ELECTRONIC SOFTWARE USED IN PROVIDING PRIVACY

Abdusamatova Shahodat Khojiakbar's daughter
Informatics and information technology teacher of the academic lyceum under the Almalik branch of TDTU named after Islam Karimov phone: +998(93) 375 – 42 - 15 e-mail: abdusamatovashahodat@gmail.com,
Mannonov Asliddin Akbar's son
Student of cyber security faculty of TATU named after Al Khorazimi, phone: +998(97) 960-03-02, e-mail: asliddinmannonov0980@gmail.com.

Abstract: *This article presents the classification of electronic digital signature and its certificate, which are used to protect the privacy of the user*

Keywords: *electronic digital signature, digital certificate, user information, digital document.*

The current capabilities of information technologies have brought real life into the digital world, and this will further accelerate the process of information exchange. In order to create convenience for users, service organizations are improving network capabilities day by day. In order for the user to freely use the network, it should not only be safe and convenient in the process of data transfer, storage and processing, but also ensure the integrity of personal data of the information exchangers and prevent it from being disclosed to other users. In the process of transferring information from one point to another, both parties send and receive information assuming that it is authentic, the integrity of the information, and the correctness of the information in the packet. In order to control this process and ensure non-interference, various protection tools and software products have been created. Whether in the real world or in the virtual world, privacy statements can be descriptive or normative, depending on whether they are used to describe the ways in which people define and value the conditions and conditions of privacy, or whether they are used to indicate that there should be restrictions on the use of information. or information processing. These conditions or restrictions usually include personal data relating to individuals or data processing methods that may affect individuals. In a normative sense, information privacy is generally defined as the non-absolute right of individuals to (1) directly or indirectly control access to information about themselves, (2) to situations in which others may obtain information about themselves. (3) may refer to technologies that may be used to create, process or distribute information about oneself. In order to ensure the integrity of personal data, many tools have been created, and in

this article we will consider one such tool, the concept of digital signature, digital certificate and its classification process.

An electronic digital signature is a digital code attached to an electronically transmitted message that is used to verify the origin and content of the message. A signature created as a result of a special change of this electronic document information in an electronic document using the private key of an electronic digital signature, and with the help of the public key of an electronic digital signature, it is possible to determine the absence of errors in the information in the electronic document and to identify the owner of the private key of the electronic digital signature.

Digital certificates are data files used to identify users and electronic assets to protect online transactions. A digital certificate is an electronic or paper document issued by an authorized authority to the owner of the private key of an electronic digital signature, confirming that the public key of an electronic digital signature corresponds to the private key of an electronic digital signature; A digital certificate system is issued by a trusted third party known as a certificate authority (CA) to verify the user's identity. uses A digital certificate system, for example, allows a credit card user and merchant to confirm that digital certificates are issued by an authorized and trusted third party before exchanging data. Public Key Infrastructure (PKI), the use of public key cryptography that works with a certificate authority, is a key technology for providing secure authentication of identity online. Digital signatures and digital certificates help with authentication. Digital certificates help identify people or electronic assets. They protect online transactions by providing secure, encrypted, online communication.

In accordance with the Law of the Republic of Uzbekistan dated December 11, 2003 No. 562-II "On Electronic Digital Signature", the validity period of the digital signature key certificate shall not exceed 24 months from the date of registration of the electronic digital signature key. The electronic digital signature key certificate can be extended through the private office at https://e-imzo.uz until the expiration date of the electronic digital signature key certificate.

According to the Law of the Republic of Uzbekistan dated September 11, 2017 No. O'RQ-445 "On Appeals of Natural and Legal Entities", the electronic digital signature is designed to identify the person who signed the electronic document. it is a direct analogue of the signed signature and is used to confirm the authorship and immutability of the information reflected in the electronic document. Also, in accordance with the laws of the Republic of Uzbekistan "On

applications of natural and legal entities", applications that are not confirmed with an electronic digital signature are considered anonymous applications.

REFERENCES:

1. Law of the Republic of Uzbekistan dated December 11, 2003 No. 562-II "On Electronic Digital Signature"
2. Stanford Encyclopedia of Philosophy "Privacy and Information Technology" November 20, 2014.
3. “6 Emerging Trends in Physical Security” by Jay Palter March 8, 2021 in Emerging Trends in Physical Security.
4. “Security Technology Guide and Trends to 2022” 2023 Openpath