УДК 004.056.523 DOI: https://doi.org/10.30837/IYF.IRTTPI.2024.429

COMPARATIVE RESEARCH OF OPTIONS FOR OBTAINING ECPS

Bondarenko A.A.
Scientific supervisor – Ovcharenko D. R.
Kharkiv National University of Radio Electronics, Dep. CRETISS
anton.bondarenko1@nure.ua

This paper will consider the theoretical basis of digital signatures and certificates and analyze various ways of obtaining electronic digital signatures (EDS) in Ukraine. In addition, the currently available formats of electronic signatures and EDS providers will be considered.

The purpose of the work is to find the most optimal method of obtaining an electronic digital signature in terms of complexity, time, and security, as well as the most preferable provider of this service. Maintaining documentation in electronic form is becoming increasingly popular these days, which is not surprising for the so-called "era of digitalization", which has affected both business and society as a whole. The need to work remotely during the pandemic and now wartime has greatly accelerated the population's transition to the use of electronic document management. As a result, there is an urgent need to accelerate the introduction of electronic digital signatures to verify identity without the need for physical presence.

An electronic digital signature (EDS) is an analog of the handwritten signature and seal of a legal entity in electronic document flow. Technically, an EDS is obtained as a result of a cryptographic transformation of a set of digital data, which is added to this set or logically combined with it and allows to confirm the integrity of the document and identify the signer.

There are three types of digital signature in total:

- A Simple Electronic Signature (SES) is the most basic type of electronic signature used to verify the signer's identity and ensure the integrity of the document. SES is based on the authenticity of the signatory, which can be verified by comparing the signature with the signatory's basic identification data.

- An Advanced Electronic Signature (AES) is linked to the signer's identity and allows for verifying its authenticity. Although the intervention of a Certification Authority (CA) is not required to issue digital certificates, it is still necessary to have reliable means to ensure the signer's identity.

- A Qualified Electronic Signature (QES) is the highest level of electronic signature. The qualified electronic signature is suitable for transactions with the public administration. It is uniquely linked to the identity of the signatory with a qualified certificate issued by official electronic means and a certification authority and is used to verify its authenticity. The qualified electronic signature is based on a trusted public key infrastructure (PKI). This infrastructure includes the issuance and management of qualified certificates, which are generated and stored securely.

According to the Law of Ukraine dated November 7, 2018 "On Electronic Trust Services", the only format of electronic signature now used is the qualified electronic signature (QES). This type of digital signature has a higher degree of protection than the other two types of EDS.

A QES has all the basic properties of a handwritten signature:

- testifies that the received document came from the person who signed it;
- guarantees the integrity and protection against distortion and amendments to the signed document;
- does not allow the person who signed the document to refuse the obligations he/she undertook by signing the document.

It should be noted that at the moment in Ukraine, there are quite a large number of organizations providing services for obtaining EDS. Therefore, there is a need to conduct a qualitative analysis of the available options for the procedure of obtaining EDS.

In the work it is necessary to solve such tasks:

- to indicate the importance of data integrity in cyberspace as one of the basic principles of information security;
- determine the most convenient type of verification (BankID, Diia);
- review the theoretical basis of digital signatures and certificates, as well as their purpose and properties;
- analyze algorithms for obtaining digital signatures from different digital service providers;
- to note the differences between the formats of the proposed EDSs for data security;

According to the information from the electronic register of valid, blocked, and canceled public key certificates, there are 20 qualified EDS providers in Ukraine. These are public services, financial enterprises, and various joint stock companies. For our analysis, we decided to choose several organizations that provide EDS to individuals free of charge: PrivatBank, Oschadbank, Vchasno Servis LLC, and ACSC Ukraine (other options are also possible).

The paper will present comparative research of the offered qualified signatures according to such criteria as time and number of steps spent on obtaining QES, convenience of the service, its reliability, security availability, and other parameters. Based on the results of the comparison, the most optimal option for obtaining and using a qualified electronic signature will be determined, taking into account the needs of a modern user.

References: 1. Law of Ukraine “On Electronic Digital Signature” dated May 22, 2003 No. 852-IX. 2. Law of Ukraine “On electronic documents and electronic document management” dated May 22, 2003 No. 851IV. 3. Law of Ukraine “On Electronic Trust Services” dated May 10, 2017 No. 2155-VIII 4. Electronic register of valid, placed on hold or revoked public key certificates. URL – https://czo.gov.ua/en/ca-registry