EDS SECURITY RULES: PROTECTION AGAINST FRAUD

Muminova Sunbula Shaxzodovna
Tashkent University of information technologies named
after Muhammad al-Khwarizmi
E-mail: sunbulaaxmedova@gmail.com

ABSTRACT

This article analyzes current trends that determine the increase in the number of fraudulent actions involving the use of an electronic digital signature in the structure of crime in the Republic of Uzbekistan, as well as the features of the mechanism for committing such crimes. Moreover, the issues of protecting electronic digital signatures from such cases of fraud are considered.

Keywords: EDS, EDMS, fraud, physical crimes, technological crimes, social crimes.

A qualified electronic signature is your personal “tool” and protects your document from unauthorized actions. To form it, technology based on modern cryptographic algorithms is used. It is a guarantor of legal force and meets all requirements for the protection of confidential information. But even with such serious protection methods, you are not immune from unauthorized criminal actions due to your carelessness and insufficient security of electronic digital storage.

If in the wrong hands, electronic signature keys can become a weapon of fraud. Despite the high level of protection, attackers know how to compromise the signature.

Recently, cases of illegal actions with electronic signatures have become more frequent. If you discover that your electronic signature key has been lost or stolen, immediately contact the certification center. It will be necessary to immediately revoke the certificate in order to minimize the risks of fraudulent schemes, so that in the future criminals will not use the electronic signature.

Below are the types of fraudulent schemes using digital signatures:

Physical crimes - the fraudster requires contact with the carrier himself:

1. Theft of media – a criminal steals a USB key on which an electronic signature is recorded, and uses someone else’s digital signature in his schemes.

2. Transfer of digital signature to another person. Company managers transfer their electronic signature, for example, to the chief accountant or their subordinates, without understanding all the risks and consequences.

Technological crimes are carried out by fraudsters using skills in the field of IT technologies and information security:

The fraudster gains access to the computer or laptop of the owner of the digital signature. Thus, he can find out the password of the key carrier and gain access to the electronic signature.

Social crimes - these include criminal schemes based on the personal qualities of people. For example, impersonate this person - if he is similar in appearance, and engage in forgery of documents.

1. Receipt of digital signature by another person. A fraudster, having taken possession of the personal documents of the desired person and using a person who looks similar to him, can obtain an electronic signature instead of the real owner.

2. Obtaining electronic signature using forged documents and power of attorney. When you receive an electronic signature for the first time, you need to be present in person. Whereas when re-issuing an electronic signature, you need to provide copies of the necessary documents and a power of attorney. Fraudsters can take advantage of this situation.

How to protect yourself from a fraudulent digital signature attack:

– Do not give your electronic signature to strangers. Store it in a protected place;

– Set a reliable PIN code on the digital signature carrier, and do not share it with anyone;

– Switch to Cloud Electronic Signature or EDS. This digital signature is stored on a secure server in the CA cloud, without the use of a flash drive, and, therefore, cannot be stolen;

– Ensure the safety of your personal documents - do not transfer your passport, its copies, scans of the company's constituent documents to other people and dubious organizations;

– Contact the tax office and submit an application for a ban on registering a legal entity. persons without personal presence;

– Change the login/password you use periodically.

Several ways to protect your account in information systems from fraudulent schemes:

– Check your account, for example, on the State Services portal and monitor the "Recent Actions" section - you can see all the latest transactions there. But if suddenly the list shows suspicious actions that someone else is using your electronic signature, immediately change your login/password and activate the notification system in the service.

– Regularly check your profile in the “Taxpayer’s Personal Account” section on the website my.soliq.uz. If fraudsters have gained access and illegally registered an LLC or individual entrepreneur in your name using a qualified electronic signature, immediately write a statement to the police and the registration authority, indicating the company details. Then write an application to revoke the electronic signature. Also install additional security measures - set up email notifications.

– Do not issue an ES verification key certificate in your name at the request of third parties, friends or relatives. If in the future the keys of this signature are not stored with the owner and are used by third parties, there is no need to issue an electronic signature certificate, no matter what monetary reward is offered for it.

– Do not transfer electronic signature keys. Employees should not have access to the private signing key to avoid unauthorized actions that could lead to financial losses.

– Revoke a machine-readable power of attorney or electronic signature key certificate of an employee of a legal entity.

– When an employee resigns, the MChD issued in his name must be revoked. Otherwise, he may steal the organization’s money or even close it down.

– Do not provide scans and passport details. If this data falls into the hands of attackers, they can issue an electronic signature on it. Despite the fact that the likelihood of obtaining an electronic signature in this way is low, do not underestimate scammers.

– Protect your computer. The computer must be protected with a password and antivirus. When the user leaves the workplace, the computer must be locked and the token must not be left in it.

– Check the availability of issued certificates of electronic signature verification keys at State Services. There you will be able to find out in time whether a new electronic signature has been issued for you.

In conclusion, it is worth noting that when using an electronic signature, security rules must be observed - the electronic signature key must be kept secret and under no circumstances should it be transferred to another person. If this happens, it threatens you not only with financial risks, but also with serious consequences. Therefore, be careful and store your personal data carefully.

REFERENCES:

1. Social engineering explained: how criminals exploit human behavior. https://www.techcentral.ie/social-engineering-explained-how-criminals-exploit-human-behaviour/
2. Chernyx V.V. Problemy rassledovaniya moshennichestva, sovershennogo s ispol’zovaniem bankovskix kart, I puti ih resheniya. Bulletin of the Taganrog Institute of Management and Economics. 2018. №1 (27). P – 123-126/