



## LEGAL ISSUES OF PARTY IDENTIFICATION IN ELECTRONIC CONTRACTS

Gaybullaeva Zilola Gaybullo qizi <sup>1</sup>

<sup>1</sup> Master of Tashkent State Law University

<https://doi.org/10.5281/zenodo.4737697>

### ARTICLE INFO

Received: 20<sup>th</sup> April 2021

Accepted: 25<sup>th</sup> April 2021

Online: 30<sup>th</sup> April 2021

### KEY WORDS

*electronic transaction,  
electronic contract,  
electronic commerce,  
electronic message,  
identification, mobile  
number, electronic  
signature, public key, private  
key.*

### ABSTRACT

*This article provides information on the importance of identification, types of identification to ensure the security of the parties in electronic transactions, which are currently widely used by individuals and legal entities. It is also proposed to provide a broader definition of electronic signature, which is a means of identification in national legislation.*

It is known that in electronic transactions, the parties enter into a relationship from a distance without seeing each other. It is important that the parties make sure that each other is trustworthy as obligations arise in the middle and the burden of responsibility falls on them.

In this case, the parties must have identified themselves. Given that electronic transactions are concluded through electronic documents and electronic messages, it can be said that the most basic form of identification of the parties is the electronic signature.

According to Article 3 of the Law of the Republic of Uzbekistan "On electronic digital signature" and an electronic digital signature is a signature that allows the owner of a private key to be identified. [1]

Usually, the signature is the main document confirming the authenticity of the document. Signing ensures that its owner is compulsorily recognized through that

document. In e-contracts, too, the signature is as important as a regular signature, the relationship is paperless, completely online.

While the use of an electronic signature to ensure the identification of the sender and acceptor of an offer is as important as a signature in a simple contractual relationship, there is still a higher percentage of misunderstandings in society about the importance of an electronic signature and its ability to identify its owner.

In accordance with the legislation of Uzbekistan, the authenticity of an electronic digital signature must be verified in order to recognize that an electronic digital signature has the same value as a paper signature. , the electronic digital signature must be used for the purposes specified in the certificate of the electronic digital signature key.

Approved by the Resolution of the Cabinet of Ministers of June 2, 2016 No 185 "On measures to further improve the



implementation of transactions in e-commerce" "On the use of electronic digital signatures in contracts and storage of electronic documents and existing information in e-commerce According to the regulation, electronic digital signatures in the conclusion of contracts in e-commerce:

- Ensuring the circulation of legally significant electronic documents and identifying changes and terminating legal relations in the framework of concluding an e-commerce contract;
- to ensure the necessary requirements of information security, including to confirm the integrity and invariability of information after signing;
- should be used to ensure the identification of the owner of the EDS who signed the electronic document. [2]

The electronic digital signature consists of 2: open and closed keys.

The private key of an electronic digital signature is a sequence of characters generated using an electronic digital signature, known only to the signatory and intended to create an electronic digital signature in an electronic document, and the public key of an electronic digital signature is generated using an electronic digital signature. , is a sequence of characters that corresponds to the private key of an electronic digital signature, can be used by any user of the information system, and is designed to verify the authenticity of an electronic digital signature in an electronic document. A certificate is required to obtain an electronic digital signature. The certificate of the electronic digital signature key consists of a document confirming that the public key of the electronic digital signature corresponds to the private key of the electronic digital signature and issued by the registration center to the owner of the electronic digital signature private key. In short, in this way, the owner of an electronic digital signature can enter into a

relationship through an electronic signature in electronic contracts.

According to Article 9 of the Law on Electronic Commerce, electronic documents in electronic commerce, as well as information recorded in electronic form, which allows to identify the sender, are equated to handwritten paper documents and can be used as evidence of transactions. Because electronic digital signatures are considered to identify their owners, electronic transactions can be easily entered into with electronic signatures. [3]

But at the same time, transactions between citizens are not just about digital signatures. Individuals and legal entities also use other means of identification: subscriber numbers, e-mail, social network accounts. But the question must be answered as to whether these allow the identification of the parties under the law.

Article 9 of the Law on Electronic Commerce states that "information that allows to identify the sender is equated to documents signed by hand." It is understood that even with the information sent electronically, it confirms the authenticity of the sender. This is important in determining the validity of a contract. The reason is that the types of online services and the means of providing such services are increasing nowadays, and the question of whether they are a real contract should not remain open.

Now every retail store has pages on social networks. For example, the store "7rings.tashkent", which specializes in the sale of various jewelry and women's clothing, also accepts orders through the social networks Telegram and Instagram. It is understood that in online orders, the parties are identified through their accounts on these social networks. Because electronic information is also sent and received through social networks. However, realizing that the number of cases of cyber fraud is also increasing, when concluding an electronic contract, it is



advisable for the parties to request information that allows for additional identification, not just based on the messages sent by the other party. For example, it is necessary to verify the authenticity of messages sent through the social network account of the party receiving or ordering an electronic order, as well as his mobile number.

The point that a mobile number is a means of identification is reflected in the resolution of the President of the Republic of Uzbekistan in 2018 "On measures to accelerate the development of e-commerce."

The resolution states that "in order to ensure the effective operation of the mechanism of remote identification of customers by mobile number, by the end of 2018 the mobile network subscriber should develop and approve the procedure for maintaining a phone number when switching to another mobile network." [4]

This proves that the identification of the parties to the contract by mobile numbers is enshrined in our national legislation.

In addition, the resolution stipulates that electronic checks, receipts, messages and other methods generated by information systems in the process of providing services by e-commerce participants, identifying the parties to transactions, are equated to receipts, coupons, tickets and other documents confirming payment for goods (services). In this way, the parties can use electronic checks, receipts, messages as a means of identification. However, it is unclear what is meant by "other methods" in the decision.

Looking at foreign experience, there are 2 different types of electronic signatures in e-commerce relationships. The EU Electronic Signature Directive distinguishes between the electronic signature and the advanced electronic signature.

Electronic signature is an electronic information that communicates with other

electronic information and is a method of verifying them.

The advanced electronic signature must meet a number of requirements. These are:

- it is uniquely associated with its signatory;
- allow identification of the signatory;
- The electronic signature must be affixed using the only controlled means available.

You must also have a certificate of this type of electronic signature. [5]

However, this clause on ordinary electronic signatures is not included in the electronic signature law of countries with 2 different legal systems, such as Germany and the United Kingdom. However, according to the descriptions given in other sources, an electronic signature (a simple electronic signature) is indicated as a method of confirming an electronic message sent using various means.

In particular, in the US ESIGN act - Electronic Signatures in Global and National Commerce, an electronic signature is a logical contract or other information associated with an electronic sound, symbol or process for which it is intended to be signed (ratified). defined. [6] That is, not only an open and closed key signature approved by a specially authorized body with a certificate, but also other electronic methods used to certify a document can be an electronic signature.

For example, in order for a citizen to make payments using the Pay me program, he or she will first need to register through the program. In this process, a confirmation code is sent to the user's mobile number via SMS-code. The user then performs various operations by entering a code known only to himself. This code allows the identification of one of the parties in an electronic contract and can be taken as a simple electronic signature.

Based on these data, it can be said that the concept of "electronic signature" can be further



clarified in the legislation of Uzbekistan. Although not registered as an electronic signature, the Uzbek legislation lists methods and tools that allow identifying the parties to an electronic transaction. But the fact that they are in different documents and norms and are scattered can be confusing. A clear definition of this concept in a single definition can help make electronic identification easier to understand.

In addition, due to a lack of sufficient legal and financial literacy, in some cases, parties to an electronic relationship face fraud because they pass on their verification codes to others.

Especially since the beginning of the pandemic, the fact that many services have been transferred to the online form has also increased the number of cases of deception of the parties in electronic transactions and other electronic relations.

In April 2020, Uzkomnazorat, the State Inspectorate for Information and Telecommunications, issued a warning to the population: , ask about the card number and its validity period, find out the secret code received via SMS-notification, and then there may be cases of theft of money from their electronic account.

As a result of the increase in the number of bank plastic cards among pensioners and the disabled, criminals have been known to fraudulently obtain bank card numbers, send requests on behalf of social services and promise to pay special social assistance to the

card during quarantine. can misappropriate people's money.

The State Inspectorate "Uzkomnazorat" warns citizens not to be deceived by such "fake" SMS notifications, not to share personal information and important information on social networks, not to give it to strangers, to warn elderly relatives about such dangerous actions, the government's measures against the coronavirus pandemic and official and trusted sources. "[7]

**In conclusion**, in electronic transactions and contractual relationships, the parties need to better understand the importance of the information that allows them to identify themselves electronically, giving them to others so that other people can interact with the other party on their own behalf. Increasing e-literacy among the population can be a good help for this.

The Law on Electronic Signature also provides a detailed and clear definition of the means of identification of the parties, as well as a more complete definition of the concept of "electronic signature" as in US and EU law ("Electronic signature" only allows open and closed identification). signatures consisting of keys, but also electronic voice, symbols and processes that allow the identification of the parties) the essence of the concept of electronic identification should be clarified. This helps the parties to the electronic transaction to be active in the electronic relationship.

## References:

1. Law of the Republic of Uzbekistan "On electronic digital signature" Article 3, Bulletin of the Oliy Majlis of the Republic of Uzbekistan, No. 562-II 11.12.2003 // <https://lex.uz/docs/64467>
2. Resolution of the Cabinet of Ministers "On measures to further improve the procedure for implementing transactions in e-commerce", No. 185 02.06.2016 // URL <https://lex.uz/docs/2973939#2973995>



3. Law of the Republic of Uzbekistan No. ZRU-385 of May 22, 2015 "On Amendments and Addenda to the Law of the Republic of Uzbekistan" On Electronic Commerce ". // National Database of Legislation, 30.12.2017, No. 03/18/455/0492 // URL:

<https://www.lex.uz/acts/2650293?ONDATE=23.05.2015%2000#2650301>

4. Resolution of the President of the Republic of Uzbekistan "On measures to accelerate the development of e-commerce" Item 5, National Database of Legislation, 15.05.2018 // URL:

<https://lex.uz/docs/3744594>

5. The EU Electronic Signature Directive - <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l24118&from=EN>

6. US Electronic Signatures in Global and National Commerce, 2000, -

<https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf>

7. "Uzkomnazorat": fraudsters may become more active in the field of information due to the increase in non-cash payments // URL: <https://kun.uz/news/2020/04/21/ozkomnazorat-naqsiz-shaklda-tolovlar-hajmi-oshgani-tufayli-axborot-sohasida-firibgarlar-faollashishi-mumkin>