key of *elviracruz123* as certified by a CA that is independent of the Comelec and the vendor implementing computerization of elections.

This way, Comelec can collect all the certified public keys of all the signatories to the softcopy ER file from all the 80000 clustered precincts in the May 2010 elections. In turn the Comelec can make this database of public keys available for download by all the BOCs, Namfrel, KBP, etc.

### **Vendor Support for SSL Digital Signatures**

The counting and consolidation programs running on the PCOS units assigned to the precincts, and the canvassing programs assigned to the municipal, provincial, and national BOCs, must support SSL digital signatures, because after each counting-consolidation on the PCOS units, or canvassing on the BOC units, the signatories to the output document (ER, COC, etc) must digitally sign the documents. The vendor programs should use the OpenSSL suite of security programs, which is the industry-standard for SSL encryption/decryption/signing.

### **Source Code Review of Computer Programs of Vendor**

The requirement of vendor-conformity with the provisions of RA-9369, as far as computer programs is concerned, is the reason for the source-code review provisions of RA-9369. Source code review means that the programmers hired by the vendors to write the computer programs for the May 2010 elections must do a line-by-line walk-through of their programs and mock data with an audience consisting of the programmer community of the Philippines, representatives from Comelec, and representatives from the political parties, etc. This source code review is required by RA-9369, and its absence in the Comelec RFP and in the Comelec schedules for Election 2010 is extremely suspicious, and is bordering on impeachable action on the part of Comelec. Comelec must schedule this source code review so that Filipino programmers can see the code and convince themselves that

the programs will work correctly. If programmers do not believe in the computer programs of Comelec, how can the rest of the Filipinos believe in computerized elections?

### **Conclusion**

Comelec has very little time to prepare for fully computerized elections in May 2010. It may have the money, but it lacks the technical expertise needed to pull this exercise through to success. It needs all the help it can get, especially in the area of IT, at which it is weak, by its own admission. I hope that this paper clarifies that issue of digital signatures on softcopy ER files, which is required by RA-9369 in a computerized election exercise.