Journal of Contemporary Issues in Business and Government Vol. 27, No. 2,2021
https://cibg.org.au/
P-ISSN: 2204-1990; E-ISSN: 1323-6903
**DOI: 10.47750/cibg.2021.27.02.237**

# RESEARCH AND APPLICATION OF DIGITAL SIGNATURES IN E-COMMERCE TODAY

**Nguyen Thi Thoi**
FPT University, Vietnam
*Email: ThoiNT4@fe.edu.vn*

**Abstract:** Nowaday, the digital age is expanding with the strong development of 4.0 Industry. The transformations of the flat world force businesses to have solutions to handle their works quicker, safer, more efficient, convenient and with high security so that they can trade goods. Declare tax, contracting, etc. all data are digitized in order to be easily stored, retrieved and accessed. To resolve the mentioned problems, the research topic "Researches and applications of digital signatures in Nowaday E-commerce" will explain what digital signature is, the application of digital signature (tokens) in e-commerce, hence, provides methods and goals to users, creates premises for higher development in Information Technology.

**Keywords: age 4.0, digital signature, electronic Signature, information technology, token.**

## 1. INTRODUCTION

We live in the digital age, all problems are solved by simple operations. Along with the rapid development of information technology and artificial intelligence, e-commerce is also gradually asserting its importance in the world today.

In the past, the implementation of signing economic contracts, transactions, taxes, etc.often businesses would adopt a hand signature and the company's seal. Or, when making customs declaration, enterprises must create a number with documents and pictures and wait for the reviewer, all transactions in banks also need to have personal signature. This leads to the complicated process of signing, printing and shipping documents to customers, affecting the length of the contract completion time.

Starting from 2018, according to Decree 130/2018 / ND-CP - Detailed regulations on the implementation of the law on electronic transactions and digital signature authentication services. Along with Circular 16/2019 / TT-BTTTT regulating the list of compulsory standards for digital signatures [2]. According to Nguyen (2013), digital signature is a form of electronic signature, with high safety and widely used. Digital signatures were developed on cryptography theory and asymmetric encryption algorithms. Digital signature that is widely developed and applied today is based on public cryptographic algorithm (RSA) algorithm, which is an important basis for forming public key infrastructure (PKI) to enable users of an insecure public network such as the

P-ISSN: 2204-1990; E-ISSN: 1323-6903
**DOI: 10.47750/cibg.2021.27.02.237**

internet securely exchanges data and money, through the use of a public and secret key pair issued, using through a certificate authority ( CA) is legally recognized [3].

Today, digital signatures are divided into two categories. The public key is the public information of the customer. Type of private key (private key) this is the confidential information of the customer, used to create a digital signature. The use of the USB token hardware device is essentially intended to store and secure this secret key. The application of digital signature is also gradually popular through the forms such as digital signature for electronic customs, digital signature to support tax return submission, digital signature of social insurance, etc.

## 2. RESEARCH CONTENTS

### 2.1 Overview of e-commerce

E-commerce is a combination of business activities, sale, purchase, information exchange, ordering, advertising, etc.by electronic means.

### 2.2 Outline of digital signatures

Digital signature is information attached to data for the purpose of confirming the identity of the sender of that data and asserting whether that data has been changed or not. A digital signature is a form of electronic signature, with high security and widely used and developed on cryptographic theory and asymmetric encryption algorithm [5].

### 2.3 Digital Signature Shape

The digital signature is shaped like a USB, also known as the USB token, used to create a pair of public keys and secret keys to store customer information.

### 2.4 Literature review

Based on Hoa (2010), it is not only applied in the fields of e-commerce, digital certificates but also used as an identity card. For developed countries, people will integrate ID numbers into chip cards in credit cards, identity cards to ensure safety, limit fraud and cardholders have the right to identify their identity. people on public systems such as ATM withdrawal, bus, customs declaration, electronic protection, etc. [3].

When sending an e-mail, to your business partner that uses an electronic signature, your partner can fully trust the authenticity of that e-mail. Because the electronic signature ensures that e-mail is of the correct sender, it is completely not tampered with or stolen information from a third party or someone. However, to ensure this factor, the sender and receiver must use the same digital certificate system.

### 2.4 The advantages and disadvantages of digital signature application in e-commerce today

2.4.1 Advantages

Digital signature is considered the most preeminent solution for businesses today. The benefits it brings in e-commerce such as the ability to control access instead of usernames and passwords, and digital signatures allow for better access control capabilities. In addition, the digital signature can identify the source of the information recipient and is able to confirm the sender when performing electronic transactions. Besides, it creates data integrity to ensure that the content on

P-ISSN: 2204-1990; E-ISSN: 1323-6903
**DOI: 10.47750/cibg.2021.27.02.237**

the text is not edited or tampered with. The receiver can check the integrity of the data when received from the sender. On the other hand, undeniableness will resolve the irreversible situation of digitally signing non-corrected documents.

In a transaction, a party may refuse to receive a text that is sent by itself. To prevent this possibility, the receiver may ask the sender to include a number with the text. When there is a dispute, the recipient will use this signature as evidence for the third party to resolve. An additional last advantage that makes digital signatures more valuable is the legality of digitally signed electronic documents with the same legal value as a paper document signed with a handwritten signature. The solution using digital signatures is optimal because it has legal effect, so there is no need to print the document but still can verify the document, ensure its integrity and not deny it.

Digital signatures issued by a third party that is an authority that issues, revokes, and manages digital certificates for entities performing secure transactions (certificate authority or CA) should ensure computation. objective. Thus, the process of creating digital signatures, validating legal requirements, including signature authentication, message authentication, is successful and effective [3]. Because of the advantages of digital signature, it is used in many applications to ensure communications security, online banking, e-commerce, ensure security for email, etc.

2.4.2 Disadvantages

In addition to the outstanding advantages that digital signatures bring in the current e-commerce market, there are still a few limitations that exist in the proof if there is an error or tampering. cases rarely happen, but we also need to avoid and anticipate. If the digital signature is forged, or something goes wrong that makes the verification of the user incorrect, it will be difficult to prove and verify the digital signature. However, this is also an unavoidable limitation for high-tech verification.

The most effective measure to overcome this limitation is to improve the security and certainty of digital signatures, to minimize risks for users.

## 3. METHOD AND SCOPE OF RESEARCH

This research paper is used the research method of investigating, comparing and comparing documents through statistics, surveying questionnaires with businesses operating in Binh Duong, Bien Hoa city, Dong Nai province and Ho Chi Minh City and specialized materials related to the topic in Vietnamese and English.

## 4. RESEARCH RESULTS

Survey form is based on survey results from google forms. Based on the survey questionnaire with fifty (50) companies in Binh Duong, Bien Hoa City-Dong Nai City and Ho Chi Minh City, there are quite satisfactory results on the application of digital signatures in commerce. electronic current.

Based on the chart, we can see that digital signatures have many practical applications in e-commerce today. Not only convenient, easy to use, but also has many features that make daily operations easier.

P-ISSN: 2204-1990; E-ISSN: 1323-6903
**DOI: 10.47750/cibg.2021.27.02.237**

Next is the survey chart of user satisfaction through practical applications that digital signatures bring in e-commerce with the following survey results.

Based on the chart, we can see that the survey results with fifty (50) people, the very satisfied data is 22%, the satisfaction level is 72%, and the dissatisfaction level accounts for 6%. Thus, we can see that with new features, modern and easy to use, we have received positive feedback from users. However, there are still a few users who are still not satisfied with the feature that digital signature brings.

## 5. DISCUSSION

### 5.1 Practical application of digital signature in e-commerce

Currently, digital signature is widely used to replace hand signature in e-commerce transactions in digital environment. In legal terms, the digital signature has the equivalent value of personal fingerprints, red carpentry and the signature of the representative for the business.

Digital signature in Vietnam can be used in all transactions to buy and sell products online. The exchange of products through websites, signing orders by applying digital signatures in the form of SSL (secure socket layer) transactions, helps to transmit information securely over the internet.

In addition, the application of digital signatures in securities is also a time-saving form of exchanging personal information. With new features such as encryption using a public key - private key will increase security. The public key is used only for encryption, and the private key only you can decrypt the information. Using this encryption will help prevent ourselves from stealing personal information [8].

Bank transfer and electronic payment are no longer too strange things in the digital age. With endless benefits is to use public key infrastructure (PKI). For this public key infrastructure application, it will be built on the basis of allocating a public-private key pair. In which only one key is used to encrypt the message and only the other key can decrypt the message and vice versa.
In addition, according to the regulations issued in Circular 16/2019 / TT-BTTTT, the list of mandatory standards applicable to digital signatures of the Ministry of Finance has also applied digital signatures to electronic customs procedures. such as declaring customs without having to print the declarations, affix the red carpentry of the company.

Public digital signature authentication service can only be used in electronic transactions related to individual users, organizations, businesses, in transactions between people, enterprises and agencies. government officials. Particularly, internal transactions of state agencies or between state agencies are specific transactions, not using public authentication system but must use a separate system [9].

### 5.2 Forms of using digital signatures

In the digital age, we are gradually eliminating hand signatures in all types of transactions. But we need a signature that can replace a hand-drawn signature with a reliable, authentic, authentic form. New technologies using digital signature encryption were born. The purpose is to replace hand signatures in digital age transactions.

Digital signature is information attached to electronic data such as Word, Excel, PDF, images, videos for the purpose of verifying the owner of such data. Technically speaking, digital signatures are based on a public cryptographic infrastructure (PKI). In which, the decisive part

P-ISSN: 2204-1990; E-ISSN: 1323-6903
**DOI: 10.47750/cibg.2021.27.02.237**

for all encryption is the public RSA encryption algorithm [8]. This modern technology helps users to ensure that the digital signature created is unique, cannot be tampered with, and only the owner of the secret key can create the digital signature.

The secret key is generated if the person subscribes to the service and is stored in a hardware device called a token or smartCard. The device makes the secret key securely stored, cannot be copied or duplicated and cannot be penetrated by viruses.

When you want to verify who created the digital signature, if you receive digitally signed electronic documents, you need to have an authentication service provider certify that the signature is due to a particular person. somehow create. Similar to conducting electronic public transactions such as tax declaration, customs declaration, the user is an individual, agency or organization must use a public digital signature authenticated by the service provider. public level digital signature [5].

## 6. RECOMMENDATIONS

Currently, the implementation of the main practice papers such as household registration book, visa, identity card, also known as identity card. Then the majority of employees will have to go to committees and administrative agencies to perform. The completion of the procedure has to go through many common steps such as picking numbers, waiting for the queue to pay fees, waiting for the names to sign documents, .. it takes a lot of time. The proposed proposal is an application that integrates digital signatures with identity cards, also known as identity cards. Easily complete administrative procedures, pay fees online without the need of issuing agencies or committees to wait for cumbersome and complicated procedures.

In addition, the use of digital signatures in the specialized digital certificate management software of the Ministry of Health in the process of examining and treating patients. Make electronic medical records, pay online. On the other hand, the digital signature will apply directly to the management of people participating in health insurance and online social insurance. Applying modern technology in hospitals, helping to minimize complicated procedures.

Suggestions for applying digital signature in e-commerce. With the advantages that it brings, we will give us complete access to information technology. Creating a digital age, a paperless society.

## 7. CONCLUSION

Digital signatures have a profound influence on the world economic market in general and the e-commerce market in Vietnam in particular. We cannot deny the benefits it brings to us through economic transactions, market surveys and other forms of activity. Although this topic has been studied for a long time, to convert digital signatures to popularization, it will take a lot of time to change the high technical level, as well as the ways of using it to become simpler and more convenient. .

## ACKNOWLEDGMENTS

The author of the article would like to thank individuals who completed the survey as well as ideas for contributions from colleagues.

P-ISSN: 2204-1990; E-ISSN: 1323-6903
**DOI: 10.47750/cibg.2021.27.02.237**

## REFERENCES

[1] Subramanya, S. R., & Yi, B. K. (2006). Digital signatures. *IEEE Potentials*, *25*(2), 5-8.

[2] Ateniese, G. (2004). Verifiable encryption of digital signatures and applications. *ACM Transactions on Information and System Security (TISSEC)*, *7*(1), 1-20.

[3] Halevi, S., &Krawczyk, H. (2006, August). Strengthening digital signatures via randomized hashing. In *Annual International Cryptology Conference* (pp. 41-59). Springer, Berlin, Heidelberg.

[4] Roy, A., &Karforma, S. (2012). A Survey on digital signatures and its applications. *Journal of Computer and Information Technology*, *3*(1), 45-69.

[5] Bansal, P. K., Begeja, L., Creswell, C. W., Farah, J., Stern, B. J., &Wilpon, J. (2014). *U.S. Patent No. 8,751,233*. Washington, DC: U.S. Patent and Trademark Office.

[6] Zhou, J., & Deng, R. (2000). On the validity of digital signatures. *ACM SIGCOMM Computer Communication Review*, *30*(2), 29-34.

[7] Alam, M., Chowdhury, S., Tehranipoor, M. M., &Guin, U. (2018, April). Robust, low-cost, and accurate detection of recycled ICs using digital signatures. In *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)* (pp. 209-214). IEEE.

[8] Bansal, P. K., Begeja, L., Creswell, C. W., Farah, J., Stern, B. J., &Wilpon, J. (2014). *U.S. Patent No. 8,751,233*. Washington, DC: U.S. Patent and Trademark Office.

[9] Anwar, M., Abdullah, A. H., Butt, R. A., Ashraf, M. W., Qureshi, K. N., &Ullah, F. (2018). Securing data communication in wireless body area networks using digital signatures. *Technical Journal*, *23*(02), 50-55.

[10] Kar, D. M., Ray, I., Gallegos, J., &Peccoud, J. (2018, August). Digital signatures to ensure the authenticity and integrity of synthetic DNA Molecules. In *Proceedings of the New Security Paradigms Workshop* (pp. 110-122).