COMMENT

# ELECTRONIC SIGNATURES UNDER CURRENT PHILIPPINE LAW

*Jose Gerardo A. Alampay**

## I. INTRODUCTION

The information and communications technology (ICT) sector is a key driver in Philippine efforts to promote lasting economic growth and development. In particular, e-services[1] has been singled out for promotion by the government as a priority because of its potential for growth and revenues, as well as for the high value jobs that are expected to be generated by increased investment in this area.[2] Indeed, it is now the oft-stated intent and vision of the country to compete directly with India and China and become *the* e-services hub of Asia.

To make a credible run at this vision, at least two things need to be assured. First, in any given online transaction, parties – such as foreign and domestic investors, entrepreneurs and potential business partners – must have a mechanism that will reliably and securely prove the origin, receipt and integrity of electronic information; identify the parties involved; and finally, associate those parties with the contents of the communication. And second, government and private sector transactions and commitments made through electronic data messages or documents must be clearly binding, enforceable and admissible in evidence.

---

* LL.B. (1991), U.P, LL.M. (1993), University of San Diego, MPIA (1996), University of California, San Diego. Jose Gerardo A. Alampay is a lawyer specializing in information and communications technology issues and is partner in the Makati-based law offices of Alampay Gatchalian Mawis & Alampay. He may be reached by email at gigo_a@skyinet.net.

[1] E-services include an entire range of services that make use of information and communications technology to enable an organization to improve and increase its operational efficiency. These services include technical services such as web development and management, database design and development, computer networking and data communications, software development and the like; as well as information technology-enabled services like call centers, animation and content creation, market research, human resource services and other business processing outsourcing services.

[2] In February 2003, President Gloria Macapagal Arroyo launched the Information Technology & E-Commerce Council Strategic Roadmap which identified 21 priority projects aimed at improving Philippine competitiveness in the e-services global marketplace.

It is in this context that Republic Act 8792, better known as the Electronic Commerce Act of 2000 sought to

> facilitate domestic and international dealings, transactions, arrangements, agreements, contracts and exchanges and storage of information through the utilization of electronic, optical and similar medium, mode, instrumentality and technology to recognize the authenticity and reliability of electronic documents related to such activities and to promote the universal use of electronic transaction in the government and general public.[3]

At the heart of the Act's purpose is a recognition that the use of electronic signatures to verify the authenticity and reliability of electronic documents is critical to the promotion of electronic transactions and indeed, all commerce in general. Without it, parties involved in e-commerce transactions would not be able to fully assess the risks of doing business, such as whether there is a likelihood of the transaction being able to be successfully completed; whether it can be challenged; and whether the recipient will have legal recourse in such circumstances, irrespective of the location of the parties.

This paper provides an overview of one type of electronic signature – the digital signature, which is a type of electronic signature that is generated through the use of what is known as public key infrastructures (PKI).

PKI is important for two reasons. First, PKI is currently the most popular and widely used technology for electronic authentication in the Philippines and elsewhere. And second, it is the only type of electronic signature that presently is presumed to be authentic under the Interim Rules on Electronic Evidence issued by the Supreme Court.

The following section outlines in simple terms the process and technology behind PKI. This is followed by a discussion of electronic authentication and digital signatures under Philippine law. Focus is given particularly to the policy impact of biases seemingly reflected by two major issuances on electronic signatures, namely, the Supreme Court's Interim Rules on Electronic Evidence, and of course, the E-Commerce Act of the 2000 and its accompanying Implementing Rules and Regulations. The paper concludes by identifying other relevant issues and concerns that may arise in the near to medium term future.

---

[3] Rep. Act No. 8792, sec. 3.

## II. HOW DIGITAL SIGNATURES WORK

Under the Electronic Commerce Act of 2000, electronic signatures refer "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."[4]

There are many methods for creating an electronic signature. These methods range from simple ones--- such as typing a name at the bottom of an email message--- to more complex and secure ones--- for example, biometric technologies, such as fingerprints or retinal scans.

Still other types of authentication methods include: magnetic strip cards with personal identification numbers (PIN), user names and passwords, public key cryptography, writing tablets with electronic pens, and even smart cards that generate a unique access code every few seconds. As technology advances, the list of viable electronic signature alternatives is sure to grow.

Note that electronic signatures and digital signatures are not the same things.

"Electronic signatures" refer to any distinctive mark, characteristic and/or sound in electronic form, representing the identity of a person and are attached to or logically associated with an electronic data message or electronic document.

A "digital signature" does not refer to the image of a signature in any way. Unlike both an "electronic signature" which is simply any form of mark intended to be a signature (such as the sender's name typed at end of an email message), and a "digitized signature" which refers to an electronic image of a signature, a "digital signature" is actually a term of art that refers to scrambling data in order to provide security and authentication. "Digital signatures" form a subset of electronic signatures, and are created and verified using cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible form and then back into the original form.

Military communications have relied on encryption for thousands of years. For example, Alexander the Great communicated with his generals by sending

---

[4] Rep. Act No. 8792, sec. 5(e).

messages in which each letter was shifted a certain number of positions. This was a form of "secret key encryption," and anyone who knew the secret code (or key) would be able to send and receive messages with relative security.

Today, commercially available encryption software creates encryption so strong that it is all but impossible to break the code and ascertain the original message without the use of the authorized software.

Of course, to be secure, a secret-key coding system requires some method of distributing the secret key to intended users, without it falling into the hands of other parties.

By its nature, the Internet is poorly suited for a secret-key system because it is an "open" network in which a message may make several "stops" before arriving at its final destination. This creates a serious risk that a third party could intercept a secret key at some point along its route, and allow the third party to read messages, or even send encoded messages purporting to be from the authorized holder of the key.

Physically delivering a secret key to every user, on the other hand, would be slow, expensive and unwieldy. It would discourage, if not effectively rule out one-time transactions between people and/or firms that are unknown to each other and who have not previously exchanged secret keys.

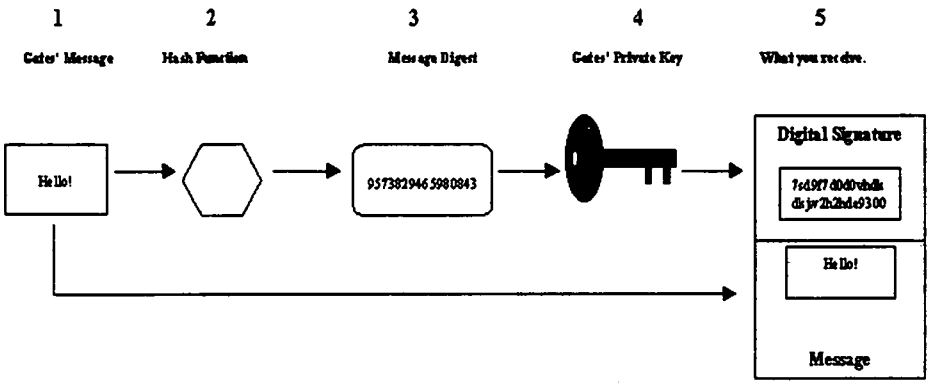
### A. PUBLIC KEY CRYPTOGRAPHY

Public key cryptography eliminates the need for users to share a secret key, which makes it ideally suited for communications over open networks such as the Internet. In a public key system, each user has software that generates two related keys, a public key and a private key. The fundamental characteristic of this key pair is that a message encrypted with a given private key can only be decrypted by its corresponding public key, and vice versa.

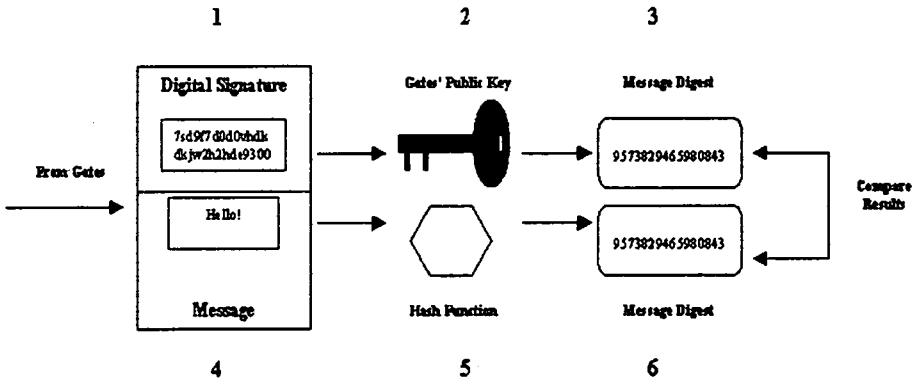
The process is illustrated in the two diagrams below.[5]

---

[5] *See* "Consultative Document on Electronic Authentication and Digital Signatures." Department of Trade and Industry (DTI) of the Republic of the Philippines (issued May 2001).




Let us assume that (1) Bill Gates has a message that he wants to digitally sign and send to you. He would then (2) run his message through one of several standard algorithms known as a "hash function" that performs a series of mathematical operations on the original message. The hash function produces a number called a (3) "message digest" which can be thought of as a fingerprint of the message, because any change in the message, no matter how slight, will cause the hash function to produce a completely different message digest. (4) Using his private key, Bill Gates then encrypts the message digest. The message digest encrypted with Bill Gates' private key forms the actual (5) "digital signature" for the message. Both the digital signature and the actual message are then sent to you.



Upon receipt of the message, your computer and software would then perform two separate operations to verify Bill Gates' identity and to determine if the message had been altered in transit.

To verify Gates' identity, your system would (1) take the digital signature and (2) use Gates' public key to decrypt the digital signature, which would then (3) produce the message digest. If the operation is successful, you would then know for a fact that Bill Gates' (who alone has access to his private key) must have sent the message.

In order to ensure that Gates' message had not been altered, your system would (4) run Gates' message through the (5) same hash function that Gates' used, which would then (6) yield a message digest of Gates' message. You would then be able to (7) compare the two message digests, and if they are identical, confirm that the message has remained unaltered in transit.

Generally then, users of this system would keep their private key very safe (perhaps password-protected, or even embedded in a smartcard) but they would make their public key freely available, by sending it to all potential recipients of messages or posting it to an Internet public key directory.

In this way, the private key holder (in the example, Bill Gates) can send a message to anyone on the Internet, and, if his public key decrypts the message, the recipient knows it must have come from the private key holder. Conversely, anyone on the Internet who wants to send the private key holder a message can encrypt the message with his public key, and send the message with the knowledge that only the private key holder can read the encrypted text.

### B. PUBLIC KEY INFRASTRUCTURES AND CERTIFICATION AUTHORITIES

The process of public key cryptography described above can work well between parties who know each other.

But what happens in transactions between parties who have never met each other before? In the example above, how would you know for certain that Bill Gates, and not someone else posing as Bill Gates, did in fact send the message?

In broader terms, in an age where persons who have never met are able to transact over the Internet, how can one party bind the identity of another to a particular public key?

Companies known as "Certification Authorities" (CA) provide one solution.

The CA vouches for the identity of a person who subscribes to their service. It issues a certificate in effect guarantees the identity of the person (or subscriber) associated with a given public key. The CA is responsible for undertaking certain measures to ascertain the identity of the person to whom it issues a certificate. This certificate issued by the CA

1. identifies the CA issuing it;

2. identifies the subscriber ;

3. contains the subscriber's public key; and

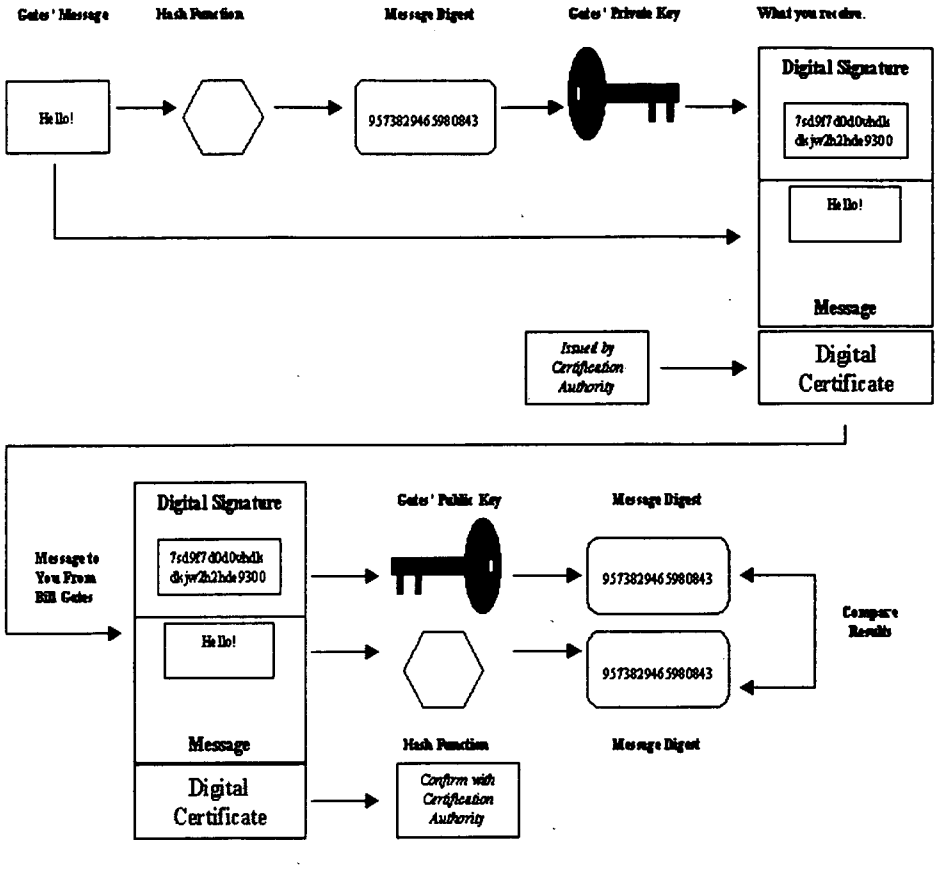
4. is digitally signed with the CA's private key.

The digital certificate can also contain additional information including a reliance limit, or a reference to the CA's "certification practice statement" that gives relying parties notice of the level of inquiry conducted by the CA before issuing the certificate.

Thus, if Bill Gates wished to use a CA to vouch for his identity on the Internet, he would have to present the CA with a copy of his public key along with sufficient proof of his identity (or else the CA could also issue Gates' private and public keys). Once satisfied with the identity of Bill Gates, the CA would issue Gates' a digital certificate.

Going back to our example, and as shown in the diagram below, Gates will send you, along with his digital signature, a copy of his digital certificate. And, in addition to the steps described above, upon receipt of Gates' message, you can also confirm with the CA identified in the digital certificate that Gates is who he says he is, and that his certificate has not expired or been revoked.

Note that all these activities would be transparent to you, and would happen in much the same way as occurs with online credit card validation systems.




Ultimately, given a situation where Person A sends an electronic document over the Internet to Person B, PKI reasonably assures Person B of the following:

> (a) *Data Origin Authentication*. First, Person B must have some assurance that the message has in fact come from its purported sender, Person A.
>
> (b) *Message Integrity*. Second, that the message received by Person B is the exact message that Person A sent. Person B should be able to verify that the message has not been intentionally or accidentally altered during transmission.

(c) *Non-Repudiation*. And finally, that Person A cannot later deny that he or she did in fact send the message. No one else should have been able to send the message but Person A, and Person B should be able to prove this fact unequivocally.

These assurances effectively render digital signatures as functional equivalents of traditional handwritten signatures. They make it possible for online transactions to be formalized in a manner which assures the parties of their validity and now, because of the E-Commerce Act, undoubted enforceability.

## III. ELECTRONIC AUTHENTICATION UNDER CURRENT PHILIPPINE LAW

Electronic authentication is covered by Sections 8 and 9 of the E-Commerce Act of 2000:

> Sec. 8. *Legal Recognition of Electronic Signatures*
>
> An electronic signature on the electronic document shall be equivalent to the signature of a person on a written document if that signature is proved by showing that a prescribed procedure, not alterable by the parties interested in the electronic document, existed under which:
>
> (a) A method is used to identify the party sought to be bound and to indicate said party's access to the electronic document necessary for his consent or approval through the electronic signature;
>
> (b) Said method is reliable and appropriate for the purpose for which the electronic document was generated or communicated, in light of all the circumstances, including any relevant agreement;
>
> (c) It is necessary for the party sought to be bound, in order to proceed further with the transaction, to have executed or provided the electronic signature; and
>
> (d) The other party is authorized and enabled to verify the electronic signature and to make the decision to proceed with the transaction authenticated by the same.
>
> Sec. 9. *Presumption Relating to Electronic Signatures*
>
> In any proceeding involving an electronic signature, it shall be presumed that

> (a) The electronic signature is the signature of the person to whom it correlates; and
>
> (b) The electronic signature was affixed by that person with the intention of signing or approving the electronic document unless the person relying on the electronically signed electronic document knows or has notice of defects in or unreliability of the signature or reliance on the electronic signature is not reasonable under the circumstances.

To emphasize, it is important not to be misled by the law's use of the term "electronic signature" under section 9. Taken in the context of section 8 of the E-Commerce Act--- which requires "a prescribed procedure not alterable by the parties," as well as other requirements to ensure party identification, method reliability, intent and verifiability --- it appears that not all electronic signatures necessarily enjoy the legal presumptions afforded under section 9.

How the requirements of section 8 of the E-Commerce Act are to be applied in real world situations will ultimately be fleshed out by future jurisprudence and/or legislation. But there certainly is room for lawyers to put forth substantially different interpretations.

For instance, at least one e-commerce law expert has taken a narrow interpretation and opined that "it appears that the Act validates only digital signatures which exist within the context of public key infrastructures."[6]

This view is reinforced by the Supreme Court's Interim Rules on Electronic Evidence, to the extent that under these Rules, only secure electronic signatures, defined as electronic signatures that are "linked to an electronic data message or electronic document through a prescribed procedure unalterable by the parties interested in the transaction and affixed with the intention of authenticating, signing or approving the electronic document or electronic data message"[7] are admissible in evidence.[8] Significantly, the same Rules recognize digital signatures as secure electronic signatures and thus, PKI-generated signatures are admissible in evidence,

---

[6] *See* JESUS M. DISINI, JR., THE ELECTRONIC COMMERCE ACT AND ITS IMPLEMENTING RULES AND REGULATIONS (2000).

[7] INTERIM RULES ON ELECTRONIC EVIDENCE, Rule 2, sec. 1(t)

[8] INTERIM RULES ON ELECTRONIC EVIDENCE, Rule 6, sec. 1.

while other types of electronic signatures do not automatically enjoy that presumption.[9]

Such a technology-biased position could have unintended policy consequences.

It is obviously easier to accord meaningful legal consequences to the use of known and specific technologies – as the Supreme Court has done with PKI – and more difficult to do the same for electronic authentication techniques less known or used, or those which have yet to be invented.

The danger, however, is that favoring, intentionally or not, a known authentication mechanism such as in this case, public key infrastructures, could stunt the development of other authentication mechanisms, or at least give undue benefits to a technology that is itself only in the earliest stages of commercial use. Apart from these concerns and a general desire to avoid the rapid obsolescence of new legislation, there is also a concern that premature endorsement of a particular technology could set the country outside of the mainstream of technological and legislative developments internationally.

For this reason, an alternative, broader interpretation was adopted by the Department of Trade and Industry in the Implementing Rules and Regulations on Electronic Authentication and Electronic Signatures that it issued pursuant to the E-Commerce Act, to wit:

> Section 5. *Legal Recognition of Electronic Signatures.* - An electronic signature on the electronic document shall be equivalent to the signature of a person on a written document if that signature is proved by showing that a prescribed procedure, not alterable by the parties interested in the electronic document, existed under which:
>
> (a) A method is used to identify the party sought to be bound and to indicate said party's access to the electronic document necessary for his consent or approval through the electronic signature;

---

[9] INTERIM RULES ON ELECTRONIC EVIDENCE, Rule 2, sec. 1(t). "Secure Electronic Signature" refers to a digital signature or any electronic signature that is linked to an electronic data message or electronic document through a prescribed procedure unalterable by the parties interested in the transaction and affixed with the intention of authenticaing, signing or approving the electronic document or electronic data message.

> (b) Said method is reliable and appropriate for the purpose for which the electronic document was generated and communicated, in the light of all circumstances, including any relevant agreement;
>
> (c) It is necessary for the party sought to be bound, in order to proceed further with the transaction, to have executed or provided the electronic signature; and
>
> (d) The other party is authorized and enabled to verify the electronic signature, and to make the decision to proceed with the transaction authenticated by the same.
>
> The parties may agree to adopt supplementary or alternative procedures provided that the same are not contrary to law or public policy.

Note that the provision above would cover public key infrastructures as well as other technologies and electronic signatures. Even simple common email signatures, it can be argued, would be covered, as long as it is "reliable and appropriate" in light of the circumstances. For example, an automatically generated online response acknowledging receipt of an email message would be valid and ideally should be enforceable under the E-Commerce Act and its Implementing Rules and Regulations.

## IV. CONCLUSION

This paper is primarily intended to serve as an introduction to electronic signatures, and particularly, the technology of public key infrastructures. For members of the legal profession, particularly, it is important to have some understanding of the technologies that underlie electronic signatures and authentication, as these would ultimately impact on the enforceability of electronic contracts or other documents.

Future developments in technology will undoubtedly test the limits and capability of Philippine law and jurisprudence. Some of the questions that are likely to arise in the near future will include issues related to the emergence of alternatives to PKI, jurisdiction, and liability, especially of third party certifiers like certification authorities. It is interesting to see how the legislature and the judiciary will respond to these emerging challenges, and indeed, these issues – particularly their legal and policy ramifications – are worthy of further scholarly exploration.

Finally, it will not be surprising to see the Interim Rules on Electronic Evidence revisited and revised, even if these only took effect less than two years ago.

The events of September 11, 2001 have led to a dramatic increase in demand for electronic authentication technologies worldwide. New methods of electronic authentication, such as biometrics and voice authentication, are now emerging as commercially viable alternatives to PKI.[10] How should the courts treat these emerging types of authentication technology and other methods that remain undiscovered?

Given the fact that numerous, if not a majority of all online transactions and relationships are conducted by parties who reasonably rely on methods as ordinary or unsophisticated as regular typed email signatures – a less PKI-biased and more technology neutral set of Rules will have a better chance of ensuring that the courts remain consistent with the E-Commerce Act's stated purpose "to promote the universal use of electronic transaction in the government and by general public" and in step with rapid developments in electronic commerce.

—oOo—

[10] For a brief introduction to the use of biometrics, *see* SHAWN ABBOTT, *Marriage of Biometrics and PKI Tokens Holds Key to Security*, CISCO WORLD (January 2001).