IMPLEMENTATION OF DIGITAL SIGNATURE APPLICATIONS USING HASH FUNCTION ALGORITHM SHA-256 AND RSA AT BADAN PERTANAHAN NASIONAL OF CIMAHI CITY

Egi Cahyo Prabowo[1], Irawan Afrianto,S.T., M.T.[2]

[1] Teknik Informatika – Universitas Komputer Indonesia
Jl. Dipatiukur 112-114 Bandung
E-mail : ghie21@ymail.com[1], irawan.afrianto@email.unikom.ac.id[2]

ABSTRACT

Badan Pertanahan Nasional (BPN) of Cimahi City is a government agency that has the task in the land sector in accordance with the provisions of the legislation. BPN Cimahi provides several services to the community, one of the service registration and registration of land title documents. However, it was found that the land certificate document forgery and manipulation of the contents of the document. In addition, the lack of alternative services for document publishing digital certificates. Considering the alternative service for document publishing land certificates digital in BPN Cimahi very important it needed a good security system to prevent the falsification of documents and land certificates digital being misused by unauthorized people.

Digital signature can be used to test the integrity and authentication of a document land certificates digital, and can detect changes in a document land certificates digital from the manipulation by unauthorized people. One way to make a digital signature on a document land certificates digital by using a hash function. Hash algorithm used in the study is the Secure Hash Algorithm-256 (SHA-256), while the public key algorithm used algorithm is the Rivest-Shamir-Adleman (RSA).

Based on the results of testing that has been done, it can be concluded that implements digital signature using hash function SHA-256 algorithm and the RSA algorithm can provide document authentication security services on land certificates digital in BPN Cimahi City so as to prevent forgery and manipulation of documents by unauthorized people.

Keywords : Digital Signature, Fungsi Hash, Secure Hash Algorithm-256 (SHA-256), Algoritma Rivest-Shamir-Adleman (RSA), Badan Pertanahan Nasional (BPN) Kota Cimahi.

1. INTRODUCTION

BPN Cimahi is a government that has the task in the field of land nationwide, regional and sectoral legislation according to the provisions. At this time at BPN Cimahi has used data management within an integrated land Sistem Informasi dan Manajemen Pertanahan Nasional (SIMTANAS), built to store, and process the data in the national scale in the areas of land.

Based on interviews conducted with BPN Cimahi obtained information that ever happened to forgery of certificates of land and existence of manipulation against the amount of land that exists in the document, although in that document there is a signature and BPN stamp the original, but the documents contents already does not correspond to the actual data. Another issue is the existence of alternative services for document publishing digital certificates.

Considering the alternative service for publishing documents in digital land certificate BPN Cimahi is very important so it takes a good security system to prevent the occurrence of certificate forgery digital land and not to be abused by people who are not entitled to.

To ensure a digital document is genuine or not, there is a method of authentication that is with the concept of using a digital signature. A digital signature can serve to test the integrity and authentication of a digital document, and can detect any changes in the document of results manipulations [1]. One way to do digital signatures on a document that is by using a hash function, from the hash function will generate a message digest.

To generate a message digest takes a secure hash function which has a length of the hash value more, and SHA-256 is a secure hash algorithm with a length of 256 bits [3], while the public key algorithm used public key algorithm is Rabin, ElGamal algorithm, and algorithm RSA. Among the algorithms, third algorithm RSA is an algorithm that is not too simple but also not too complex, so RSA algorithm is the algorithm that is most fitting if desired to implement public key cryptographic algorithms [4].

2. RESEARCH

2.1 The Security and Confidentiality of Data

Security is a mechanism and techniques to protect something that can be either data or information in the system. Basically the system security is used to protect the system in a network security to keep awake. The issue of security and confidentiality of data is one of the important aspects of an information system. In this case, it is very related to how important the information was received by the person concerned. The information will be invalid if the information is in the know or hijacked by people who are not entitled to [6].

Information or data at this time has become something very important for an organization, universities, government agencies as well as individual, including the ability to access and provide information quickly and accurately. Because of the importance of an informed, often the desired information can be accessed only by certain people for example the desired recipient, and if the information is to be received by unwanted parties will impact of losses on the part of the sender.

2.2 Aspects of Information Security

Information security is how we can prevent fraud, or at least detected fraud in an information-based system, to protect your information from access, use, dissemination, destruction, alteration, and destruction without legitimate authorization. For that required an approach in the conduct of security information, such as encryption, steganography, digital signature, all ciphers and hashing against that information.

Aspects of computer security is a form of reasoning that States a computer can be declared safe. Security aspects in cryptography are as follows: [7]

1. Confidentiality i.e. is an attempt to keep the information from a person who is not entitled to access.
2. Authentication i.e. so that recipients of information can ensure the authenticity of the message is coming from a guy who asked for information
3. Non-repudiation i.e. it is concerned with the sender, the sender cannot shrug off that she was the one who sent the information.
4. Integrity i.e. the authenticity of messages sent through a network and can be sure that the information sent is not modified by people who have no right in the course of such information.

2.3 Cryptography

Cryptography is the study of how our message or document so that it is safe, can not be read by unauthorized parties. There are two types of cryptographic algorithms based on the type of the key: [8]

1. Symmetry algorithm is also known as the conventional algorithm is an algorithm that uses the same encryption key with the key decryption. Symmetric algorithms are often also referred to as a secret key, algorithms are algorithms the key algorithm or a single key. In Figure 1 the symmetric cryptography stated that at the time in the encryption and decryption key in use.

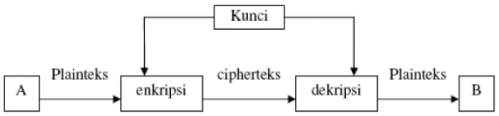


Figure 1. Process of Symmetry Cryptographic

2. Asymmetric algorithms are designed such that the key used for encryption is different from the key used for decryption, visible in Figure 2 key for encryption is not the same as the key for decryption. The key to encryption is not secret, so also called the public key, while the key to decrypt the secret, so it is called a private key. The sender encrypts the message using the public key of the recipient of the message, only the message recipient can decrypt the message to its original plainteks by using the private key. Examples of asymmetric cryptographic algorithms such as RSA (Rivest-Shamir-Adleman), Rabin, and ElGamal.

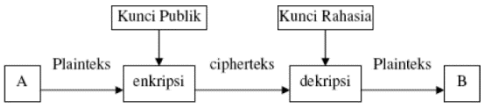


Figure 2. Process of Asymmetry Cryptographic

2.4 Digital Signature

One of the concepts on modern cryptography are digital signature. The way things work and the usefulness of the digital signature is similar to signing autographs in the real version, namely, to provide assurance of the authenticity of the document and the agreement by the signatories. In the digital signature, the "signature" in digital form is used to approve a digital document.

The principle used in this digital signature is a document submitted must be signed by the sender and the signature can be checked by the recipient to ascertain the authenticity of the documents submitted. Its function is to perform validation against data sent. Digital signatures using an algorithm called the hashing algorithm. The function will generate a unique combination of characters called a message digest. in this way the sender is responsible for the content of the document and the document's authenticity can be checked by the recipient. Its uniqueness is if in the middle of the journey of the data undergoing modification, removal and sadap secretly by the hackers even though it is only 1 character only, then the message digest that is on the

recipient will be different with the delivered at first. Other uniqueness is the message digest will not be reinstated into the early forms like before being touched with the function of the algorithm, so called as the one-way hash [2].

The main function of the digital signature on the security aspects of cryptography is non-repudiation or anti denial where if the document is valid then the sender cannot deny that the presence of the correct documents are sent by the sender is concerned.

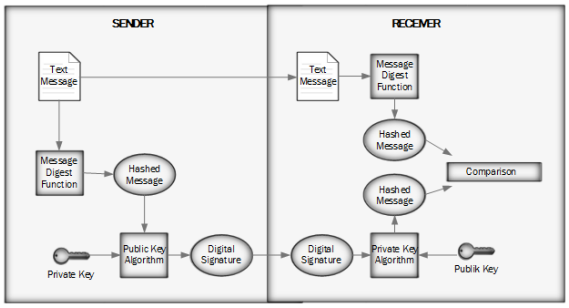


Figure 3. Scheme Digital Signature

The workings of the digital signature as seen in Figure 3 are as follows:

1. The Sender performs the process of hashing algorithm to generate a message digest of a message that is contained in a document that will be sent.
2. After the hashing is done, Sender did sign against the message digest by using the public key that was used to create the digital signature.
3. Then Sender sends the digital signature together with the document to the Receiver.
4. The Receiver receives a message sent by the Sender.
5. After that Receiver verify messages sent by Sender. On the verification process messages in advance resulting hashing the message digest and digital signature will be on the private key using unsign. If the message digest his equal, then this message is genuine and the message came from the sender. When the message was modified by outside parties, then the message digest also changes.

2.5 Hash Functions

A hash function is a function that receives input in the form of an arbitrary length string and converts the input into strings that have a fixed length and generally being smaller than the original length. The output of the hash function is also called a hash value or message concise (message digest). A hash function is a one way function that can produce a characteristic (signature) of the data. Changes one bit alone will change the hash output dramatically. A hash function is usually used to ensure the integrity and digital signature.

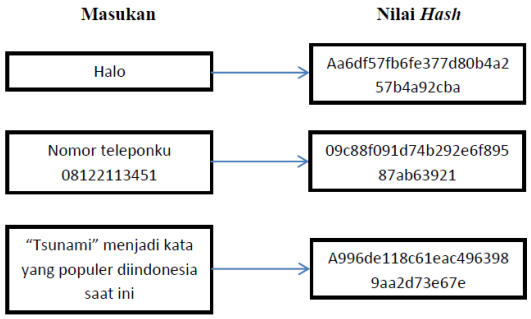


Figure 4. Example Usage Of Hash Function

In Figure 4, shows the hash function that converts a string of any length into a message digest that have a fixed length. Hash function basically works in one direction, it means the original message or the original message will be converted into a message digest, but the message digest that is generated can not be returned into the original message or the original message back. The sender and receiver have a way so that the integrity of the data can be investigated, the parameters of commonly used hash functions can be seen in table 1 as well as a list of hash function algorithm on table 2.

Table 1. Hash Function Parameters

Parameter	Keterangan
M	Pesan
h	Fungsi *hash*
y	Merupakan *h(M)* atau *message digest*

Table 2. List Hash Function Algorithm

Algoritma	Output size	Internal state size	Block size	Lenght size	Word size	Collision
HAVAL	256/224/192/160/128	256	1024	64	32	Yes
MD2	128	384	128	No	8	Almost
MD4	128	128	512	64	32	Yes
MD5	128	128	512	64	32	Yes
PANAMA	256	8736	256	No	32	With flaws
RIPEMD	128	128	512	64	32	Yes
RIPEMD-128/256	128/256	128/256	512	64	32	No
RIPEMD-160/320	160/320	160/320	512	64	32	No
SHA-0	160	160	512	64	32	Yes
SHA-1	160	160	512	64	32	With flaws
SHA-256/224	256/224	256	512	64	32	No
SHA-512/384	512/384	512	1024	128	64	No
Tiger(2)-192/160/128	192/160/128	192	512	64	64	No
VEST-4/8	160/256	176/304	8	80	1	No
VEST-16/32	320/512	424/680	8	88	1	No
WHIRLPOOL	512	512	512	256	8	No

Hash functions have the following properties:

1. *Preimage resistant*
   If given a hash value for *y*, it would be hard finding *M* such that *h (M) = y*
2. *Second preimage resistant*
   If a given input *M*, will be hard to find *M '* such *that h (M) = h (M ')*
3. *Collision resistant*
   It will be hard to find *M* and *M '* such that *h (M) = h (M ')*

2.6 Secure Hash Algorithm-256 (SHA-256)

Secure Hash Algorithm-256 hash type is one that is still commonly used. This function is a variant of SHA-1, SHA-256 is made because it has found a clash of SHA-1, SHA-1 is the successor of SHA-0.

Up to this point no one can solve for the SHA-256 algorithm. SHA-256 is generally used as a function between to other functions, including the MAC, the HMAC hash functions, and some of the functions of producing a digital signature [3]. The main function of SHA-256 can be seen in Figure 5.

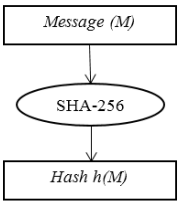


Figure 5. The main function of SHA-256

2.7 RSA

RSA discovered by three men who later shortened to RSA. The third inventor it was Ron Rivest, Adi Shamir, and Leonard Adleman. Asymmetric algorithms including RSA, which means it has two keys, i.e. the public key and the private key [7]. RSA cryptographic system the most popular public-key as it is the first system that at once can be used for key distribution, confidentiality and digital signature. RSA key generation parameters can be seen in table 3.

Table 3. RSA Key Generation Parameters

Parameter	Keterangan
p	Bilangan prima
q	Bilangan prima
n	Merupakan hasil dari $p \times q$
ø (n)	Merupakan hasil dari $(p-1) \times (q-1)$
e	Dengan ketentuan, gcd (ø (n), e) = 1 gcd = *greatest common divisor*
d	e^{-1} *(mod ø (n))* Menggunakan algoritma *extended euclid*
Kpublik	*(e,n)*
Kprivat	*d*

After the public key Kpublik raised by decrypting, then anyone can use the public key. RSA encryption algorithm using exponential functions in the modular n, as described in table 4.

Table 4. RSA Encryption Algorithm

Algortima Enkripsi RSA	
Input	*Kpublik = (e,n)*
Output	$C = P^e \bmod n$ Menggunakan algoritma *square and multipy*

As with encryption, RSA decryption algorithm is a modular exponential function of n by using the private key, as described in table 5.

Table 5. RSA Decryption Algorithm

Algortima Dekripsi RSA	
Input	*Kprivat = d* *Kpublik = (e,n)*
Output	$P = C^d \bmod n$

2.8 Discussion

The system to be built can be accessed by the officer and head of Office of BPN Cimahi, whereas the appellant only place the PIN through the officer where the system architecture to be built illustrated in Figure 6.

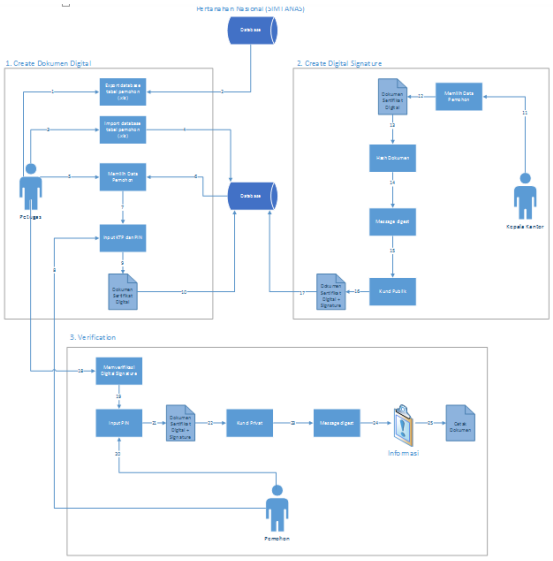


Figure 6. System Architecture

1. *Create* Digital Documents
   The first officer will download the applicant's export data formats (*.xls*) that emanate from the applicant table on database Sistem Informasi dan Manajemen Pertanahan Nasional (SIMTANAS) has existed in BPN Cimahi, then the officer will download the import file (*.xls*) to the system, the officer will create digital documents belonging to the appellant when the appellant came for the second time to the BPN, but before the officer asks the applicant to enter KTP and PIN when going to create digital documents. KTP and PIN are used to generate a public key and a private key.

2. Create Digital Signature
   The Head Office will download digital certificates document hash has been create by using the SHA-256 algorithm, the result of documents that have a hash will produce a message digest. The next process that is processing the message digest with the public key that has already been kind in before using the RSA

algorithm. After this process is complete, it will produce a signature of the digital certificate.

3. Verification

Verification is performed when an applicant coming for a third time, when the document belongs to the applicant is missing or damaged, the officer verifies the document digital certificate which has been issued a digital signature by the head office by asking the applicant to enter the same PIN with the PIN that you have made previously, the process of verification is made to ensure the validity of the certificate is a digital document that this land is truly from head office. Verification will use the private key to process a document that has been issued a digital certificate is a digital signature using the RSA algorithm, the output of this process will generate a message digest.

If the message digest of the document's hash process digital certificates are performed by the Head Office of the same as the message digest generated from the process of verification, then the system will give you information that the document was successfully verified and the digital certificate of the land document can be directly printed for the purposes of the applicant, but if the results of massage digest generated from a hash process is not the same as massage digest generated from the process verification , then the system will give you information that the document fails to be verified.

2.8 The Process of Hash

On the process of using the hash algorithm SHA-256 message digest for producing of a data message, a document already in the digital certificate hash can be seen as table 6.

Table 6. The Results of Message Digest Document

Input dokumen	*Massage digest* (*Hex Format*)
Sertifikat_4802002.pdf	ec660b8304c12dfabf0b6df01ec352ee26d5249ff5f7e273dca39e0d6cec9884

2.8 Key Generation Process

Key generation process uses the RSA algorithm, which would later produce the *p, q, n, (n), ø e, d, Kpublik*, and *Kprivat*. The following will explain more about the process of the algorithm the RSA key generation:

1. Number KTP used as a *p*, a description of the number KTP can be seen in Figure 7.



Figure 7. Number KTP

Number KTP just taken the last 6 digits only, because if the initial digit take there is a possibility for the number is equal to the number KTP belonging to another person, where the two-digit province code early, then followed with a two-digit code of the county or city, and the next two digits are the code sub. Thus the last 6 digits where selected two-digit initially consists of the year of birth and the next four digits is the number a computerized numbers definitely unique. As for *q* using the 6-digit PIN. In relation to *p* and *q* have to prime numbers, then if *p* and *q* are not prime numbers will be used next prime function to get the number of prime numbers before.

For example *p* = 3273020312500032 *q* = 210195, and *p* taken 6 last digit being 500032, on *p* and *q* is not prime numbers then look for the next prime number. The obtained *p* = 500041 and *q* = 210209

2. Search *n*, where *n* is the modulus being used.
   $n = p \times q$ = 500041 × 210209
   = 105113118569

3. Count ø(*n*) = (*p* − 1) × (*q* − 1)
   = (500041 − 1) × (210209 − 1)
   = 105112408320
4. Public key (*e*), where e is the public exponent (often called encryption exponent). so the value of the e relative prima against *ø (n)*, for example was determined *e* = 7
   A value of 7 was chosen because eligible *gdc* (105112408320,7) = 1
5. Private key (*d*) using the equation *d. e* = 1 (mod *ø (n)*). Note that *d. e* = 1 (mod *ø (n)*) is equivalent to *e.d* = 1 + *k ø (n)* so that in a simple d can be computed by *d* = (1 + (*k ø (n)*)/*e*. With the formula on the value can be:
   d = {1 + (*k* × 105112408320)}/7 with *k* = 1,2,3, 4, ... *n*. By trying the value *k* = 1,2,3, 4 ..... *n* so obtained *d* round, selected *k* = 2, produce:
   d = {1 + (2 × 105112408320)}/7
   = 30032116663
6. Then *Kpublik* = (*e*,*n*) = (7, 105113118569) and
7. *Kprivat* = (*d*,*n*) = (30032116663, 105113118569)

2.9 Encryption Process

The encryption process uses the RSA algorithm takes the value $e = 7$ and $n = 105113118569$ has been resurrected before. Next break down the message digest is generated from a hash process certificate documents the land into blocks of $P_1, P_2, ... Pn$. before break up message digest into smaller blocks, message digest is transformed into ASCII code beforehand as in Table 7.

Table 7. Conversion of Message Digest to the ASCII code

***Massage digest* dalam format Hex**	**ec6**60b8304c12dfabf0b6df01ec352ee26d5249ff5f7e273dca39e0d6cec9884
***Massage digest* dalam kode ASCII (*Pi*)**	**101 99 54** 54 48 98 56 51 48 52 99 49 50 100 102 97 98 102 48 98 54 100 102 48 49 101 99 51 53 50 101 101 50 54 100 53 50 52 57 102 102 53 102 55 101 50 55 51 100 99 97 51 57 101 48 100 54 99 101 99 57 56 56 52

Every character plainteks (P_i) encrypted into one block cipherteks (C_i) and $C_i = P_e \bmod n$ and given the separator dot (.) as in the table of 8 with $e = 7$ and $n = 105113118569$. For example, the process of message digest that is encrypted is **ec6** with ASCII code **101 99 54**.

Table 8. Encryption Process

Kunci publik	(e, n)
	$e = 7$
	n = 105113118569
Rumus Enkripsi	$C_i = P^e \bmod n$
Proses pemecahan dan enkripsi blok-blok P_i	$C_1 = 101^7 \bmod 105113118569 = 103267388890$
	$C_2 = 99^7 \bmod 105113118569 = 40817281514$
	$C_3 = 54^7 \bmod 105113118569 = 77567787156$
Hasil Enkripsi	**103267388890.40817281514.77567787156**

2.10 Decryption Process

The decryption process is done using the RSA algorithm, each block cipherteks (C_i) was changed back into a block plainteks (P_i) with the formula $P_i = C_i^d \bmod n$. Decryption is done by using the private key $d = 30032116663$ and $n = 105113118569$, then the block is decrypted as cipherteks on table 9.

Table 9. Decryption Process

Kunci privat	(d, n)
	$d = 30032116663$
	n = 105113118569
Rumus Dekripsi	$P_i = C_i^d \bmod n$
Proses pemecahan dan dekripsi blok-blok P_i	$P_1 = 103267388890^{30032116663} \bmod 105113118569 = 101$
	$P_2 = 40817281514^{30032116663} \bmod 105113118569 = 99$
	$P_3 = 77567787156^{30032116663} \bmod 105113118569 = 54$
Hasil Dekripsi	**1019954**

The block message digest is returned by way of similar results from decrypting the original message digest lookup as in Table 8. If it has been decrypted generate message digest (*M*') which is the same as the message digest (*M*) while the process hash, means the document received is the same document with the original.

Table 10. Results Decryption

***Input* (*C*)**	103267388890.40817281514.77567787156
***Output* (*P*) *Message digest* dalam kode ASCII**	1019954
Hasil *Message digest* dalam format Hex (*M'*)	ec6

From decryption as in Table 10 it can be concluded that the document received proved its authenticity, because the message digest of the decryption process is the same as the message digest of the original document when it will be encrypted.

2.11 Testing Results

Document authentication credentials do when the applicant requires a certificate the document back ground that has been lost or damaged. The applicant must enter a PIN that was created when the creation of digital documents is done. Testing authentication credentials document done to check that the document to be printed is a document that really still the original document when it is first created, the certificate is an original certificate data can be seen in Figure 8.

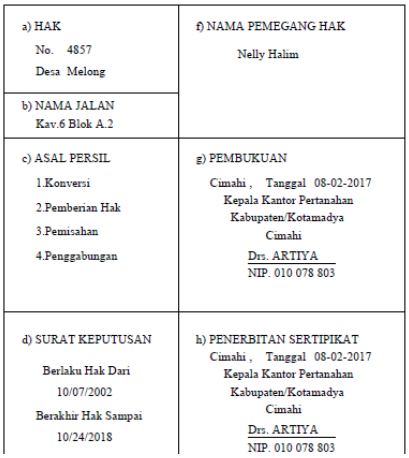


Figure 8. The Original Certificate Documents

When the applicant wants to print documents certificate of land and it turns out that the document has been changed as shown in Figure 9 the name of the holder of the rights whose origin is Nelly Halim transformed into Dadang Saep, then when the PIN is entered even though the verification is correct, but it will appear a notification that the document has been changed as shown in Figure 10.

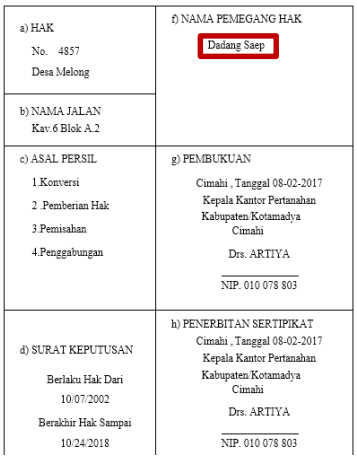


Figure 9. A certificate is a document that has been changed

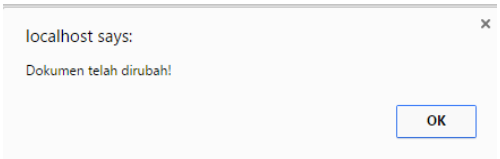


Figure 10. Notification Of The Document Has Been Changed

Based on the results of tests conducted with the test case, the conclusion that can be drawn if the data entered is correct, then the system will produce output according to expectations. If the data entered is wrong, then the system will show the error message correspond to faults.

3. CONCLUSION

Based on the results and the testing that has been done then the conclusion can be obtained as follows:

1. The application of the mechanism of creation of digital documents in the system can provide alternative services to publish digital documents.
2. The implementation of the security mechanism of digital signature can provide security services in the form of authentication documents are applied on the digital documents of the applicant by the head office so that applicants can determine the validity of the documents received.

As for a few suggestions for the development of the system, such as:

1. The need for the integration of database systems that are built into Sistem Informasi dan Manajemen Pertanahan Nasional (SIMTANAS) has existed in BPN Cimahi in order for the applicant's data be updated more easily.
2. The need for the development of a digital signature with certificate author (CA) to create a digital signature mechanism.

BIBLIOGRAPHY

[1] Isvarahadi, Fansiskus Asisi Tri. "Implementasi Digital Signature Menggunakan LSB Embedding untuk Uji Keutuhan, Otentikasi dan Penyangkalan Dokumen Pertanahan Digital", Universitas Kristen Satya Wacana.

[2] Dwiperdana, Aditia, "Cryptographic Hash Function dan Penggunaannya Dalam Digital Signature", Institut Teknologi Bandung.

[3] Azhar, Hanifah, “Perbandingan Algoritma Fungsi Hash MD5 dengan SHA-1”, Institut Teknologi Bandung.

[4] Pratama, Aditya, “Studi Perbandingan dan Implementasi Kombinasi Fungsi Hash dan Kriptografi Kunci-Publik”, Institut Teknologi Bandung.

[5] Bin, Ladjamudin, Al-Bahra, Analisis dan Desain Sistem Informasi, Yogyakarta : Graha Ilmu, 2005.

[6] Basharat, I, et al., "Database Security and Encryption: A Survey Study", International Journal of Computer Applications. vol.44, pp. 888-975, June 2012.

[7] Munir, Rinaldi, Kriptografi, Bandung : Informatika, 2006.

[8] Kromodimoeljo, Sentot, Teori dan Aplikasi Kriptografi, Jakarta : SPK IT Consulting, 2010.