Implementation Of Digital Signature On Banking

Nurul Hamdi[1] , Junidar [2]
[1] Lecturer of Department of Informatics Engineering, Faculty of Computer Science Ubudiyah Indonesia University, Jalan Alue Naga Desa Tibang, Kota Banda Aceh, Indonesia.
[2] Lecturer of Department of Management Informatics, Faculty of Math and Science Syiah Kuala University, Jalan Teuku Nyak Arief, Darussalam, Kopelma Darussalam, Syiah Kuala Kota Banda Aceh, Indonesia.

nurulhamdi@uui.ac.id , [b)] junidar678@unsyiah.ac.id

ABSTRACT

Abstract-one of the advantages of doing business in the internet world is can he do trade transactions where and at any time, without the presence of physical or face to face directly. In terms of profit in its own problems arose, mainly related to authentication. Bagaimanapenj ual can rest assured that the purchased product is the correct person or how the seller know that the credit card used the buyer is legitimate credit card hers. The example above is one of the problems in the internet world you can finish with a digital signature. There are still many more problems in the internet that can be solved with the use of a digital signature or digital signature misalnyadi the field of ecommerce, internet banking and more.

Keyword:D igital Signatures, internet, e-commerce

INTRODUCTION

The development of information technology in modern times very quickly. Computer technology facilitate transactions with the customer does not have to meet now with computers can do transaction by utilizing internet networks so that the customer does not need to come to Office.

The Internet as a highway of information (the information highway) has been felt really bring about change in many aspects of human life. This new technology offers many advantages and at the same time can also be a threat.

We would have many utilize the facilities that exist in the internet and may be one of these online transactions facility. Of course, often times we do online shopping on sites that provide online shopping facilities But perhaps we

Forget that the internet is a jarini anpu Republic unsafe transaction bisft ' only a person with illegal change the contents in such transactions. Without good security facilities, the recipient will receive the transaction order order order tersebt without suspecting any change. Therefore needed a facility to guarantee the security of transactions dilakuka the sender and the recipient is a vald. In the discussion this time we will expose the use of Digital Signature in financial transactions online.

THE INTRODUCTION OF DIGITAL SIGNATURE

A. About Digital Signature

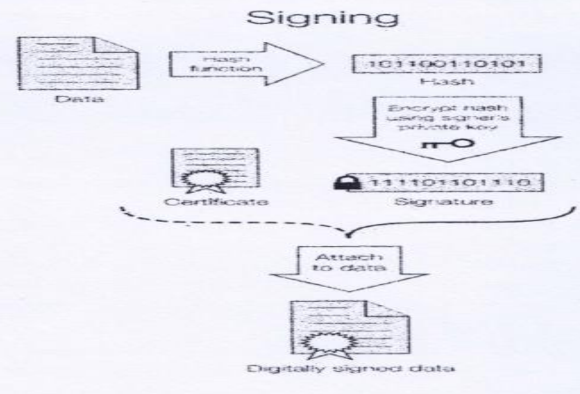
A Digital Signature is one of the technologies used to enhance network security. A Digital Signature has a function as a marker on the data which ensures that the data is the data that sebenamya (nothing has changed). That way, the Digital Signature can fulfill at least two terms of network security, namely Authenticity and Nonrepudiation.

A Digital Signature is a way of working by leveraging two key i.e. a public key and a private key. The public key is used to encrypt the data, while the private key is used to decrypt the data. First, document-hash and generate Message Digest. Then, the Message Digest is encrypted by the public key into a Digital Signature.

To open the necessary Digital Signature private key. When the data has been modified by outside parties, then the Digital Signature also changed so that the existing private key will not be able to open it. This is one of the terms of the keaman network, namely Authenticity. Meaning, the authenticity of the data can be assured of the changes-changes made to outside parties.

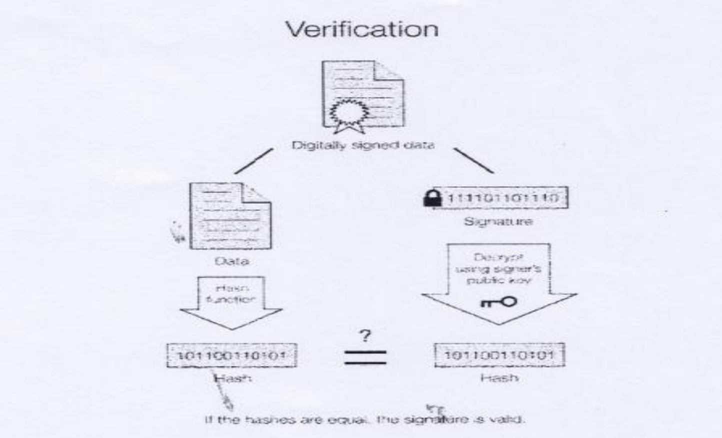
As has been explained earlier scheme of digital signature consists of three processes:

1) Key generation Process. This process of choosing a random private key from a collection of private keys is possible. Basil of this process is the private key and the corresponding public key.
2) The process of awarding of the signature. The process of inimenerima the contents of the message and the private key, thus generating a signature.



Gambar 1 Pemberian tanda tangan

3) The process of verifying the signatures. This process verifies the message signature that has terbubuhi. The process of verifying this takes the public key.



Gambar 2. Verifikasi Tanda Tangan

E-BANKING AND THE CHALLENGE

Talking about e-banking, will not take off from the internet banking. After ATM and phone banking and banking world, now comes jugadengan internet banking. This technology is the answer to the challenges the world community who want a modem lifestyle increasingly easy, fast, reliable, convenient, and cheap.

Internet banking services allow clients to perform almost all types of banking transactions over the internet, particularly via the web site. Through this means, any person can do some checking accounts, transfer funds, purchase vouchers, mobile telephone bill payment account until the electricity, telephone, and water.

Internet banking has existed in the world since the year 1994. Stanford Federal Credit Union was the first financial institution in the world to use the internet banking through its website which was released in October 1994. Currently, most of the major banks in Indonesia has been providing internet banking services.

As the development of the internet, internet banking is starting to become a prima donna among bank clients after ATM and phone banking. The ease of dealing with comprehensive features without hams out of the home, is the internet banking advantages that cannot be matched only by other e-banking technology.

A. Security threats

Although it offers convenience, nonetheless there are security threats that lurk. Typically, this threat is addressed to the user who is nota bene's weak awareness of tech. Some of the threats that often arises, among other things:

B. Typo-site or website forging

Is the technique of creating a site that has a domain and look similar to situsaslinya. The goal, get usemame and the user's password. For example, a site with the name netbank.com. Twinning the site usually have similar names, such as: net-bank.com, net_bank. com, or netibank.com.

C. Key-logger

Is a virus or trojan is hidden and is in charge of recording every key typed user input keyboard. This application is embedded in a computer unbeknownst to users and is in charge of getting the usemame user and password access to a website.

D. Man in the middle attack

the activity of a cracker (hacker term for evil) who to tap information from the user. The information could be intercepted password, usemame, and electronic messages. These events usually override the users who use public computers such as Internet cafes and surroundings free hotspot.

E. Prioritizing

In this world there is no one hundred percent secure. Despite that, the bank always strive the best in terms of security of customer sites and online transactions. Some of the techniques commonly used by security bank, among others:

1) Application of the technology of secure socket layer (SSL) 128 bit and secure HTTP {HTTPS), which serves mengenskripsi information that is sent to users. So, when it happens to man in the middle attack, information remains secure and cannot be read by a bug.
2) Complement the borrowers with additional safeguards in the form of address token PIN. This tool is berfungsir. generate the PIN that always changed when the customer when doing transaction.
3) Install the certificate on its website as an additional protection. So, customers can tell the difference between genuine and bogus sites sites by seeing a warning in your browser.
4) The use of firewalls and antivirus to prevent ak: illegal banking network in the ses.
5) Application of Digital Signature on idenitas charging, e.g. created a web portal identitass which users can enter information about him. From the information submitted ditambabkan signatures. The portal and the user is given a key, more precisely the private key from the key generation. The user it should really remember that, because the private key using the user's private key can perform the register on some websites.

But despite the bank as the provider of the internet banking service has improved its services, pengainanan still the most padded target is a user of the service. The point of weakness is on the lack of awareness of tech users. For example, users share the PIN code, always click "Yes" when the notification appears on your computer, and forgot to logout.

IMPLEMENTASI DIGITAL SIGNATURE IN THE BANKING WORLD

The future is increasingly pointing to the use of a digital document and digital signature. The speed of the bank in adopting new technology is not as important as the quality of the solution that diaodop sibank. The Bank should think to consider a new information system attributes to ensure it can operate with existing systems.

Technology. digital signature is the equivalent of a written signature on a written document. The e-commerce market is generally focused on digital signatures as an important component. This is, in large part, because the digital signature authentication, troubleshooting a non-rejection and the integrity of the message.

Online transaction value growth shows indicates that the e-commerce and digital signature is an area that can be in the broader eksplore by the bank. However, due to the complexity of digital signature technology, then it is very important that the bank should conduct careful research in the planning before implementation.

We will elaborate on the four issues that are most critical for financial institutions to consider when going to implement digital signature technology.

A. The Bank will develop a digital signature technology should be careful in selecting vendors and adopt his solution.

Because of the large initial cost and ongoing, then very rare banks will choose to develop their own digital signature technology. Thus the choice of the most appropriate is the bank will perform a digital signature function outsourcing rent or buy its functions by blending with existing infrastructure.

A number of new vendors have emerged as a result of the increasing demand for digital signature technology. Unfortunately, a solution from a vendor may not be compatible with existing bank system is up and running. Interoperability, now and in the future, should be the primary consideration.

Lack of inter operability standard and too little can lead to failure of the end of the purchased system. According to consulting firm Gartner Group, "... 30% to 40% of the community's major infrastructure deployment will fail within two years of the launch because they failed to show the value. This means banks that involves a certificate authority (CA) may find themselves using a digital signature that is unverifiable or information systems that do not have technical support. The Bank must do duediligence comprehensive digital marketing solutions on each signature belongs to the vendor.

B. Employ the use of digital technology, the need for updates on services and policies of the bank.

When the bank decided to apply a digital signature, the bank should also apply to digital documents and requirements related to, among others, document management, storage, security, access, hardware periodic upgrades, and recovery facilities disaster. Furthermore, implementing bank could incur additional costs as a result of the need for more staff in the form of new technology management position.

After the bank decided to apply a digital signature, the bank has made a strategic decision to maintain digital records and documents of the digital service. Maintain digital documents will require new policies and procedures, and introduce new complexities that are associated with system upgrades and conversion information.

If digital documents are used, the customer will require reasonable access to documents. In addition, if the bank chose to implement remote access to digital documents, the bank may need to set up a secure information area that allows access to customers.

C. A bank can operate services CA (Certificate Authority) to customers. However, being a CA may require different technical skills

While banks routinely verifying the identification of existing customers and new, the electronic authentication process is more complex, and the decision to operate the CA is heavier. The main role of the CA is for issuing and verifying digital certificates. the issue of the certificate of the CA that is used, in part, to verify the authenticity of the user digitally signed or encrypted.

There are advantages and disadvantages associated denganbank be CA (see below). A thorough review over these things should be included in decision-making efforts of a bank.

Becoming A Certificate Authority:

1) Advantage

- Set the identity of the bank.
- The technology is relatively inexpensive.
- Add the potential for customer retention.
- Provides for community outreach.

2) Deficiency

- The standard is still changing.
- Require additional costs to operate the service.
- Need more technical expertise.
- Make potential new liability for the bank.

CA operations require additional facilities for the hardware, operating policies and procedures, disaster recovery systems, security and attention to managing and monitoring of the revocation list over unauthorized access.

D. Hardware and software in support of digital signature and digital document will become obsolete and require replacement.

Hardware and software will surely become obsolete. Lifetime of the computer hardware is about three to five years. The functional life of the software being shorter, often only six months to a year. If the bank does not upgrade and replace older equipment, the bank could operate at a disadvantage.

CONCLUSION

As for the inferences that can be drawn are: digital signature Technology is one solution to record transactions in the banking world but in its application to the world of banking should be considering some important factors are:

1. The Bank will develop a digital signature technology should be careful in selecting vendors and adopt his solution
2. Employ the use of digital signatures requires updates to a set of technologies, services and policies of the bank
3. A bank can operate services CA (Certificate Authority) to customers. However, being a CA may require different technical skills
4. Hardware and software in support of digital signature and digital document will become obsolete and require replacement.

BIBLIOGRAPHY

[1] fdic.gov/regulations/information/fils/banktechbulletin.html www.

[2] Andi, understand Encryption & Security Model Data, 2003

[3] Ahmad Redi, Electronic Signatures in e-commerce in the banking sector, FHU UI, 2009

[4] William Foe, Digital Signature and e-commerce. 2008