Mindanao Journal of Science and Technology Vol.12 (2014) 86-108

Development of a Secured Web Page of CAAP SIS using Cryptography

Marylene S. Eder
College of Industrial and Information Technology
Mindanao University of Science and Technology
Cagayan de Oro City, 9000 Philippines
lhynshel@gmail.com

Date received: March 31, 2014
Revision accepted: June 04, 2014

Abstract

With the growth of the information technology (IT) power, and with the emergence of new technologies, the number of threats a user is supposed to deal with grew exponentially. The objective is to make a message encrypted with state of the art software virtually impossible to decode without a key. This research is intended for security matters which answers the issues of confidentiality, authorization, non-repudiation and integrity. With a hacker attack, you simply have to keep them out of the data, with a legal attack, you have to hide the existence of the data, as the legal system has at their disposal an additional channel for getting the data, they can subpoena it and demand you to disable any protective measures and hand over the data. The results of the study showed that with the development of audit trail this becomes more promising in terms of security. Users are now updated with the files that are being sent and received by them. It also provided an easy access in transmitting confidential reports. The confidentiality and integrity of transmitted data are secured, and the authorization of the user to perform task is fully ensured and files are being transmitted, non-repudiation occurs.

Keywords*:* asymmetric cryptography, secured web page, E commerce

1. Introduction

Security in today's world is one of the important challenges that people are facing all over the world in every aspect of their lives. Similarly, security in electronic world has a great significance (Basharat *et al.*, 2012). Information or data is a valuable asset in any organization. Almost all organizations whether social, governmental, educational and others, have now automated their information systems and other operational functions. Data that is determined by a responsible authority to be sensitive, data that has a high value, or data that represents a high value should be cryptographically

protected if it is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage (Barker, 2008).

With rapid advancement in Internet and networking technologies during the recent years, communication and information exchange have become much easier and faster, but at the same time the issues related to data security and confidentiality have become a major concern of the time. To cater to this need of information security, a number of hidden and secret communication techniques such as cryptography, anonymity, covert channels, steganography and watermarking have been developed (Mishra *et al*, 2012).

Cryptography consists in processing plain information applying a cipher and producing encoded output, meaningless to a third-party who does not know the key (EV SSL, 2011). It is a science which uses mathematics to encrypt and decrypt data. This science enables you to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication.

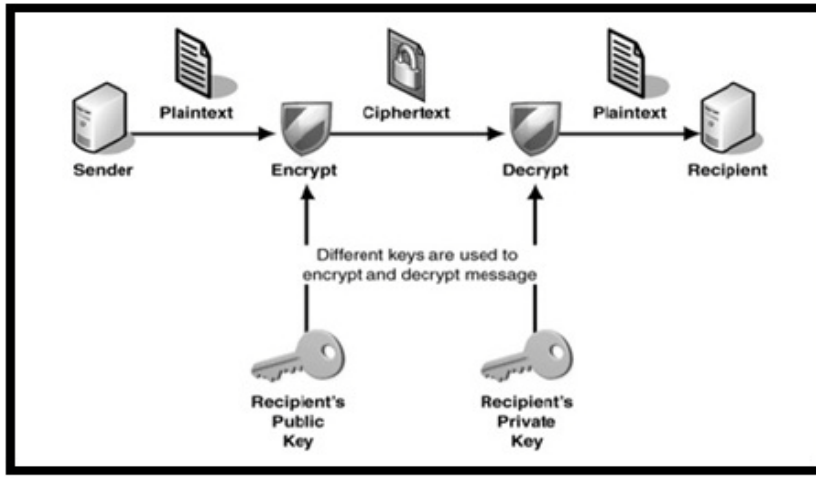


Figure 1. Asymmetric cryptography process

Figure 1 illustrates the typical asymmetric cryptography. There are two keys that are very essential in this process, namely; the public key and the private key. This would mean that different keys are being used to encrypt and

decrypt. When the user tends to send a plaintext to a ciphertext, the key used is the public key while that of decrypting the file is the private key where the intended user will be held liable for the secrecy of the private key. This means that one user equals one private key. Protecting the confidential/sensitive data stored in a repository is actually the database security. It deals with making database secure from any form of illegal access or threat at any level. Database security demands permitting or prohibiting user actions on the database and the objects inside it. Organizations that are running successfully demand the confidentiality of their database. They do not allow the unauthorized access to their data/information. And they also demand the assurance that their data is protected against any malicious or accidental modification.

The Philippine Electronic Commerce Act (COP, 2000) provides for the recognition and use of electronic commercial and non-commercial transactions and documents, penalties for unlawful use thereof and for other purposes. An electronic document shall be regarded as the equivalent of an original document under the Best Evidence Rule if it is a printout or output readable by sight or other means, shown to reflect the data accurately.

As stated in Philippines Rules of Court on Electronic Evidence (SC, 2001), electronic documents are considered as the functional equivalent of paper-based documents. Whenever a rule of evidence refers to the term of writing, document, record, instrument, memorandum or any other form of writing, such term shall be deemed to include an electronic document as defined in these rules.

Civil Aviation Authority of the Philippines Security and Intelligence Service (CAAP SIS) Area X covering six (6) satellite Airports with the Laguindingan Airport as Area Center X have just been experiencing problems regarding sending of reports and to maintain updated records and avoid losing of the documents. On the other hand saving it safely and secured from unauthorized person is another problem encountered by the respondents.

This study proposesd a secured web page document system for CAAP SIS that may be used in protecting data passing through the internet against malicious intruders and saving it safely in the database.

The general problem is the security of the files that are sent through the

public environment which is the internet and the loss of files for not having a secured storage. The outflow of the reports gave anyone a chance to be at risk. The following are the specific problems identified:

1. Confidentiality of the message or data sent to the internet. The CAAP SIS are having a problem with the utmost security of the confidential files for it to be protected from disclosure to unauthorized parties.

2. Integrity of the message or data sent to the internet. The message transmission is not also safe from unauthorized modification because the information can be altered in storage or transit between sender and intended receiver without the alteration being detected.

3. Authentication and Non-Repudiation of the message or data. It gives them a hard time to identify if the authorized sender is really the one who sent the message and the message was received by the specified party, so the recipient cannot claim that the message was not sent.

4. Loss of files. For not having a proper storage of their files, confidential reports are sometimes lost from the computer without knowing who did it.

The study aimed to develop a secured webpage document system that catered to the need of the agencies for security purposes. This study would help the agency in maintaining the privacy of intelligence data and reports for the management information and guidance. Specifically, the study aimed to:

1. Design a system that protects the data from network attacks and unauthorized access by encrypting the file.

2. Develop a database that serves as a storage of the important data.

3. Develop a user log or audit trail for user's activities.

4. Test and evaluate the system's functionality and usability.

Indeed, an airport, anyplace it may be located, needs full security. If and only if it is taken for granted, the involved risks encompass life, expensive equipment, cargo, and transportation infrastructures.

The study gives affirmative effect to CAAP SIS because the people inside the group are imposing security so their properties must be safe. This study is for the protection of the files that need not or should not be exposed to an unauthorized person. The implementation was used to prevent the leakage of special operational information, leakage of information that the CAAP SIS are taking measures to safeguard. Above all, only the person who has the appropriate level of clearance and a need to know-person can have the full access.

For the authorized person's part, sending and receiving reports from other Station Supervisors, Area Supervisors, and from the Central Office in Manila is now easier to do. Through online, both end users had easy access to their webpages and can view the information displayed.

The study is significant for the secure dissemination of information through data encryption. It benefited the aviation and also the people involved here.

This study is only limited at securing all kinds of reports like documents, videos and pictures that will be sent through the internet. This also includes the records of all applicants and employees of CAAP SIS in a particular Aerodrome.

It covers the confidentiality, integrity, non-repudiation of reports and authorization of users. The users (company) or bearer of the private key will be held liable for its security, especially when it is being exposed to an unauthorized person.

2. Methodology

This chapter presents the development process of the project, namely research design, design of the Security Web Page, development of the system and evaluation of the system. A security web page is carefully design to enable the use of encryption technology in ensuring confidentiality, authorization, integrity and non repudiation.

2.1 Design of the Security Web Page

2.1.1 Analysis

One of the CAAP SIS employees was interviewed and he cited different kinds of reports which need to be secured before it is being sent to the recipient through the internet. This includes the daily situation report, incident report, investigation report, information report, spot report, and consolidated report. These files need to be secured before being sent to its remote users through the internet.

2.1.2 Database Design

Centralized databases of the API for the key generation, and registered user information have been designed. To achieve this, the number of tables to be created and the fields to be included in the table are initially decided. There are entities that are initially decided and these are as follows: inbox, sent, transactions, user_logged, and users. The title of the database is CAAP SIS with five (5) tables with one or more fields that contain the information needed for the project.

2.1.3 Key Generation

Network security is typically handled by a network administrator or system administrator who implements the security policy, network software and hardware needed to protect a network and the resources accessed through the network from unauthorized access and also ensures that employees have adequate access to the network and resources to work. In order to have a full security of the message from the sender to the receiver, it has been decided to use an Asymmetric Encryption (also known as Public Key Cryptography). Since users typically create a matching key pair, one key is for public use while keeping the other secret.

Users can compose messages by encrypting them with their private keys. This is effective for any message recipient can verify that the user's public key can decrypt the message, and thus prove that the user's secret key was used to encrypt it. If the user's secret key is, in fact, secret, then it follows that the user, and not some fraud, really sent the message. Users can send secret messages by encrypting a message with the recipient's public key. In this case, only the intended recipient can decrypt the message, since only that

user should have access to the required secret key. Figure 2 shows an example of a key set group that is configured to manage two key sets: key set 1 and key set 2.

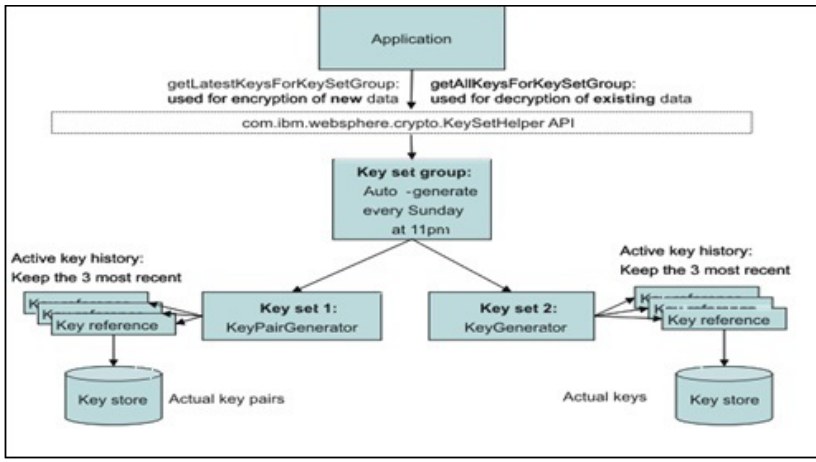


Figure 2. Key management

Key set 1 generates key pairs. Key set 2 generates secret keys. The application needs both types of keys for its cryptographic operations, signing and encryption, on data. The keys for each key set need to be generated in tandem. The application stores the key set group name with the encrypted data. The key set group generates a new set of keys every Sunday night at 11 P.M. The application maintains key generation data for two weeks.

Public Key Infrastructure (PKI) provides a management framework for enabling deployment of public key cryptography. Public key cryptography processes the data with a pair of keys, which are two distinct but corresponding computer codes. Encryption is done with one of the key-pair and decryption are only possible with the use of the other key in the same pair. One of the keys in the pair is kept by the owner of the certificate (as a personal secret), and is therefore called a 'private key'. The other key is publicly available, and hence called a 'public key'.

Figure 3 demonstrates the encryption/decryption process, the means by which the PKI ensures confidentiality. For instance, the privacy of messages sent via email can be protected by encryption with a recipient's public key.

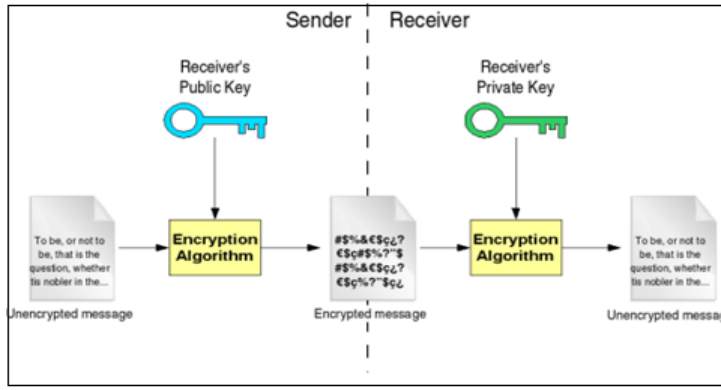


Figure 3. PKI encryption

Since only the recipient's private key can decrypt the encrypted message, this is an assurance that nobody other than the intended recipient can read the message.

A digital signature is another means to ensure integrity, authenticity, and non-repudiation. A digital signature is derived by applying a mathematical function to compute the message digest of an electronic message or document, and then encrypt the result of the computation with the signer's private key. Recipients can verify the digital signature with the use of the sender's public key. Figure 4 shows the means of digital signature.

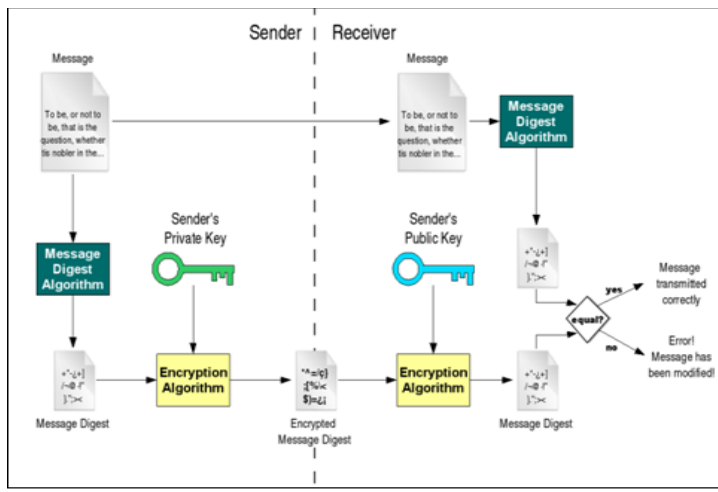


Figure 4. Digital signature

Figure 5 demonstrates the steps on how a message be secured from threats. First, the sender creates a ciphertext message by encrypting the plaintext message with an asymmetric encryption algorithm and the recipient's public key. Second, the sender sends the ciphertext message to the recipient. Last, the recipient decrypts the ciphertext message back to plaintext using the private key that corresponds to the public key that was used to encrypt the message.

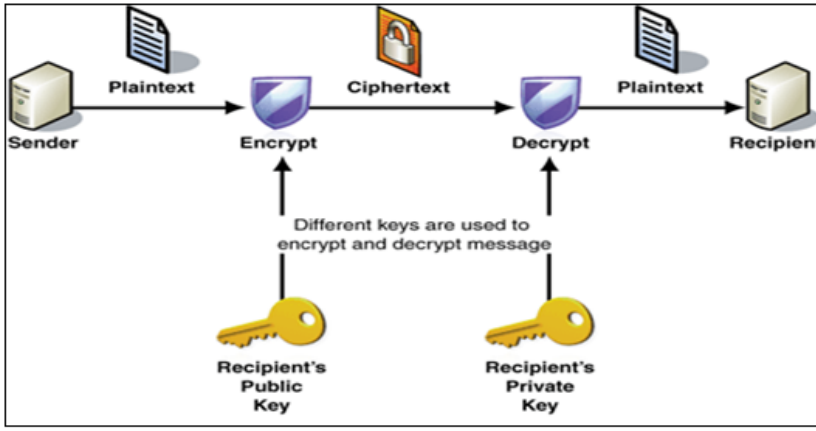


Figure 5. Asymmetric diagram

2.2 Development of the System

2.2.1 Built in Libraries

Front-end or client-side development is a relatively obscure Internet discipline. Historically, this role has been known under several aliases, htmler, web designer, coder, frontender and so on, but its core functions remain the same while expanding with the progress of the Internet. It is a hinge role that requires both aesthetic sensitivity and programmatic rigor.

Since the client wants to have his personal website for having an own format of his reports, they decided to do a hard-code site. This includes Javascript, HTML, and PHP that might be used as tools for the front-end of the project.
JavaScript is a scripting language, that is, a lightweight programming language that is interpreted by the browser engine when the web page is loaded. As part of web browsers, implementations allow client-side scripts to

interact with the user, control the browser, communicate asynchronously, and alter the document content that is displayed. It has also become common in server-side programming, game development and the creation of desktop applications (JavaScript, 2014).

HTML is the main markup language for creating web pages and other information that can be displayed in a web browser. The purpose of a web browser is to read HTML documents and compose them into visible or audible web pages. The browser does not display the HTML tags, but uses the tags to interpret the content of the page. HTML allows images and objects to be embedded and can be used to create interactive forms. It provides a means to create structured documents by denoting structural semantics for text such as headings, paragraphs, lists, links, quotes and other items. It can embed scripts written in languages such as JavaScript, which affect the behavior of HTML web pages (HTML, 2014).

PHP is a widely-used open source general-purpose scripting language that is especially suited for web development and can be embedded into HTML. What distinguishes PHP from something like client-side JavaScript is that the code is executed on the server, generating HTML which is then sent to the client. The client would receive the results of running that script, but would not know what the underlying code was. You can even configure your web server to process all your HTML files with PHP, and then there's really no way that users can tell what you have up your sleeve (PHP, 2014).

2.3 Development of Audit Trail

An audit trail (or audit log) is a security-relevant chronological record, set of records, or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event. The process that creates an audit trail is typically required to always run in a privileged mode, so it can access and supervise all actions from all users; a normal user should not be allowed to stop/change it.

Through this, the unauthorized access was detected easily by the ip address, browser used and location.

2.4 Testing and Evaluation of the System

In testing the efficiency of the system that satisfied the user and also

answered the security issues, a lecture was conducted at the CAAP SIS office located at the Laguindingan International Airport, Misamis Oriental. This was accommodated by the CAAP SIS Area Supervisor, Station Chief and chosen officer were given an authorization to access the system. They were oriented on the terms used in the system for them to know what they do about it. Also, the design of a website was presented in order to know the functions of each activity displayed. The confidentiality of reports was explained through the diagrams showed to them, and the process of how to use the system was also demonstrated. The CAAP SIS personnel were given a chance to manipulate the project in order to familiarize and learn how to send and receive messages from and to other Airports. They also answered questions about the security of the system that served as a survey questionnaire for the project. By these things, they gave comments about the project and suggested something to make it better. It guides them to improve the project for the satisfaction of the client to the secrecy of the reports.

3. Results and Discussion

3.1 Designing of the Security Web Page

3.1.1 Analysis

After studying the reports that were sent through the internet to the Central Office, the consolidated report is the most important file that needs security from the hackers and unauthorized person, for the reason that it composes the spot report, information report, incident report, daily situation report, and investigation report that be sent once in every month. In other words, consolidated report is the summary of all happenings, stated in the other reports. There is also what they called as “direct report” that contains very risky information that may cause trouble to the aerodrome or may need a direct response from the Central Office, so they are going to send it immediately. There are some documents that the CAAP SIS also keeps as a record for the new Airport police like personal data sheet and personal history statements of individual.

Table 1 shows the descriptions of all reports and documents that are being kept by the CAAP SIS personnel which are needed to be secured.

Table 1. Description of the transactions needed to be secured.

Documents	Descriptions	Security Requirements Needed
1. Daily situation report	Includes flight operation, number of cancelled flights, weather condition, and security measures.	Confidentiality
2. Incident report	This includes traffic violators, passengers complains, and reason of flights cancellation.	Confidentiality, Authorization
3. Investigation report	If there is an incident in the aerodrome, this kind of report may occur.	Confidentiality, Authorization,
4. Information report	This is by giving update situation of airport.	Confidentiality Authorization,
5. Spot report	After the incident report happened, spot report may follow.	Authorization, Confidentiality,
6. Consolidated report	It consists of 5 reports; the daily situation report, incident report, investigation report, information report and spot report. This report is sent once in a month.	Authorization, Confidentiality, Integrity, Non-repudiation
7. Direct report	It will be sent immediately to the central office if it has a high risk to the Airport.	Authorization, Confidentiality, Integrity, Non-repudiation
8. Personal data sheet	It is a form for the new applicant to be filled up and become a record in the office.	Authorization, Confidentiality,
9. Personal history statement of individual	It is a background investigation of the new applicant, and it includes NBI , Barangay Clearance and any personal information	Authorization, Confidentiality,

Encryption is required to address the problem on security. The software used is MySQL for database and openSSL function for key generation. MySQL was chosen because it is a free, open source relational database management system and can be used for a variety of applications, most commonly on

Web servers. In generating a key, openSSL function is used because it provides various encryption and decryption algorithm that can be of great help for the said security requirements of the files.

The function *file_encrypt ()* encrypts data that are sent using public key (*openssl_pkey_get_public*) and stores the result into encrypted_file. The encrypted data can only be decrypted via function *file_decrypt()*. The function *generatekey()* generates new private and public key pair. OpenSSL_decrypt() decrypts data that was previously encrypted via function *file_encrypt()*. The function file_decrypt() is used to decrypt data only for the intended person. Figure 6 shows the modular design where it organizes the mechanisms of the entire system.

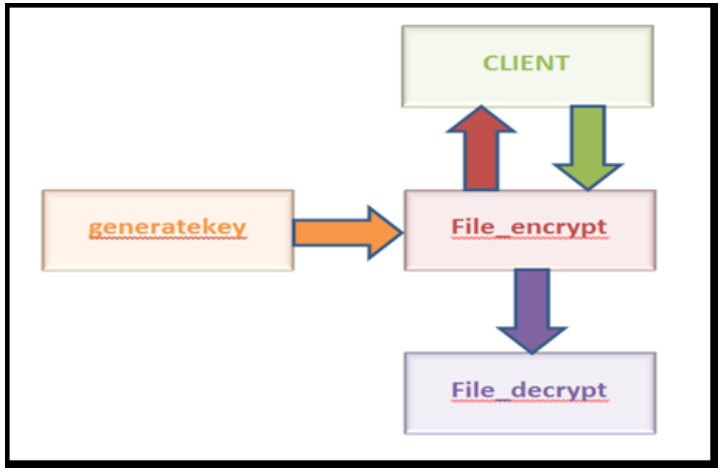


Figure 6. Modular design

3.2 Design of the System

3.2.1 Key Generation

The illustration presented in figure 7 shows the process of generating a key. The four steps in key generation are the following: selecting the user, clicking 'Generate Key', selecting the drive letter destination, and confirming the successful process of generating the key.

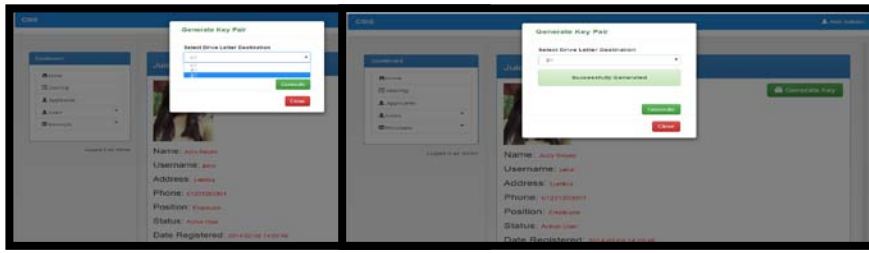
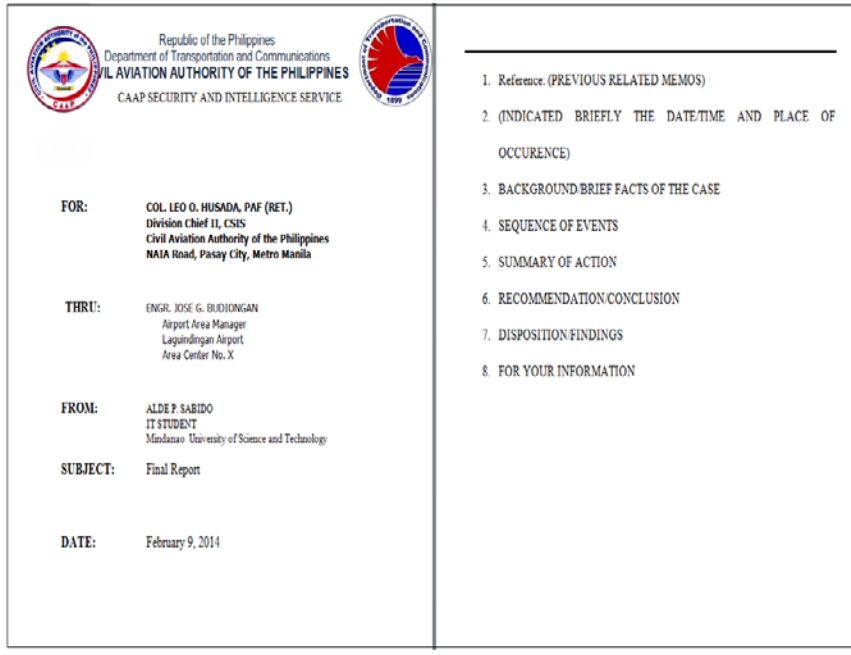


Figure 7. Screenshot of how key generation is being process

3.2.2 Confidentiality, Authorization/Authentication, Non-repudiation and Integrity

Figure 8 displays example of the original file report of CAAP SIS to be sent through the internet by the sender to another user or recipient. The public key of the recipient is needed in order to encrypt the file resulting into cipher text.



Republic of the Philippines
Department of Transportation and Communications
IL AVIATION AUTHORITY OF THE PHILIPPINES
CAAP SECURITY AND INTELLIGENCE SERVICE

FOR: COL. LEO O. HUSADA, PAF (RET.)
Division Chief II, CSIS
Civil Aviation Authority of the Philippines
NAIA Road, Pasay City, Metro Manila

THRU: ENGR. JOSE G. BUDIONGAN
Airport Area Manager
Laguindingan Airport
Area Center No. X

FROM: ALDE P. SABIDO
IT STUDENT
Mindanao University of Science and Technology

SUBJECT: Final Report

DATE: February 9, 2014

1. Reference. (PREVIOUS RELATED MEMOS)
2. (INDICATED BRIEFLY THE DATE/TIME AND PLACE OF OCCURENCE)
3. BACKGROUND/BRIEF FACTS OF THE CASE
4. SEQUENCE OF EVENTS
5. SUMMARY OF ACTION
6. RECOMMENDATION/CONCLUSION
7. DISPOSITION/FINDINGS
8. FOR YOUR INFORMATION

Figure 8. Original copy of the report

Figure 9 shows the encrypted file which solves the problem on confidentiality for the disclosure to unauthorized parties.

Figure 9. Screenshot of confidentiality and non-repudiation

Figure 10 shows how authorization or authentication of the users is attained.

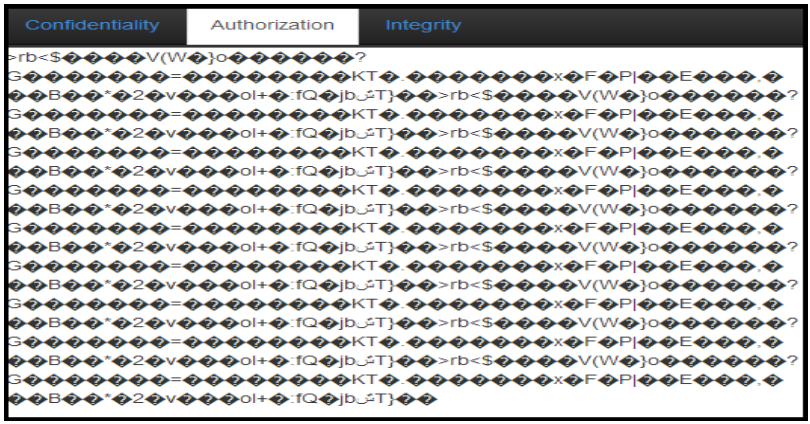


Figure 10. Screenshot of authorization/authentication

Figure 11 for integrity of the encrypted file wherein the message is safe from unauthorized modification.

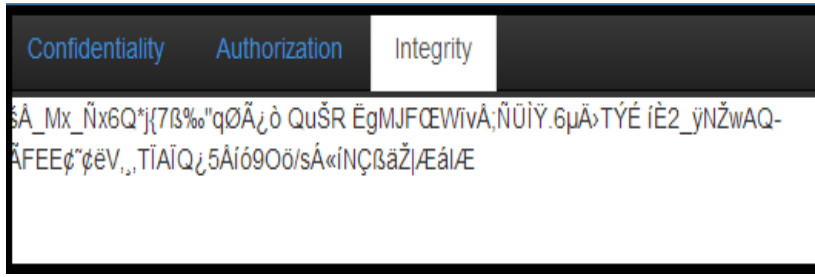


Figure 11. Resulting screen of integrity

Figure 12 shows the tracking of activities that the users are doing in the system.

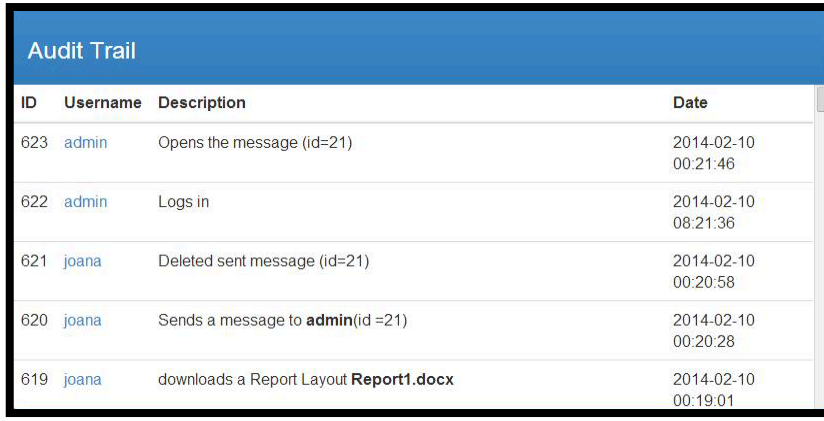


Figure 12. The resulting screen on how to track the activities

3.3 Development of the System

In developing the security gateway, open source programs are chosen since they are free. OpenSSL, CodeIgniter, WAMP, and Sublime are the software used in developing the security gateway. Figure 13 shows the source code for

generating the private and public keys. Figure 14 shows the screenshot of the public and private keys.

```
public function generateKey()
	{
		$prof_username = $this->input->post('prof_username');
		$prof_user_id = $this->input->post('prof_user_id');
		$privateKeyPath = $this->input->post('keyPath');
		$publicKeyPath = 'userFolder/'.$prof_username.'/key/pub_'.$prof_username.'.key';

		if(!file_exists("userFolder/".$prof_username))
		{
			$newFolder = "userFolder/".$prof_username;
			mkdir($newFolder,0777);
				mkdir($newFolder."/encrypted_file",0777);
				mkdir($newFolder."/storage",0777);
				mkdir($newFolder."/key",0777);
		}

		$config = array(
		"digest_alg" => "sha512",
		"private_key_bits" => 1024,
		"private_key_type" => OPENSSL_KEYTYPE_RSA,
		);
		// Create the keypair
		$res=openssl_pkey_new($config);

		// Get private key
		if(openssl_pkey_export_to_file($res,$privateKeyPath.'pri_'.$prof_username.'.key'))
		{
			$pubkey=openssl_pkey_get_details($res);
			$pubkey=$pubkey["key"];
			if(!file_put_contents($publicKeyPath,$pubkey))
			{
				echo "error";
			}

			$description = 'Generates a new key for <b>'.$prof_username.'</b>';
			$this->model_process->setUserlog($description);
			echo "okay";
		}
		else
		{
			echo "error";
		}
	}
```

Figure 13. Key generation code

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCV9wP2SF7oPgaYVnAMq
+fmeYEItS6yjzxFmCGnKmW+wsVzrW6DbNSaOoCw1oTFxONIAN
+zXW2r2kd1vivgstoizbF48U+F8xXNfOzYBJlSCu4tBb+j/EUzdofiq
+qE55oRSeMFRJFe55C8Qm/H5tQ0xUk6rbDOVlK6yc1kpOTNywIDAQAB-----END
PUBLIC KEY-----



-----BEGIN PRIVATE KEY-----
MIICdwIBADANBgkqhkiG9w0BAQEFAASCAmEwggJdAgEAAoGBAJX3A/ZIXug+BphW
cAyr5+Z5gQi1LrKPPEWYIacqZb7CxXOtboNs1Jo6gLDWhMXE4OgA37NdbaVaR3W+
JwCy2iLNsXjxT4XzFc187NgEmVIK7i0Fv6P8RTN2h+Kr6oTnmhFJ4wVEkV7nkLxC
b8fm1DTFSTqtsM5WUrrJzwSk5M3LAgMBAAECgYAwFdJpZ+82nJzUv/KRvZVQK2mady4QBymWTx
+LUGbrcdyKKPQkpALPqS6WhVJxb55I+i7Afpap4gXD1UJ67R5QSOQhGN+1Ov6bsVF5tm
+qrXveC14IR1yMfzyZaF5F/vMadnLYMj2H3W2lzUMoBoXqrZhD
C2tbxuh7Lcof70v8EQJBAMdhtIIyXD2qtvlRrXzA7nAEOdveqLJ3P/85YaNjuixG
qQagfM03nc7ApFgJ2U/f73mqlgbvjKVUNAkrR3Me//UCQQDAjOYFUALD6tLg6KIj
WTEVREzJS9M9d0NcTBWGQJe+8Viy+WPJgwCg3xAPIOQd4vtByg2kjqLzud2VwoXA
HL6/AkEAoQozyC1w/4YRwBLOs8MJU4S2Tvbq/yr+j+EDEfuM9hIkl+usofzYA5Tp
qQpbcf6H6Jd2EigOS8NVPEqurTdOuQJBAJvH4rldmD8lluL7k2IB4SIRlgYt4IOU
H91meOubCqoi3N5BEzlPUYzVq0pyE9zSLPF3JT6DX/bL4ygsrsVU/EUCQBCeQYtn
PvC1wm2uK94I52cx63CKQVoOcqLcStbABBpTZRewS3bYGGg/ktOeBJyba7ojBlzy
gc9F9AOJIBB7BSw=-----END PRIVATE KEY-----
```

Figure 14. Public and private keys

Figure 15 shows the source code used to encrypt data with the public key of the recipient. The function *file_encrypt()* encrypts the data.

```
public function file_encrypt()
  {
        $username = $this->session->userdata('username');
    $recipient = $this->session->userdata('recipient');
    $address = "userFolder/".$username."/encrypted_file/";
        $number = 0;
     foreach ($_FILES["file1"]["name"] as $n => $fileName)
     {
        $fileTmpLoc     = $_FILES["file1"]["tmp_name"][$number];
        $increment = '';
        $fileparts = pathinfo($address.$fileName);
        $basename = $fileparts['filename'];
        $basenameExtn = $fileparts['extension'];

        while(file_exists($address.$basename.$increment.".".$basenameExtn))
        {
            $increment++;
        }
            $fullfilename = $address.$basename.$increment.".".$basenameExtn;
            $basename = $address.$basename.$increment;
            $password = $recipient;
            $method = 'aes128';
            $pubkeystr = "userFolder/".$recipient."/key/pub_".$recipient.".key";
            $keyfile = file_get_contents($pubkeystr);

            $file2encrypt = file_get_contents($fileTmpLoc);
            $hashedFile =  md5($file2encrypt);
            $encrypted_file = openssl_encrypt($file2encrypt, $method, $password,0,'@!$&^$@g%w$g%^JF');
            file_put_contents($fullfilename,$encrypted_file);
            openssl_public_encrypt($password,$encrypted_pass,$keyfile);
            file_put_contents($basename.'_pass.txt',$encrypted_pass);
            $number++;
     }
  }
```

Figure 15. File for encryption

Figure 16 shows the source code used to decrypt data with the private key of the recipient. The function *file_decrypt()* decrypts data that was previously encrypted via function *file_encrypt()*.

```
public function file_decrypt() {
    {
            $privatekeystr = $_FILES['file']['tmp_name'];
            $privatekeyfile = file_get_contents($privatekeystr);
            $fileUrl = $this->session->userdata('fileUrl');
            $hashedFile = $this->session->userdata('hashedFile');
            $path_parts = pathinfo($fileUrl);
            $basename       = $path_parts['basename'];
            $file2decrypt = file_get_contents($fileUrl);
            $encrypted_pass = file_get_contents($path_parts['dirname'].'/'.$path_parts['filename'].'_pass.txt');

            if($file2decrypt)
            {
                $username = $this->session->userdata('username');
                $pass = $username;
                $method = 'aes128';
                $iv_size = mcrypt_get_iv_size(MCRYPT_RIJNDAEL_128, MCRYPT_MODE_CBC);
                $iv = mcrypt_create_iv($iv_size,MCRYPT_RAND);

                if(!openssl_private_decrypt($encrypted_pass,$decrypted_pass,$privatekeyfile))
                {
                    $inboxID = $this->session->userdata('inboxID');
                    redirect(base_url().'loadpage/loadViewMessage?id='.$inboxID.'&error=1', 'location');
                    $this->session->unset_userdata('fileUrl');
                    $this->session->unset_userdata('hashedFile');
                }
                if($decrypted_pass == $username)
                {
                    $decrypted = openssl_decrypt($file2decrypt, $method, $decrypted_pass,0,'@!$&^$@g%w$g%^JF');
                    if($hashedFile == md5($decrypted))
                    {
                        $transactionID= $this->session->userdata('transactionID');
                        $description = "Downloads a file attachment <b>".$basename."</b> (id=".$transactionID.")";
                        $this->model_process->setUserlog($description);
                        $this->session->unset_userdata('transactionID');
                        force_download($basename, $decrypted);
                    }

                }
            }
    }
```

Figure 16. File for decryption

3.4 Evaluation of the System

The testing of the study was successfully conducted at the Laguindingan International Airport, Misamis Oriental, CAAP SIS office last February 10, 2014. There were four (4) respondents who carefully listened and gave feedback regarding the system. The definitions of terms were being explained and the steps on how to use the functions found in the system were well demonstrated. It was also required to make a manual for them to easily understand the terms, and functionalities of the system. Afterward, the evaluation sheet was given to them for the feedback of the respondents and know whether it reaches its aim or not. Likert scale is more convenient than that of the yes-no question because the answers from respondents had quality and accuracy in its results. The following pie charts are the results of the evaluation.

Figure 17 shows that that the message or document sent to the receiver is successfully secured which pertains to confidentiality that resulted in 50% who agreed on it and 50% strongly agreed.

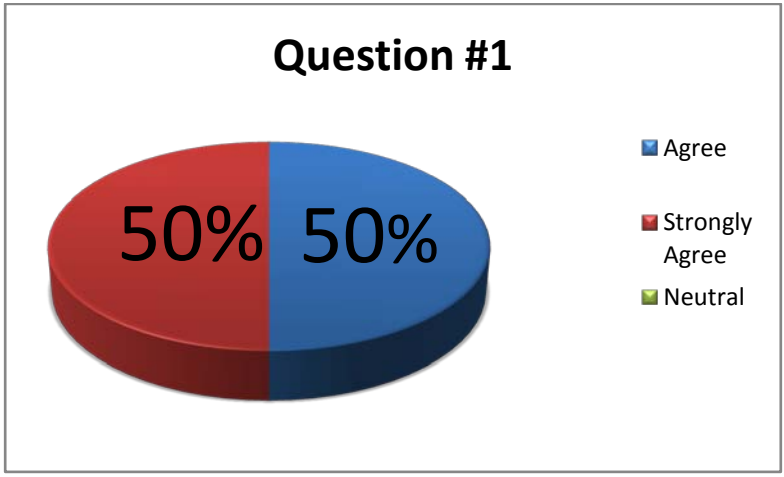


Figure 17. Responses to the question about confidentiality

Figure 18 illustrates the result which is all about authorization wherein only the authorized users can perform a certain task in the system and 75% of the respondents agreed and 25% of them strongly agreed.

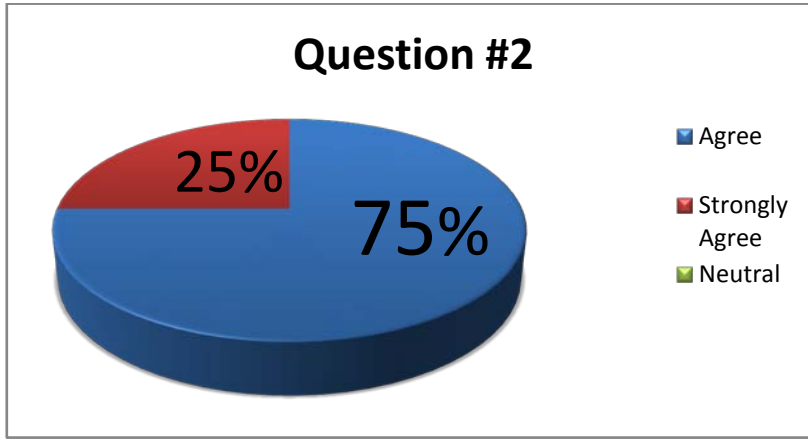


Figure 18. Responses to the question about authorization

Figure 19 shows the result where a user cannot subsequently reject a transaction which pertains to non-repudiation and 75% of the respondents agreed and 25% strongly agreed.

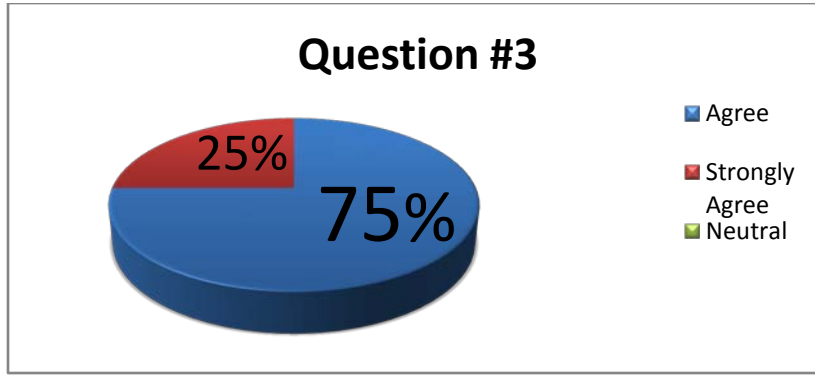


Figure 19. Responses to the question about non-repudiation

For the integrity, question #4 explains it and the result is opposite from the authorization and non-repudiation because 25% answered agreed and 75% strongly agreed wherein the received message is exactly the original one and is not edited.

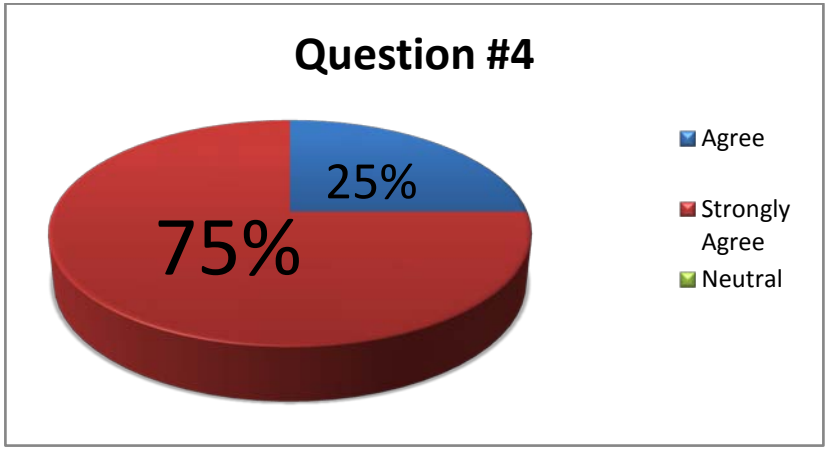


Figure 20. Responses to the question about integrity

Question no. 5 is about the website security and if it can really be trusted in terms of sending confidential files through internet which has 75% of strongly agreed and 25% of them answered agreed only.

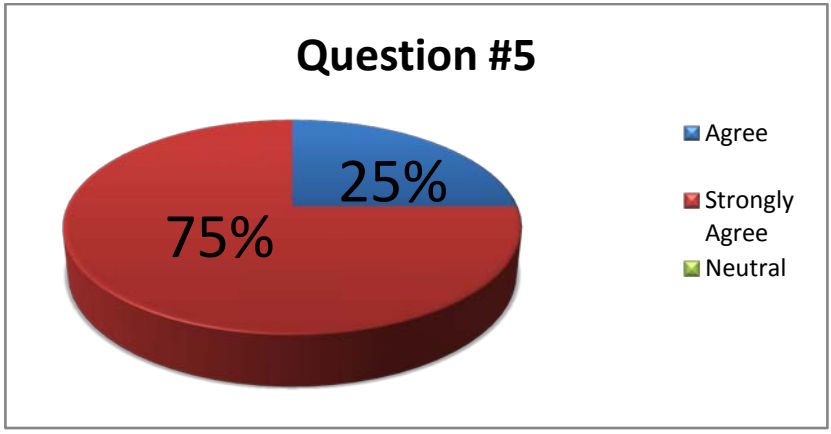


Figure 21. Responses to the question about system security

Figure 22 represents the question no.6 which is about accessing the website easily where 75% strongly agreed and 25% only agreed.

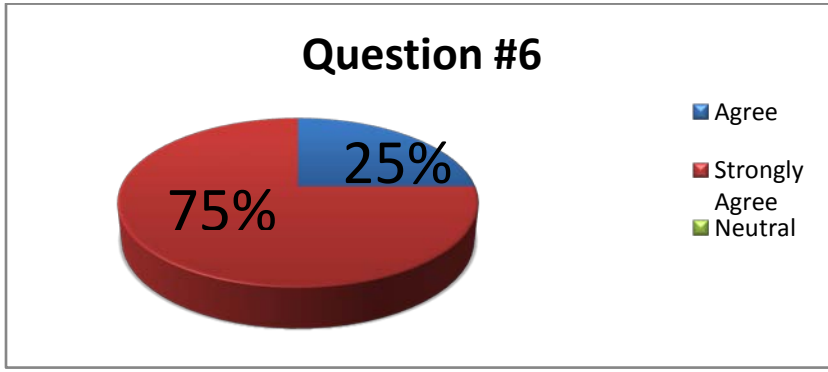


Figure 22. Responses to the question about being user-friendly

4. Conclusions and Recommendations

Secured Web Page is developed for integrating digital security requirements that is – practically at the same time cost effective and to address security issues namely confidentiality, authorization, integrity and non repudiation. Based on the findings of the study, it is concluded that with the development of Audit trail this becomes more promising in terms of security. Users are now updated with the files that are being sent and received by them. It also provides an easy access in transmitting confidential reports. The confidentiality and integrity of transmitted data are secured, and the authorization of the user to perform a task is fully ensured and files are being transmitted, non-repudiation occurs.

The present system has failures and nonexistence in some of its processes. For its further development, the following details are highly recommended;

1. Improve the system's capability of uploading files of big sizes. The system can upload a large file if there will be no encryption existing, but if there is, it can only cater 100Mb. There should be a bigger size of file that can be uploaded than the present one so in case there will be important files that is necessarily being uploaded, no more errors will occur.
2. The audit trail present in the system does not include the current location of the user and the device being used. So, for future development of this system, there should be a tracking of location should be included so that if a malicious intent occurs in the document being sent through the internet, it will be easily tracked.

5. References

Barker, W. (2008) Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, NIST Special Publication 800-67Version 1.1

Basharat, I., Farooque A., and A. W. Muzaffar (2012) Database Security and Encryption: A Survey Study. International Journal of Computer Applications (0975 – 888) Volume 47– No.12, June 2012

COP, (2000) Republic Act No. 8792: An Act Providing for the Recognition and Use of Electronic Commerce and Non – Commercial Transactions and Documents, Penalties for Unlawful Use Thereof and for other Purposes", Congress of the Philippines, Metro Manila, Philippines, June 14, 2000.

EV SSL, (2011) Extended Validation SSL Certificate The Next Generation High Assurance Certificate, from: http://www.evsslcertificate.com/ssl/description-ssl.html

HTML, (2014), from: http://en.wikipedia.org/wiki/HTML

Javascript, (2014), from: http://en.wikipedia.org/wiki/HTML

Mishra, M., Priyadarsini M., Adhikary, M.C. and S. Kumar (2012). Image Encryption using Fibonacci-Lucas Transformation. International Journal on Cryptography and Information Security (IJCIS),Vol.2, No.3, September 2012

PHP, "PHP", (2014), http://www.php.net/manual/en/introwhatis.php

SC (2001) Rules on Electronic Evidence A.M. no. 01-7-01-sc.Committee on the Revision of the Rules of Court, Senate Congress, Metro Manila, Philippines, June 18, 2001