THE AUTOMATED ELECTION SYSTEM COMPLIANCE AND SECURITY ISSUE: DIGITAL SIGNING

Synopsis:

The 2010 National and Local Elections is the first in Philippine history as it was the first ever national and local election conducted using an automated election system. One of the missteps in election administration in this first ever Philippine automated election is the implementation of the digital signature. The two reasons proffered by the Commission of Elections (Comelec) in the way it implemented digital signing are (1) that the Poll Automation Law or RA9369 which amended RA8436 did not identify who will sign the election reports, and (2) that by limiting digital signing to the Chairman of the Board of Election Inspectors led to savings by at least a billion pesos. With regard to the reference to Republic Act 8792 or the Electronic Commerce Act which provides for the legal recognition of electronic documents and electronic signatures, the Commission insists that such reference is limited to the authentication provision of the said law.

The national and local election is imbued with public interest as it involves the free and democratic right of the electorate. No less than the Philippine Constitution mandates the protection of said right. The Constitution vests on the Commission on Elections the sacred task of upholding and protecting such right. By implementing digital signing the way the Commission did, can it be said that sacred exercise was amply protected? Did it ensure the authenticity of the election reports?

THE AUTOMATED ELECTION SYSTEM COMPLIANCE AND SECURITY ISSUE: DIGITAL SIGNING

The Election Laws

The Omnibus Election Code or Batas Pambansa 881 (BP881) mandates that the election returns be signed by the Board of Election Inspectors (BEI)[1] and the certificate of canvass be signed by the Board of Canvassers (BOC)[2].

Republic Act 9369[3] also mandates that the election returns[4] and certificates of canvass[5] be digitally signed for these election reports to be used to proclaim the winning candidates. Echoing this mandate, the Commission on Elections, in its "Request for Proposal for Solutions, Terms & Conditions for the Automation of the May 10, 2010 Synchronized National and Local Elections" (RFP-AES2010) specified that the BEI shall digitally sign the election return[6] and that the generated results at all levels of canvassing shall be digitally signed using the respective BOC's security keys.[7]

Bid Bulletin No. 10

The requirement for the digital signature was clarified in COMELEC's Bid Bulletin No. 10 (relating to RFP-AES2010) promulgated on April 15, 2009, to wit:

> "Question/Issue: The Consolidation and Canvassing System shall allow the BOCs to digitally sign all electronic results and reports before transmission. Please specify your requirements for the digital signature.
>
> "Answer/Clarification: The digital signature shall be assigned by the winning bidder to all members of the BEI and the BOC (whether city, municipal, provincial, district). For the NBOCs, the digital signatures shall be assigned to all members of the Commission and to the Senate President and the House Speaker.
>
> "The digital signature shall be issued by a certificate authority nominated by the winning bidder and approved by the Comelec."

Authentication of Certificates of Canvass and Electronic Signature

RA9369 incorporates with it by reference Republic Act 7166, "An Act Providing for Synchronized National and Local Elections and for Electoral Reforms, Authorizing Appropriations Therefor, and for Other Purposes", Republic Act 8792, "Electronic Commerce Act", and the rules promulgated by the Supreme Court.[8]

RA8792 provides for, among others, the legal recognition of electronic documents and electronic signatures.

RA7166 provides for the determination of authenticity and due execution of the certificates of canvass[9].

The Supreme Court's Rules on Electronic Evidence (REE) promulgated on July 17, 2001 and which came into effect on August 1, 2001 provide rules for the authentication of electronic documents as well as rules governing electronic signatures[10].

Technical vs Legal Considerations

At the core of this discussion are electronic document, electronic signature, and digital signature and the determination of authenticity and due execution of an electronic document and the authentication of electronic signature and/or digital signature and how these relate to the Election Returns generated by the voting and vote counting machine or the Precinct Count Optical Scan (PCOS) and the Statement of Votes (SOV) and Certificate of Canvass (COC) generated by the Canvassing and Consolidation System (CCS) laptops at all levels of canvassing. It is therefore necessary to discuss what these are as legally recognized under RA9369.

ER, SOV, and COC are Electronic Documents

RA8792 provides the following definition of an electronic document:

> f. **"Electronic document"** refers to information or the representation of information, data, figures, symbols or other modes of written expression, described or however represented, by which a right is established or an obligation extinguished, or by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored, processed, retrieved or produced electronically.

In the context of RA9369, the ER, an output of the PCOS, is generated electronically by detecting a vote mark on the ballot, crediting the vote to the correct candidate, and there after count the votes per candidate, such vote count recorded in the ER. RA9369 requires that the ER be digitally signed then electronically transmitted to the first level of canvassing or to the city or municipal canvassing center and the servers of the majority party, the dominant minority party, the KBP, and the accredited citizens' arm. The ER having been electronically generated and electronically transmitted meets the attributes of an electronic document. If an ER is digitally signed as required by RA9369, then that ER may be used as basis for the counting and consolidation of votes and as basis for proclamation of the winning candidates.

The SOV and the COC are generated by the CCS laptops at each stage of canvassing and consolidation. RA9369 mandates that the COC be digitally signed and thereafter transmitted to the next level of canvassing and consolidation. The SOV and COC having been electronically generated and electronically transmitted meet the attributes of an electronic document. If a COC is digitally signed as required by RA9369, then that COC may be used as basis for further vote consolidation and as basis for proclamation of the winning candidates.

The ER, SOV, and COC are electronic documents which are recognized as such by RA8792[11].

Electronic Signature

RA8792 provides the following definition of electronic signature:

> e. **"Electronic signature"** refers to any distinctive mark, characteristic and/or sound in electronic form, representing the identity of a person and attached to or logically associated with the electronic data message or electronic document or any methodology or procedures employed or adopted by a person and executed or adopted by such person with the intention of authenticating or approving an electronic data message or electronic document.

In putting this definition into the context of RA9369, it is necessary to consider the traditional definition of a (handwritten) signature and the technical definitions of electronic signature and digital signature:

> A signature is a stylized script associated with a person. It is comparable to a seal. In commerce and the law, a signature on a document is an indication that the person adopts the intentions recorded in the document.
>
> *http://en.wikipedia.org/wiki/Electronic_signature*

A digital signature is an electronic signature. But not all electronic signatures are digital signatures. Wikipedia provides the distinction:

> An electronic signature is any legally recognized electronic means that indicates that a person adopts the contents of an electronic message. The U.S. Code defines an electronic signature as "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."
>
> *http://en.wikipedia.org/wiki/Electronic_signature*
>
> A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery and tampering.
>
> Digital signatures are often used to implement electronic signatures, a broader term that refers to any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures.
>
> *http://en.wikipedia.org/wiki/Digital_signature*

RA8792 provides for the legal recognition of electronic signature[12]. Digital signatures being a special type of electronic signatures are consequently accorded legal recognition under the same law.

Digital Signature Execution and Verification and Related Technology

Digital signing and verification involves several elements: a pair of electronic keys (public key and private key), an infrastructure or an "Asymmetric or public cryptosystem" referred to as Public Key Infrastructure or PKI, and an information certifier or certificate authority who operates the PKI and issues a certificate of identity (digital certificate) to a holder of an electronic key pair.

Execution of a digital signature requires the use of an electronic key which only the signer knows. This type of electronic key is referred to as the signer's private key. Digital signing requires the use of a mathematical method which is provided in a signing program (software) that may be executed in a signer's computer.

Corresponding to a signer's private key is another electronic key referred to as the signer's public key. The signer may provide a copy of his public key to other parties for the purpose of verifying his digital signature.

Digital signature verification involves the use of the PKI operated by the certificate authority. As with digital signing, digital signature verification involves the use of a mathematical method made available in the PKI infrastructure.

The certificate authority's role starts when a signer applies for the use of the PKI infrastructure. The certificate authority conducts identity verification by asking the applicant to present identity documents, like an identification card with photo, passport, birth certificate or other similar identity documents. Depending on the level required identity certification, the certificate authority may go to the extent of conducting an investigation into the background of the applicant. Having met the requirements, the certificate authority then issues to the applicant an electronic [digital] certificate of identity. The applicant may then generate his private and public key pair.

A recipient of a digitally signed electronic document may then verify the signature of a signer using the public key of the signer and the PKI operated by the certificate authority. Verification causes the signer's electronic [digital] certificate of identity which provides the recipient-verifier the status of said electronic [digital] certificate of identity and other relevant information that will help confirm the recipient-verifier the identity of the signer.

A summary of terms relating to digital signature is provided in Annex A. Also, please refer to Annex B for an illustration of digital signature execution and verification.

Technology Specific

RA9369 is technology specific and mandates the use of digital signature which is executable with the use of "digital signature technology". COMELEC Bid Bulletin No. 10 which clarifies the requirement for digital signature provided in RFP-AES2010 refers to an entity called "certificate authority". Given that RA9369 incorporates with it RA8792 by reference, appreciation of digital signing should be based on RA8792, its Implementing Rules and Regulations, the Rules on Electronic Evidence, and other related rules and issuances that relate to "digital signature technology".

It should be noted that a certificate authority does not issue digital signatures, rather, it operates an infrastructure that provides a methodology which allows a person to execute a digital signature. It should be noted, too, that a certificate authority does not issue the public and private key pair. It is the person using the certificate authority's infrastructure who generates his own public and private keys. Bid Bulletin No. 10 reveals the level of (mis)understanding of digital signature technology by the COMELEC and Smartmatic/TIM. The COMELEC and Smartmatic/TIM could have been guided by the Electronic Commerce Act and related issuances.

Certificate Authority

A Certificate Authority is a neutral trusted 3rd party service provider. Even if Smartmatic/TIM has the capacity to operate as a Certificate Authority, it is not within its business charter to begin with. By being a party to the conduct and management of the AES and knowing the design complexities and intricacies the AES that it supplied the country, it should not even be considered as a service provider for digital signing. Perhaps the problem the Comelec and Smartmatic/TIM encountered is one that centers on cost if Comelec were to engage a legitimate Certificate Authority. About 500,000 digital certificates of identity will be required if all members of the BEIs and the BOCs were to digitally sign the election reports. The other stumbling block which hindered the proper implementation of the digital signature in the AES is it would require that the signing software be embedded together with the PCOS and CCS software which would call for another layer of customization. And, time was running out.

Digital Signature Implementation in the AES

On December 29, 2009 the COMELEC promulgated Resolution No. 8739, GENERAL INSTRUCTIONS FOR THE BOARD OF ELECTION INSPECTORS (BEI) ON THE VOTING, COUNTING, AND TRANSMISSION OF RESULTS I N CONNECTION WITH THE 10 MAY 2010, NATIONAL AND LOCAL ELECTIONS (ComRes8739), which provides among others:

ARTICLE V
PROCEDURES OF VOTING, COUNTING OF VOTES AND TRANSMISSION OF PRECINCT RESULTS

SEC. 33. *Preliminaries to the voting.* - The BEI shall meet at the polling place at six o'clock in the morning of Election Day and do the following:

a) Ensure that it has all the election forms, documents, and supplies needed including;

1) one (1) iButton security key for the chairman of the BEI for use in operating the PCOS; and

2) iButton security key and Personal Identification Number (PIN) for each member of the BEI for use to digitally sign the ERs before transmission.

iButtons will be found in the thermal printer compartment and the PINS will be in a separate envelopes (sic) found inside the PCOS box.

x x x

ARTICLE V
PROCEDURES OF VOTING, COUNTING OF VOTES AND TRANSMISSION OF PRECINCT RESULTS

x x x

SEC. 38. Counting of ballots and transmission of results; Procedure.

x x x

6. Thereafter, the PCOS shall automatically count the votes. x x x

c. Require for the digital signature of the members of the BEI. Each member shall insert his iButton security key intended for the digital signature in the iButton security key receptacle;

The foregoing quoted provisions of ComRes8739 indicates the following:

1. That an iButton security key in combination with a Personal Identification Number will be used to execute the digital signature
2. That each BEI member will have his/her own iButton security key and Personal Identification Number with which to execute a digital signature
3. That a separate iButton security key will be used to operate the PCOS, said key shall be used by the BEI Chairman.

Then on March 4, 2010, the COMELEC promulgated Resolution No. 8786, REVISED GENERAL INSTRUCTIONS FOR THE BOARD OF ELECTION INSPECTORS (BEI) ON THE VOTING, COUNTING, AND TRANSMISSION OF RESULTS IN CONNECTION WITH THE 10 MAY 2010, NATIONAL AND LOCAL ELECTIONS, (ComRes8786), which provides:

ARTICLE V
PROCEDURES OF VOTING, COUNTING OF VOTES AND TRANSMISSION OF PRECINCT RESULTS

SEC. 34. Prefiminaries to the voting. - The BE1 shall meet at the polling -
place at six o'clock in the morning of Election Day and ensure that the PCOS box and the ballot box are inside the polling place. (As revised)

x x x

e) Check whether the following are inside the PCOS box: (As revised)

I. Checklist of contents of the box;
ii. PCOS machine;
iii. Power cord of the PCOS;
iv. One (1) envelope containing spare iButton;
v. Three (3) rolls of official thermal paper;
vi. Three (3) PINS of the BEI;
vii. One (1) PIN for re-zeroing which shall remain in the PCOS box;
viii. Modem, if any*
ix. Two (2) copies of the Minutes

* There shall be at least one (1) Modem in every polling center.

x x x

m) Open the printer cover and the Chairman shall take out the iButton security key; (As revised)

x x x

SEC. 40. Counting of ballots and transmission of results; Procedure, (Renumbered) (As revised)

x x x

f) Thereafter, the PCOS shall automatically count the votes and immediately display a message "WOULD YOU LIKE TO DIGITALLY SIGN THE TRANSMISSION FILES WITH A BEI SIGNATURE KEY?", with a "YES" or 'NO" option;

g) Press "NO" option. The PCOS will display "ARE YOU SURE YOU DO NOT WANT TO APPLY A DIGITAL SIGNATURE?" with a "YES" and "NO" option;

h) Press "YES" option. A message shall be displayed "PRINTING 8 COPIES OF NATIONAL RETURNS. PLEASE WAIT";

x x x

The above-quoted provisions of ComRes8786 clearly indicate that:

1. A spare iButton security key is provided
2. A primary iButton security key, stored in underneath the printer cover presumably to be used to operate the PCOS machine is provided
3. The BEI members will each have a Personal Identification Number

It is to be noted, nay highlighted, that the revised general instructions to the BEI, ComRes8786, clearly instruct the BEIs to skip the execution of digital signatures.

The COMELEC also promulgated Resolution No. 8809 or the GENERAL INSTRUCTIONS GOVERNING THE CONSOLIDATION/CANVASS AND TRANSMISSION OF VOTES AT THE MUNICIPAL/CITY/PROVINCIAL AND DISTRICT BOARDS OF CANVASSERS IN CONNECITON WITH THE MAY 10, 2010 NATIONAL AND LOCAL ELECTIONS. Nothing in this resolution instructs the Board of Canvassers to digitally sign the Certificates of Canvass and Statement of Votes prior to transmission to the next level of canvass.

What prompted the change in the instructions to the BEI? Mr. Jose Armando R. Melo, Chairman, COMELEC, offered an explanation:

> "MR. JOSE ARMANDO R. MELO (Chairman, Commission on Elections). Yes, sir. When we were talking about this, the signature of the BEI chairman and the other members… it came about that... we were saying that the BEI people may be threatened or some of them may not report at all. So what will happen to the transmission? So we limited it to the actual signature of the Chairman. And the other members, we did not ask them to have a signature anymore because it will... the cost will come out to a more than a billion altogether."
>
> Transcript of Stenographic Notes
> Committee on Suffrage and Electoral Reforms
> May 20, 2010

The fears expressed by the COMELEC Chairman Melo that the BEIs might be threatened or might not show up are realities that election workers, watchers, and other parties had experienced in previous elections and, therefore, do not justify not enabling them to digitally sign the election returns. The matter could have been addressed with careful, meticulous planning, including the provision of the backup actions in the event that members of the BEI do not show up on election day.

As an aside, the explanation offered by Chair Melo with regard to the resulting savings merits further investigation. When did COMELEC make the determination that it will save at least PhP1bn by limiting the digital signature to the BEI chair? If the determination was made before the bid, then COMELEC had already chosen the technology to be used for the 2010 National and Local Elections. If it made the determination during the implementation of the chosen technology, shouldn't the contract price have been reduced to PhP6.2bn?

In the hearing conducted on May 19, 2010 one of the issues sought to be clarified was the provision of ComRes8786 that clearly instructed the BEIs to skip the execution of digital signing thereby leading the public to be believe that election returns generated from the PCOS machines did not bear the required digital signatures of the BEIs.

Responding for the COMELEC, Commissioner Gregorio Larrazabal testified that the digital signature was in the iButton security key *(erroneously recorded as "ipod" in the TSN)*:

> "MR. LARRAZABAL. It's not correct. Because each PCOS machine also has a signature. So, for example, you use a CF card in a particular PCOS when that machine... when that data is transmitted, it will tell us that that ... the data is transmitted using a particular PCOS machine. So, there is a way to audit whether or not a particular PCOS was used for that precinct.
>
> xxx
>
> "MR. LARRAZABAL. The digital signature was actually in the ipod that opens it and, as I mentioned, when a PCOS machine using a particular CF cards sends the data to the different servers, that server will tell us that this particular data was sent using a specific machine. So, it's not...So, every machine has a footprint that allows us to ...to de-verify if that machine was true enough used for that particular precinct."
>
> Transcript of Stenographic Notes
> Committee on Suffrage and Electoral Reforms
> May 19, 2010

With regard to the required digital signatures on the Certificates of Canvass Mr. Correia of Smartmatic/TIM testified that said Certificates of Canvass were signed "by tokens":

> "MR. CORREIA. The election returns.... I mean, you just mentioned actually the Certificate of Canvass and the Certificate of Canvass are indeed being signed in the CCS, in the Consolidation and Canvassing Stations by tokens that are assigned to the operators of the... in this case the Board of Canvassers. So, they are also digitally signed. All of the information that is being transmitted from the precincts to the municipal canvassing and all the way up to the national canvassing, it's being digitally signed.
>
> Transcript of Stenographic Notes
> Committee on Suffrage and Electoral Reforms
> May 19, 2010

The tokens referred to by Mr. Correia in his testimony are actually the USB security token[13] issued to each member of the Board of Canvassers.

Executive Director Jose Tolentino of the COMELEC testified:

> "MR. TOLENTINO. Thank you. I am Director Tolentino, Your Honor. When the law...when R. A. 9369 prescribed that election returns should be digitally signed, the law did not actually say that it should be the Board of Election Inspectors that should have their own digital signatures to digitally sign the election returns. So what COMELEC did was to ensure that all PCOS would have its own digital signature. That is what we will use to tell our consolidation and canvassing servers that the election returns being received by it come from a valid source. Now we were balancing security because there is a possibility that the BEIs might be coerced, they might suddenly lose their digital keys."
>
> Transcript of Stenographic Notes
> Committee on Suffrage and Electoral Reforms
> May 19, 2010

The fears expressed by Executive Director Tolentino that the BEI members might be coerced echo the same fears expressed by Chairman Melo.

Executive Director Tolentino further testified:

> "MR. LOPEZ. Yes. Mr. Chairman, the law says, *The election return transmitted electronically and digitally signed shall be considered as official election results and shall be used as the basis for the canvassing of votes and the proclamation of a candidate.*
>
> "THE CHAIRPERSON. I believe I have a lawyer. Jun Tolentino, please react to that on constitutional implications, not binding on you, by the way, because we just... this thing just came up today. Let's not make this binding on COMELEC.
>
> "MR. TOLENTINO. Sir, the provision cited, Your Honor, does not say that it is the BEI that should digitally sign the election returns. It just said...
>
> *Din*
>
> "MR. TOLENTINO. No, if you read it clearly...
>
> "THE CHAIRPERSON. Let him speak.

"MR. TOLENTINO. ...it just says that the election returns shall be electronically transmitted and digitally signed.

"THE CHAIRPERSON. Yes and the reference is the E-Commerce Act. But the E-Commerce Act defines what a digital signature is.

"MR. TOLENTINO. No, under Section 25, the E-Commerce Act referred to here, Your Honor, merely refers to the determination of authenticity and due execution."

Transcript of Stenographic Notes
Committee on Suffrage and Electoral Reforms
May 24, 2010

The Executive Director's testimony only confirmed that the BEIs did not digitally sign the election returns justifying that RA9369 did not actually specify that the BEIs be enabled to digitally sign the (electronic) election returns. In his testimony, the Executive Director emphasized that the reference to RA8792 is limited only to the determination of the authenticity and due execution.

While RA9369 does not explicitly state that the BEI members be the ones to digitally sign the electronic election returns and the BOC members be the ones to digitally sign the electronic certificates of canvass, it is to be noted that the law takes root from BP881. And that not all provisions of said BP881 were amended or repealed by RA9369. By legal tradition established by BP881, the BEI members sign the election returns and BOC members sign the certificates of canvass. The determination of authenticity and due execution of the election returns and certificates of canvass should have been guided by the pertinent provisions of RA8792 and the REE which involves, among others, the examination of the digital signatures of the members of the respective BEIs and BOCs that were required to be affixed thereon.

Mr. Renato B. Garcia, erstwhile member of the COMELEC Advisory Council and later Consultant at the Office of the Chairman, Commission on Elections, explained how digital signing was implemented:

"MR. RENATO B. GARCIA. (Professor, Office of the Chairman, Commission on Elections) Good afternoon po, Chairman, and Congressmen. It is true that the digital signature, as claimed by Lito Averia, as in the Ecommerce Law has talked a little bit about this, the update today is the fact that there is an Executive Order by the President, issued by the President, creating that certification authority that he mentioned. The certification authority in that Executive Order is to be set up by the Commission on ICT and the National Computer Center. This is not in place at this time; it has not yet been implemented. So what we have now in the system....

"Well, let me explain also further the iButton. The iButton is nothing but a chip, a memory chip. What is done is that the password or your PIN, as you would normally have, let's say, in your ATMs, would be now placed in the chip so that when you put that iButton or the chip, in effect, and touch the machine, it now reads the PIN or the password.

"THE CHAIRPERSON. And that chip is personal to the Chairman?

"MR. R. GARCIA. And that chip is unique for each and every Chairman and machine.

"THE CHAIRPERSON. Chairman and machine.

"MR. R. GARCIA. That's the way we have assigned it. So that is now... that iButton now becomes a personal key signature of both the BEI Chairman and the machine. It will not work in any other machine and with any other chairman, but that specific chairman...

"THE CHAIRPERSON. And what it does, as I was saying, is that it at least certifies that the information comes from that machine and no other?

"MR. R. GARCIA. Yes. And the Chairman himself, being the one controlling it, who is now putting that signature, in effect, of that Chairman into that machine which is done twice in the process. So under the entire process, the digital signature, in effect, of the BEI Chairman is there, including the transmission."

Transcript of Stenographic Notes
Committee on Suffrage and Electoral Reforms
May 20, 2010

The Executive Order referred to by Mr. Garcia is Executive Order No. 10 "INSTITUTIONALIZING THE CERTIFICATION SCHEME FOR DIGITAL SIGNATURES AND DIRECTING THE APPLICATION OF DIGITAL SIGNATURES IN E-GOVERNMENT SERVICES" (EO810) signed on June 15, 2009. The Certification Authority referred to in said EO810 had not been set up at the time that the automated election system was being implemented. But Mr. Garcia missed to mention that there are private entities operating locally as Certification Authority. Further, the implementation of digital signing is contrary to COMELEC's Bid Bulletin No. 10 which required that "The digital signature shall be issued by a certificate authority nominated by the winning bidder and approved by the Comelec."[14]

At the resumption of the hearing on May 24, 2010, among the matters discussed was the verifiability of the digital signature in the PCOS machine. Mr. Cesar Flores, in his testimony, despite the evidence to the contrary, insisted that the digital signature exists:

"THE CHAIRPERSON. Okey, Congressman Rodriguez.

"REP. RODRIGUEZ. It says here the log for Biliran. Here it says right there in the tape. It says, *No BEI keys with which to sign results.* It's right here, Mr. Chair.

"THE CHAIRPERSON. May I have an explanation...

"REP. RODRIGUEZ. There is no... It says. *No BEI keys with which to sign results.* In other words, there's zero digital signature. That should be accepted.

"THE CHAIRPERSON. Okay, can I get an explanation, Mr. Flores, what is the meaning of those words?

"MR. FLORES. If you look at Republic Act 9369, it basically says *the results shall be signed before transmission.* The voting machine has a digital signature in itself which is also corroborated with the card and the password that is provided to the BEIs. The BEIs when they type their password, they encrypt the results and the results are digitally signed and sent to the server.

"THE CHAIRPERSON. So it is a digital signature of a machine

"MR. FLORES. Yes. It is generic for the BEIs. There was an additional option—additional option of BEIs—if they are provided with an individual signature to also affix their signatures to the results.

Transcript of Stenographic Notes
Committee on Suffrage and Electoral Reforms
May 24, 2010

The response of Mr. Flores to the clarification sought by Rep. Rodriquez quite significantly reveals that it is the machine that has a digital signature and that it was **generic** to the BEIs in the sense that with the use of the iButton keys in which a password or signing key is stored, digital signing may be executed. It is generic in the sense that the signing key is the same for every iButton key.

In sum, therefore,

While COMELEC and Smartmatic/TIM representatives explained that the election return is digitally signed by the PCOS machine, it is not clear in the process described in ComRes8786 as amended at what point digital signing by the PCOS machine occurs.

While the Mr. Correia explained at the hearing of the House of Representatives Committee on Suffrage and Electoral Reforms (CSER-HoR) the certificate of canvass is signed by the USB security token, it is not clear in the process described in ComRes8809 when digital signing is executed.

It appears that the electronic keys assigned to the members of the BEI and the BOC were generated by Smartmatic/TIM. This implementation is consistent with the first paragraph of the clarification issued under Bid Bulletin No. 10 in regard to the digital signature but is not consistent with the role of certificate authorities, which is supposed to be a neutral third party.

By not nominating a certificate authority as clarified in the second paragraph of the clarification under Bid Bulletin No. 10, it appears then that Smartmatic/TIM assumed the role of certification authority. Smartmatic/TIM is not a neutral third party as it played an active role in implementing, operationalizing, and managing the AES.

COMELEC and Smartmatic/TIM representatives had admitted in the hearing conducted by the (CSER-HoR) that what was implemented is [what was later in the hearing referred to as] "machine digital signature". Research, however, shows that "machine digital signatures" do not legally exist. RA8792 is quite explicit in its recognition of electronic signatures and the expressed presumption relating to electronic signatures is that an electronic signature is the signature of a person to whom it correlates[15].

Of iButton Keys and PINs

The iButton Key is a new technology, just in its infancy. It is an electronic device capable of storing data. It is an electronic key much like what a card key (now in common use in hotels which allow hotel guests to open their rooms) is.

PIN or Personal Identification Number is more associated with ATM cards where a bank customer's account number is shown on the face of his ATM card and the PIN is known only to the customer. Whenever the bank customer withdraws cash from the bank through the ATM he is asked to enter his PIN.

COMELEC and Smartmatic/TIM may argue that the combination code stored in the iButton Key and the BEI Chairman's PIN constitutes the public-private key pair used in digital signing and verification. But it has to be underscored that none of the BEI members generated their own public-private key pair. Smartmatic/TIM generated the code stored in the iButton Key and the PINs.

ComRes 8786 clearly shows that the iButton Key and the PINs are used to operate the PCOS, i.e., at the point of generating the initialization report prior to opening of polls or at the point where the PCOS machine is to be closed, among others.

The CSER-HoR Chairman Concludes

On the matter of digital signature, Rep. Teodoro Locsin, having heard the arguments presented during the hearing concludes:

> THE CHAIRPERSON.
>
> x x x
>
> Number 2. On the issue of the adequacy of digital signature only for the PCOS machine as opposed to the literal definition in the E-Commerce Act that clearly requires that a digital signature be personal to the person using it. My colleagues are here, I would like to explain that I am giving this explanation because sometimes media attributes to me statements that come either from you or from other witnesses because I rephrase questions to make it clearer. This is what I have been saying. May I venture to say that since every PCOS machine is assigned and registered to be in the custody and operation of particular BEIs, then, for all practical purposes, we can trace the digital signature of a PCOS machine to its particular BEI custodians in the precinct. The PCOS signature, therefore, sufficiently serves as the signature of the particular precinct BEI custodians who can just as easily be held accountable for any electronic anomalies traced to their particular and specified machine as if their own personal signatures have been used. Therefore, there is not just sufficient but equivalent practical compliance with the definition of a digital signature in the E-Commerce Act.
>
> In this regard, I must admit I was wrong to tell one reporter that the Congressional Canvass can constitutionally ignore the different meaning of digital signature in the E-Commerce Act, and accept without question all, strictly speaking, "unsigned ERs and COCs" purely for reasons of state because the elections are over and we need to proclaim a president even in the teeth of a violation of the E-Commerce Act's literal meaning. I admit I was wrong, there is a real reason why a PCOS signature is the practical equivalent of a personal signature. You can trace it to the custodian of that PCOS signature, or the PCOS machine assigned to him. Is that correct?
>
> MR. HEIDER GARCIA. (Electoral Systems Manager, Smartmatic-Total Information Management Corporation). That's correct, Your Honor.
>
> THE CHAIRPERSON. Okay. But it is also equally ignorant for one lawyer to argue that election laws are only mandatory before elections and merely directory and can be casually ignored after elections. This is pure ignorance. I do not believe that there are Supreme Court decisions that made such an ignorant ruling. It is precisely after elections that elections laws can be more strictly performed... executed because then actual and not speculative violations can be proved. Is that correct, Rufus Rodriguez? It is my view that the PCOS digital signature is fully compliant with the law. In a subsequent hearing, experts can dispute my views, but these are my views and not the views of anybody else and I think they are correct.
>
> Transcript of Stenographic Notes
> Committee on Suffrage and Electoral Reforms
> May 26, 2010

The arguments presented by the CSER-HoR Chairman in his conclusion supporting the validity of the digital signature appearing in the election return and that such digital signature is the signature of the BEI Chairman rests on the ability by the COMELEC and Smartmatic/TIM to trace the PCOS to the BEI Chairman. Indeed, the PCOS machine may be traced to the BEI Chairman as records of the COMELEC and Smartmatic/TIM would probably show. However, the issue goes beyond traceability. The matter extends to (1) independent verification of the digital signature and (2) the determination of the authenticity and due execution of the election reports.

Examination of PCOS Machines

There is also a need to consider the report of SysTest Lab[16] with regard to the verification of the digital signature appended to each election return as well as the findings of the Joint Forensic Team[17].

In his review of the SysTest Lab Report, Atty. Al S. Vitangcol points to SysTest Lab's examination of the PCOS SLOG.TXT file stored in the CF Card:

SysTest Lab Report

6. TRANSMISSION TEST SUMMARY

> The transmission of data among the reporting hierarchy was successfully implemented by the AES system: data moved among each point in the reporting structure in the expected manner. While **the digital signature could not be verified,** the transmissions were verified to be encrypted in a manner prescribed by Smartmatic. *(emphasis supplied)*
>
> Certification Test Report Summary for AES May 10, 2010
> Rev. 1.00, March 8, 2010
> SysTest Labs
> 216 16th St., Suite 700, Denver, CO

Examination of the PCOS Audit Log

Further, Atty. Vitangcol underscores a finding in the PCOS Audit Log:

> Main CF Card SLOG.TXT FILE
>
> May 10/2010 19:36:10 EmlGenerate Tabulating Results
> May 10/2010 19:36:24 Xmit FileGen Generating EML Transmit file
> May 10/2010 19:36:26 Xmit FileGen Audit **No BEI keys with which to sign results**. *(emphasis supplied)*
> May 10/2010 20:40:03 Admin Audit Transmitting reports to 'MBOC:5802000May 10/2010 20:40:03 Telecom Audit About to transmit file '/cflash/ResTrans' (18997 bytes)
>
> A POST AES 2010 EVALUATION
> Atty. Al S. Vitangcol III
> Managing Lawyer, AVALaw

The SLOG.TXT entry "May 10/2010 19:36:26 Xmit FileGen Audit No BEI keys with which to sign results" is consistent with ComRes8786 instructing the BEIs to skip the digital signing. But it is also noticeable in the log sequence that digital signing by the PCOS was not a recorded event. This only indicates that the election return is not signed by the machine.

Forensic Examination: Digital Certificates

In its final report to the Hon. Juan Ponce Enrile, Senate President, and the Hon. Prospero Nograles, Speaker of the House, the Joint Forensic Team reported:

> "Absence of Machine Digital Signatures.
>
> "Examination of the PCOS machines revealed that there was no evidence found to prove the existence of digital certificates in the PCOS machines, contrary to the claims of Smartmatic. The technicians of Smartmatic were not able to show to the forensic team the machine version of the digital signature, alleging that they do not have the necessary tool to show the same. More so, they were at a quandary as to how to extract the said machine signatures – to the dismay of the forensic team.
>
> "If there are digital certificates then these were supposed to be revealed. The forensic team tried to extract the digital signatures but to no avail. Hence, the forensic team is of the opinion that there exists no digital signature in the PCOS machine."
>
> Final Report of the Forensic Team
> June 9, 2010
> Atty. Al S. Vitangcol III, CHFI
> For the Joint Forensic Team

CONCLUSION

The implementation of digital signing in the automated election system is not technically or technologically consistent with the implementation of digital signature technology. The technology is centered on the use of a PKI operated by a Certificate Authority.

No certification authority was engaged by the COMELEC to provide services in the implementation of digital signing. Instead, Smartmatic generated and issued the electronic keys stored in the ibutton keys issued to the BEI Chairman and in the USB security tokens issued to the members of the BOC.

The claimed implementation of digital signing is contrary to the requirements of the RFP-AES2010, clarified in the related Bid Bulletin No. 10.

The claimed existence of a "machine digital signature" in each PCOS machine is debunked by the findings by SysTest Labs which failed to verify any digital signature as well as the failure of Smartmatic technicians to demonstrate existence of a digital certificate that will confirm the existence of a digital signature.

The claimed "machine digital signature" does not legally exist. RA8792 accords legal recognition to digital signatures as the signature of a person. No Philippine law, rule, or statute has accorded legal recognition of "machine digital signature".

The foregoing considered, the AES requirement for digital signing is not met.

Implications

The lack or absence of a digital signature on the ER, SOV, and COC impaired the authenticity and due execution of said election reports.

The lack or absence of a digital signature on the ER, SOV, and COC rendered the election reports vulnerable to tampering and manipulation. ***EU-CenPEG Project 3030***

ANNEX A

Definition of "Digital Signature Technology" Related Terms

Term	RA 8792	ECA-IRR	DTI-JAO02-2001	REE
Asymmetric or public cryptosystem			is a type of signature creation technology and refers to a system capable of generating a secure key pair, consisting of a private key for creating a digital signature, and a public key for verifying the digital signature.	means a system capable of generating a secure key pair, consisting of a private key for creating a digital signature, and a public key for verifying the digital signature.
Certificate			means an electronic document issued to support a secure electronic signature which purports to confirm the identity or other significant characteristics of the person who, in the case of digital signatures, holds a particular key pair or, in other cases, such signature creation or verification device or method as may be applicable under the circumstances.	means an electronic document issued to support a digital signature which purports to confirm the identity or other significant characteristics of the person who holds a particular key pair.
Certification authority			is a type of information certifier which, in the course of its business, engages in issuing certificates in relation to cryptographic keys used for the purposes of digital signatures.	

Digital Signature			is a type of secure electronic signature consisting of a transformation of an electronic document or an electronic data message using an asymmetric or public cryptosystem such that a person having the initial untransformed electronic document and the signer's public key can accurately determine: (i) whether the transformation was created using the private key that corresponds to the signer's public key; and (ii) whether the initial electronic document had been altered after the transformation was made.	refers to an electronic signature consisting of a transformation of an electronic document or an electronic data message using an asymmetric or public cryptosystem such that a person having the initial untransformed electronic document and the signer's public key can accurately determine: (i) whether the transformation was created using the private key that corresponds to the signer's public key; and, (ii) whether the initial electronic document had been altered after the transformation was made.
Electronic Data message	refers to information generated, sent, received or stored by electronic, optical or similar means.	refers to information generated, sent, received or stored by electronic, optical or similar means, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy. Throughout these Rules, the term "electronic data message" shall be equivalent to and be used interchangeably with "electronic document."		

Electronic document	refers to information or the representation of information, data, figures, symbols or other modes of written expression, described or however represented, by which a right is established or an obligation extinguished, or by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored, processed, retrieved or produced electronically.	"Electronic document" refers to information or the representation of information, data, figures, symbols or other modes of written expression, described or however represented, by which a right is established or an obligation extinguished, or by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored, processed, retrieved or produced electronically. Throughout these Rules, the term "electronic document" shall be equivalent to and be used interchangeably with "electronic data message."		
Electronic key	refers to a secret code which secures and defends sensitive information that crosses over public channels into a form decipherable only with a matching electronic key.	refers to a secret code, which secures and defends sensitive information that crosses over public channels into a form decipherable only by itself or with a matching electronic key. This term shall include, but not be limited to, keys produced by single key cryptosystems, public key cryptosystems or any other similar method or process, which may hereafter, be developed.		

Electronic signature	refers to any distinctive mark, characteristic and/or sound in electronic form, representing the identity of a person and attached to or logically associated with the electronic data message or electronic document or any methodology or procedures employed or adopted by a person and executed or adopted by such person with the intention of authenticating or approving an electronic data message or electronic document.	refers to any distinctive mark, characteristic and/or sound in electronic form, representing the identity of a person and attached to or logically associated with the electronic data message or electronic document or any methodology or procedures employed or adopted by a person and executed or adopted by such person with the intention of authenticating or approving an electronic data message or electronic document.		
Information Certifier			means any person who, or entity which, in the course of its business, issues certificates as a means of providing identification services and/or certifying information which are used to support the use of and trust in secure electronic signatures. For purposes of these Rules, the term "information certifier" includes but is not necessarily limited to certification authorities.	
Key pair			in an asymmetric cryptosystem refers to the private key and its mathematically related public key such that the latter can verify the digital signature that the former creates.	in an asymmetric cryptosystem refers to the private key and its mathematically related public key such that the latter can verify the digital signature that the former creates.

Private key			refers to the key of a key pair used to create a digital signature.	refers to the key of a key pair used to create a digital signature.
Public key			refers to the key of a key pair used to verify a digital signature	refers to the key of a key pair used to verify a digital signature
Secure Electronic Signature			means an electronic signature which is created and can be verified through the application of a security procedure or combination of security procedures that ensures such electronic signature: a. is unique to the signer; b. can be used to identify objectively the signer of the data message c. was created and affixed to the data message by the signer or using a means under the sole control of the signer; and d. was created and is linked to the data message to which it relates in a manner such that any change in the data message would be revealed. For purposes of these Rules, secure electronic signatures includes but is not necessarily limited to digital signatures.	

Annex B

What is a Digital Signature?
An introduction to Digital Signatures, by David Youd

Bob

(Bob's public key)

(Bob's private key)

Bob has two keys. One of Bob's keys is called a Public Key, the other is called a Private Key.

Bob's Co-workers:

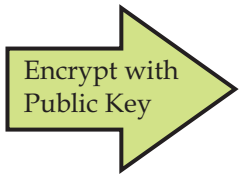
Pat Doug Susan

Anyone can get Bob's Public Key, but Bob keeps his Private Key to himself

Bob's Public key is available to anyone who needs it, but he keeps his Private Key to himself. Keys are used to encrypt information. Encrypting information means "scrambling it up", so that only a person with the appropriate key can make it readable again. Either one of Bob's two keys can encrypt data, and the other key can decrypt that data.

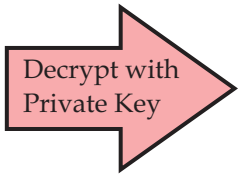
Susan (shown below) can encrypt a message using Bob's Public Key. Bob uses his Private Key to decrypt the message. Any of Bob's coworkers might have access to the message Susan encrypted, but without Bob's Private Key, the data is worthless.

"Hey Bob, how about lunch at Taco Bell. I hear they have free refills!"



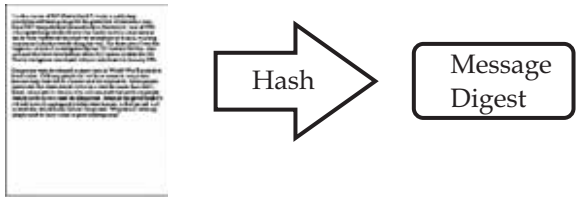
HNFmsEm6Un
BejhhyCGKOK
JUxhiygSBCEiC
0QYIh/Hn3xgiK
BcyLK1UcYiY
lxx2lCFHDC/A

HNFmsEm6Un
BejhhyCGKOK
JUxhiygSBCEiC
0QYIh/Hn3xgiK
BcyLK1UcYiY
lxx2lCFHDC/A

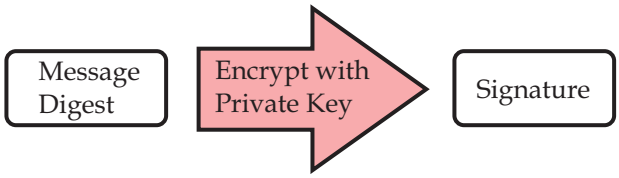


"Hey Bob, how about lunch at Taco Bell. I hear they have free refills!"

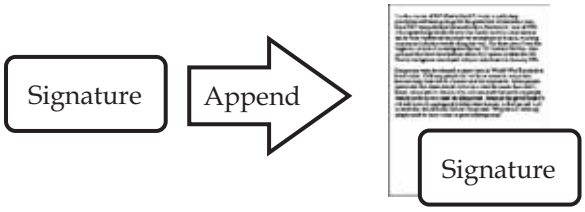
With his private key and the right software, Bob can put digital signatures on documents and other data. A digital signature is a "stamp" Bob places on the data which is unique to Bob, and is very difficult to forge. In addition, the signature assures that any changes made to the data that has been signed can not go undetected.



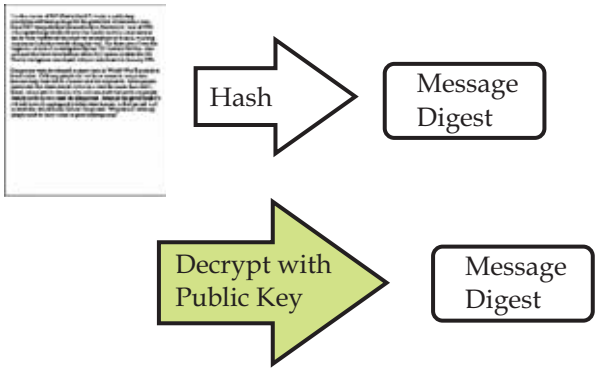
To sign a document, Bob's software will crunch down the data into just a few lines by a process called "hashing". These few lines are called a message digest. (It is not possible to change a message digest back into the original data from which it was created.)



Bob's software then encrypts the message digest with his private key. The result is the digital signature.



Finally, Bob's software appends the digital signature to document. All of the data that was hashed has been signed.

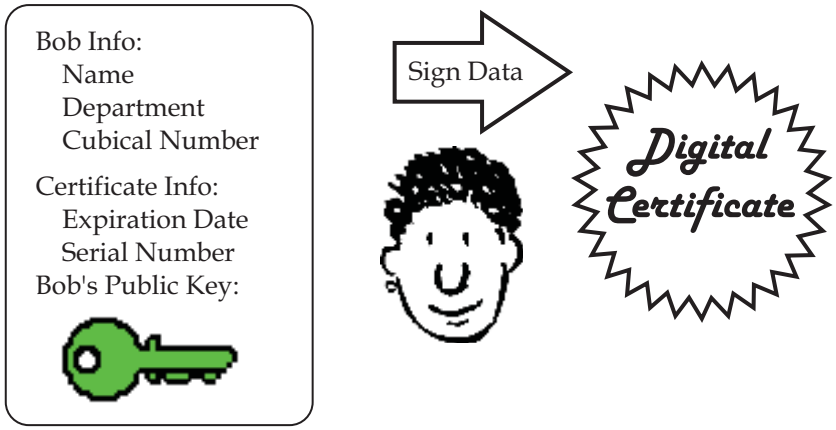


Bob now passes the document on to Pat.

First, Pat's software decrypts the signature (using Bob's public key) changing it back into a message digest. If this worked, then it proves that Bob signed the document, because only Bob has his private key. Pat's software then hashes the document data into a message digest. If the message digest is the same as the message digest created when the signature was decrypted, then Pat knows that the signed data has not been changed.

Plot complication...

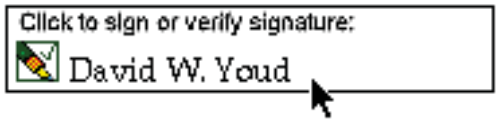
Doug (our disgruntled employee) wishes to deceive Pat. Doug makes sure that Pat receives a signed message and a public key that appears to belong to Bob. Unbeknownst to Pat, Doug deceitfully sent a key pair he created using Bob's name. Short of receiving Bob's public key from him in person, how can Pat be sure that Bob's public key is authentic?



Now Bob's co-workers can check Bob's trusted certificate to make sure that his public key truly belongs to him. In fact, no one at Bob's company accepts a signature for which there does not exist a certificate generated by Susan. This gives Susan the power to revoke signatures if private keys are compromised, or no longer needed. There are even more widely accepted certificate authorities that certify Susan.

Let's say that Bob sends a signed document to Pat. To verify the signature on the document, Pat's software first uses Susan's (the certificate authority's) public key to check the signature on Bob's certificate. Successful de-encryption of the certificate proves that Susan created it. After the certificate is de-encrypted, Pat's software can check if Bob is in good standing with the certificate authority and that all of the certificate information concerning Bob's identity has not been altered.

Pat's software then takes Bob's public key from the certificate and uses it to check Bob's signature. If Bob's public key de-encrypts the signature successfully, then Pat is assured that the signature was created using Bob's private key, for Susan has certified the matching public key. And of course, if the signature is valid, then we know that Doug didn't try to change the signed content.



Although these steps may sound complicated, they are all handled behind the scenes by Pat's user-friendly software. To verify a signature, Pat need only click on it.

End Notes

1 See Batas Pambansa No. 881, Omnibus Election Code (BP881) Section 212

2 SeeBP881 Sections 15 and 231

3 Republic Act No. 9369, "AN ACT AUTHORIZING THE COMMISSION ON ELECTIONS TO USE AN AUTOMATED ELECTION SYSTEM IN THE MAY 11, 1998 NATIONAL OR LOCAL ELECTIONS AND IN SUBSEQUENT NATIONAL AND LOCAL ELECTORAL EXERCISES, TO ENCOURAGE TRANSPARENCY, CREDIBILITY, FAIRNESS AND ACCURACY OF ELECTIONS, AMENDING FOR THE PURPOSE BATAS PAMPANSA BLG. 881, AS AMEMDED, REPUBLIC ACT NO. 7166 AND OTHER RELATED ELECTIONS LAWS, PROVIDING FUNDS THEREFOR AND FOR OTHER PURPOSES" (RA9369)

4 See RA9369 Section 19

5 See RA9369 Section 20

6 See "Request for Proposal for Solutions, Terms & Conditions for the Automation of the May 10, 2010 Synchronized National and Local Elections" (RFP-AES2010) issued by the Commission on Elections, III. General Policies, Rules, and Guidelines, Item No. 4/4.5 and IV Technical Specifications, Component 1-B Precinct-Count Optical Scan (PCOS, Item Nos. 22 and 23

7 See RFP-AES2010 III. General Policies, Rules, and Guidelines, Item Nos. 5/5.5.2, 6/6.5.2, 7/7.5.2, and 8/8.5.2 and IV Technical Specifications, Component 1-C Consolidation/Canvassing System (CCS) Item No. 1.12

8 See RA9369 Section 25

9 See RA7199 Section 30.

10 See Supreme Court Rules on Electronic Evidence Rule 5 and Rule 6

11 RA8792 Section 7

12 See RA8792, Section 8

13 COMELEC Resolution 8809, GENERAL INSTRUCTIONS GOVERNING THE CONSOLIDATION/CANVASS AND TRANSMISSION OF VOTES AT THE MUNICIPAL/CITY/PROVINCIAL AND DISTRICT BOARDS OF CANVASSERS IN CONNECTION WITH THE MAY 10, 2010 NATIONAL AND LOCAL ELECTIONS. Article III, Sec 26 d) 1) 1.6 and Sec 26 d) 1) and Sec 26 e)

14 COMELEC Bid Bulletin No. 10 issued in relation to RFP-AES2010 clarifying the requirement on digital signature.

15 See RA8792, Section 9

16 SysTest Lab, a private sector company based in Denver, Colorado, operating as a certifying agency engaged by the COMELEC to review and certify the Automated Election System.

17 The Joint Forensic Team was constituted by the Joint Canvassing Committee tasked to conduct a forensic review of the PCOS machines then in the custody of the Senate of the Philippines.