UDC 342.9 (004.9)
DOI https://doi.org/10.32782/2524-0374/2019-6/63

COMPROMISE OF THE PERSONAL KEY OF THE ELECTRONIC SIGNATURE

КОМПРОМІС ОСОБИСТОГО КЛЮЧА ЕЛЕКТРОННОГО ПІДПИСУ

Kostnenko O.V., Postgraduate Student
Research Institute of Informatics and Law
of the National Academy of Legal Sciences of Ukraine

Legal relationships in the field of electronic trust services and digital signatures are regulated by the norms of international and national legislation, which provide a broad range of legal rights and obligations of legal entities in general. However, there are many areas of legal relations that are actually carried out by actors, but they are not regulated or insufficiently regulated by law. Thus, today the procedures for cross-border recognition of digital signatures certificates and electronic trust services are not regulated. It is social relations that arise during these procedures and processes that are subject to legal regulation, first of all, in the legislation of Ukraine.

Significant factor of nowadays is a rapid development of political, economic, scientific, business, trade, informational and public relations that affect directly not only international situation, but also corresponding processes in a particular countries, as well as exercise of rights, satisfaction of interests and needs of their citizens and state institutions. One of the main requirements for implementation of such relations is a rapid exchange of information, reflected in a digital form, ensuring its relevance, reliability, integrity, efficiency, identity, reliability and completeness.

The article is devoted to the study of the concept of compromising the personal key of digital signature, the legal aspects of compromise in the context of the theory of law. The paper presents the concept of explicit and implicit compromise and the limits of their actions, as well as the legal consequences of compromise. Taking into account analyzed approaches to definition of private key compromise, its types and specific features, it is possible to draw conclusion that, the lack of legal response of such socially dangerous act as "a personal key compromise" in the field of law affects stability of state information resources and their security.

Key words: compromise, personal key, signer, digital signature.

Правовідносини у сфері електронних довірчих послуг та електронного підпису регулюються нормами міжнародного та національного законодавства, які забезпечують широке коло юридичних прав і обов'язків юридичних осіб загалом. Однак існує багато сфер правовідносин, які фактично здійснюються суб'єктами, але вони не регулюються чи недостатньо регулюються законом. Отже, сьогодні не регулюються процедури транскордонного визнання сертифікатів цифрового підпису й електронних довірчих служб. Саме суспільні відносини, що виникають під час цих процедур та процесів, підлягають правовому регулюванню в законодавстві України.

Вагомим чинником сучасності є швидкий розвиток політичних, економічних, наукових, ділових, торговельних, інформаційних та суспільних відносин, які безпосередньо впливають не лише на міжнародну ситуацію, але й на відповідні процеси в певній країні, а також на здійснення прав, задоволення інтересів потреби своїх громадян та державних установ. Однією з головних вимог щодо реалізації таких відносин є швидкий обмін інформацією, відображеною в цифровій формі, що забезпечує її актуальність, надійність, цілісність, ефективність, ідентичність і повноту.

Стаття присвячена дослідженню концепції компрометації персонального ключа електронного підпису, правових аспектів компрометації в контексті теорії права. У роботі представлено поняття явної та неявної компрометації та межі їх дій, а також юридичні наслідки компрометації. Ураховуючи проаналізовані підходи до визначення компрометації особистого ключа, її види та специфічні особливості, можна зробити висновок, що відсутність правового реагування щодо такого суспільно небезпечного вчинку, як «компрометація особистого ключа» електронного підпису у сфері права, впливає на стабільність державних інформаційних ресурсів та їхньої безпеки.

Ключові слова: компроміс, особистий ключ, підписант, цифровий підпис.

Challenge problem. Significant factor of nowadays is a rapid development of political, economic, scientific, business, trade, informational and public relations that affect directly not only international situation, but also corresponding processes in a particular countries, as well as exercise of rights, satisfaction of interests and needs of their citizens and state institutions. One of the main requirements for implementation of such relations is a rapid exchange of information, reflected in a digital form, ensuring its relevance, reliability, integrity, efficiency, identity, reliability and completeness.

Powerful information computer technologies create new opportunities through the use of digital information (data), that, in turn, creates new social relations that arise between subjects of legal relations during: Electronic Data Interchange (Electronic Data Interchange); Electronic Funds Transfer (Electronic Funds Transfer); E-Commerce (e-Trade); use of electronic money (e-cash); electronic marketing (e-market); electronic banking (e-banking); electronic health system (e-health) and in other areas. Exchange of information is carried out in the process of electronic transactions in the form of electronic (digital) documents. Reliability of information during exchange is ensured through the use of trust electronic services, and requirements for reliability and integrity of information – due to application of digital cryptographic protection algorithms using technology of electronic signature. However, widespread use of this technology at the same time has brought to light legal problems, connected with the use of personal key of electronic signature. One of such problems is legal uncertainty of definition "compromise" of personal key of electronic signature.

As soon as possible, settlement of the problem of legal uncertainty of definition "compromise" and prompt response of the law to risks that arise or are caused by compromise of personal key of electronic signature is a burning problem

Purpose of the article is a research of legal issues, connected with definition "compromise" as an element of conceptual structure in the current legislation, as well as proposals for definition "personal key compromise".

Results of analysis of scientific publications. The issue of legal regulation of social relations, connected with the use of electronic signature was researched by the following domestic scientists: G. Koziel, A. Petrytsky, V. Pleskach, L. Ponomarenko, A. Shpirko, L. Yancheva, A. Lokshin and others. Among foreign scientists, this subject was researched by: S. Mason, A. Thiri, M. Wenbo, A. Petrov, O. Bezzubtsov. Over the last years the issue of creation of reliable mechanisms with a view to recognition of electronic signatures was researched by following scientists: O. Perevozchikova, S. Belov, I. Gorbenko, O. Potiy, B. Pogorelov, A. Melashchenko, however, the problem of compromise in the context of compromise ofpersonal key of electronic signature in Ukraine was highlighted at large in the technical aspect.

Thus, in the article by S. Belov "Models of construction of national infrastructure of key certification centers and their risks" it is highlighted exceptionally consequences of electronic signature compromise [1], and in publication by B. Pogorelov "Concerning definition of basic cryptographic concepts" it

is emphasized neutralization of threats of compromise for system management of electronic keys [2]. At the same time, at present there are not enough theoretical works and researches in the complex of issues that determine definition "personal key compromise of electronic signature".

Statement of conceptual issues. Before moving on to research of definition "personal key compromise", let us consider the story behind of genesis of definition "compromise" itself in the legal model of social and legal relations, that govern field of signature use.

Development of telecommunication technologies has promoted creation of machineries of documents exchange among users in electronic form that have legal significance. The need of use and exchange of such documents was so high, that many countries almost simultaneously adopted special laws, that governed basis of e-commerce and use of electronic signatures Thus, European Parliament and the Council on 13-th of December adopted EU Directive "On the system of electronic signatures, used within the Community", the Law "On Electronic Signatures in Global and National Commerce" was brought into force in the USA, Decree "On electronic Signature" was approved in France, federal law "On Digital Signatures" was adopted in Germany.

However, at that time, neither Ukraine nor the majority of countries had no practical experience in creation of electronic signatures systems both in organizational and legal aspects. Many national laws were developed as models of general rules of electronic signatures use. Practical application of abovementioned legislative acts have brought to light a number of unregulated by standards of law public relations, connected with electronic signature use, including the lack of clear definition "personal key compromise".

It should be noted that the need to create a new definition "personal key compromise" is due to following reasons.

Firstly, international legal norms in the field of electronic signature do not have clear, generally accepted definitions of the notion "compromise" Definition "compromise", in the context of "electronic signature compromise", has been applied in the UNCITRAL Model Law "On Electronic Signatures and Guidance On Decision-making" [3], adopted in Vienna on 5-th of July 2001 at the 34-thsession of UNCITRAL, Article 57 of which definition "Unreliable certificate" interprets as such, the personal key of which is "compromised" due to the loss of control by the signer.

In the United States, definition "compromise" is defined by the National Institute of Standards and Technology (NIST) as "unauthorized disclosure, modification, substitution or use of confidential data (including cryptographic key texts and other data of the Center of Safety Politic (CSP) [4] or unauthorized disclosure, modification, substitution or use of confidential data (such as keys, metadata and other information, connected with safety)" [5; 6].

Secondly, domestic legislation interprets "compromise" in more than one way Thus, paragraph 26 of the Article 1 of the Law of Ukraine "On electronic trust-based services" indicates that "special key compromise – is any event or act, that has led or will lead to unauthorized use of a personal key. Thus, the same definition contained the previous Law of Ukraine "On electronic digital signature". Unfortunately, such definition on the one hand, does not determine exactly what kind of object or subject of legal relations take abovementioned actions and exactly what kind of actions/events lead to unauthorized use of a private key, and, on the other hand, uncertainty of the definition creates grounds for free construction of specified provision of law.

At the same time, Ukrainian technical experts in the field of information security have introduced several alternatives of definition "compromise" as a technical term. Thus, Department of Special Telecommunication Systems and Information Security of the Security Service of Ukraine in 1999, creating ND TZI 1.1–003–99 "Terminology in the field of information protection in computer systems from unauthorized access", definition "compromise" is used as a violation of security policy; unauthorized acquaintance" [8]. Such definition "compromise" is aimed at resolving destructive events in the security system, connected with violation of clear rules of digital signatures use. However, such definition is not extended to relations, that take place with private key use outside borders, determined by security policy, and security policy-makers themselves may differ fundamentally. Also, such definition does not explain meaning "unauthorized acquaintance".

What is more, according to the order of State Service of Special Communication and Information Protection of Ukraine under date of 20.07.2007 № 141 "On Approval of Policy Statement of Procedure of Development, Production and Operation of means of Cryptographic Protection of Confidential Information and Open Information with the use of Electronic Digital Signature" it is determined more extended definition of compromise – as any event (loss, disclosure, theft, unauthorized copying, etc.) with key documents (key data) and means of cryptographic protection of information that have led (may lead) to the disclosure (leakage) of information about them, as well as information that is being processed and transmitted [9]. Undoubtedly, this is the most successful definition of "compromise", which should be accepted as a basis for the definition "personal key compromise" and enshrined at the level of legislative act that will promote administration of law.

Thirdly, in the Ukrainian legislation there is a situation where the lack of definition "private key compromise" in public relations, that regulate electronic keys use, has deprived the right of clarity and specificity, and has complicated process of its use, that has reduced credibility to electronic documents and deals, made with a help of electronic signatures, as shows judicial practice.

Over the last years the number of legal wrongs and crimes, connected with compromise and illegal use of personal keys of electronic signatures has increased. The overwhelming majority of crimes with personal key use of electronic signature, committed as a result of evident compromise of private key by a signer himself. Namely signers create conditions for private key compromise and its further illegal use. In the most cases, such crimes are committed in the banking sector, as well as in the field of notary and registration of legal entities. Example is a number of criminal cases, where defendants, being bank employees, ignored rules of banking security policy, for a variety of reasons captured personal keys of digital signatures of their colleagues or subordinates and organized schemes of misappropriation of funds, belonged to banks clients [10; 11]. There is a practice of private key compromise of a notary or a registrar during consummation of transactions. Thus, here are uncommon cases of compromise due to improper storage and occupation of a personal key of a notary or a registrar, that lead to illegal transfer of property by interfering into the work of the Unified State Register of Real Property Rights and the Unified State Register of Legal Entities and Individual Entrepreneurs [13].

Also, there are cases, when third persons capture personal keys of company managers and chief accountants, or obtain such keys in Accredited certification centers due to fraudulent letter of authorization with further commission of financial crimes [14].

Fourthly, specific problems of providing services in the field of electronic signatures, connected with private key compromise, consists rather in a complex structure and types of compromise.

Taking into account uncertainty of the definition, it is proposed to divide "personal key compromise" into evident and non-evident compromise. Let's consider types of compromise.

Evident private key compromise should be considered as a loss of access to personal key information, that is being confirmed guaranteed by facts of security policy violations and unauthorized access to key information.

In turn, evident compromise can be divided into:

– Compromise, which took place due to participation or will of a signer;

– Compromise, committed by third parties behind signer's back.

Thus, to the evident personal key compromise, that took place due to participation or will of a signer the following factors should be included with the following factors:

– loss (theft) of key carriers, loss of keys (codes) from safes at the moment of key carriers storage and loss of keys (codes) with their further finding;

– conscious or by breach of trust transfer of a personal key to a third party;

– violations of rules in effect of use and storage of private keys, disclosure of passwords, password of crypto protection, rules of storage and destruction (after term of validity) of a private key, as well as requirements for maintaining of password or PIN code to a personal key;

– storage of a private key in open, plain view, directly on user's HDD PEOM;

– private key compromise, committed by third parties behind signer's back and access of third parties to key information;

– violation of integrity of stamps on safes with key carriers in the case when it is applied procedure of safes sealing;

– access to key carriers by unauthorized copying;

– theft of a private key as a result of a response to a request, sent with elements of fraud or forgery;

– making of a personal key with forged documents [15; 16].

Unlike evident compromise of private key, non-evident compromise is based on assumptions or versions of events that have created or create conditions of private key compromise by third parties, who use hardware also. Non-evident compromise may include:

– rise of suspicions about leak of data as to key data;

– cases, when it is impossible to establish correctly what has happened with a key carriers (in the case, when key carriers got out of order and beyond reasonable doubt do not disprove possibility that such fact occurred as a result of uncontrolled actions by third parties);

– any other events, that give reason to believe, the key information has become known or available to third parties;

– interception by special technical means of sound information, electromagnetic or radio emission of computers, on which information is being processed with use of personal keys;

– information capturing by special technical means, specialized or spy software, that circulates in the Internet or on a local network, in which information is being processed with personal keys use [16; 17].

Fifthly, non-evident compromise with use of technical methods and devices of unauthorized access to personal keys of subscribers today is more limited in illegal possibilities due to rather complicated mechanism of cryptographic data protection. The world-wide scientific society periodically demonstrates possibilities of technical, impersonal access to keys of personal electronic signature. Thus, group of scientists from Japan, Switzerland, the Netherlands and the United States has successfully implemented technical access to data, codified with use of a cryptographic key [18]. Well-known cryptographer Adi Shamir (letter "S" in the abbreviation RSA) has developed method of technical access and reproduction of a private key through acoustic cryptanalysis without evident physical interference in telecommunication networks and systems [19].

Sixthly, problems, connected with complexity of assessment providing by legislators of legal consequences of a personal key compromise in the period between actual fact of compromise and fact of its official announcement, with next blocking or cancellation of a private key certificate. Namely during such period there is probability of compromised personal key use for committing actions, that have legal consequences.

Let us consider course of events in time, conditionally divided into five periods, from the beginning of private key compromise to elimination of consequences of its compromise.

The first period is a time when private key compromise has happened, but a signer has no suspicion and facts of evident or non-evident compromise. This period is the most difficult to register procedurally, and legal consequences, that create this period, have official standing and status of such, that have low probability of their recognition in future as invalid, due to insufficient evidence base, which is usually based on assumptions [20].

The second period is in evidence that under subjective analysis of certain facts or events at the subscriber's site is being formed suspicion about possibility of a personal key compromise. The next period characterizes by the need to make decision as to disclosure of private key compromise.

The third period can last from a few minutes to several days. This is due to the following factors: decision-making as to compromise by a user, if the electronic signature was used for work with resources that do not have legal risks and require little time.

Instead, decision-making as to private key compromise that is being used permanently work in registries or groups of keys that provide operation of information-computer networks, and institution network require analysis of situation and calculation of time for keys changeover and restoration of systems operation. In public authorities or local self-government authorities decision-making as to disclosure of personal key compromise may take several days.

Compromise disclosure is being made during the fourth period. Legislation provides procedure of compromise disclosure by appeal to Accredited Key Certification Center with application about compromise that is being transmitted by any technical means of communication [7].

The last period is provided by the Law of Ukraine "On Trustworthy Services" and it should not exceed 2 hours during which the EDS certificate is being blocked or canceled [7].

Analyzing stages of compromise from real fact of compromise and fact of official blocking or cancellation of a personal key certificate of electronic signature, we can assert that acts with a personal key, carried out in the first period, fall within the most risk have, since possibility of gathering of evidence base as to commitment of a socially dangerous act with use of a compromised private key has low probability.

Seventh, as of today in the legislation definition of personal key compromise of electronic signature in practice does not have clear definition and list of events or grounds that make it possible to consider them undoubtedly and, consequently, basic "beacons" for lawyers, who today assess precedents of violations of the law, connected with a personal key use of electronic digital signature exceptionally for the purposes of Articles 361–363 of the Criminal Code of Ukraine. Dispositions of these articles determine, that a personal key signer may be classified as an object or an instrument of a crime, as a technical means of unauthorized interference with operation of electronic computers (computers), automated systems, computer networks or telecommunication networks [21].

At the same time, actions or inactions of a signer that have led to a personal key compromise of electronic signature, as well as definition "personal key compromise", have not yet been found in the legal assessment. The lack of a list of basic concepts of personal key compromise of electronic signature creates ambiguity of interpretation of elements of crime by law enforcement agencies, courts and legal profession, committed with the use of electronic signature that, in turn, creates conditions for avoiding punishment.

Therefore, definition "compromise" in the current legislation in fact is a vague term for which may arise marginal situations, in which it may be unclear whether the term is permissible or not. For this reason, it is necessary to extend approved practice of use of definition "compromise" in order to make the term less vague and more informative, to take into account definition of evident and non-evident compromise that will promote more qualitative application of rules of law.

Undoubtedly, existing problems in the legal model of social and legal relations, that govern the field of electronic signature use, give rise all in all to distrust to legislation in the field of electronic signature, connected namely with uncertainty

of definition "compromise", create doubt about reliability of electronic signatures, integrity of electronic documents, signed by them, authenticity of transactions, made by notaries and state registrars in electronic form, invariability of information, listed in the Unified State Register of Real Property Rights to Real Estate and the Unified State Register of Legal Entities and Individual Entrepreneurs, reliability of agreements and treaties, concluded in electronic form also.

Taking into account the existing unregulated by rules law problem of public relations, connected with use of electronic signature, it is considered reasonably to force into application definition "personal key compromise of electronic signature" and to replace by the following: "Personal key compromise of electronic signature – as any evident or non-evident event and/or act (loss, disclosure, theft, unauthorized copying also) with data of personal key of electronic signature and means of cryptographic protection of information, that has led or may lead to unauthorized disclosure, change, destruction, blocking, interception, copying and use of personal key of electronic signature, as well as information, that is being processed and transmitted with its help".

Evident compromise of personal key of electronic signature is loss of access to personal key information with participation or inactivity of a signer or third parties without use of technical means.

Non-evident compromise of personal key of electronic signature is loss of access to personal key information of electronic signature with use of any technical means without participation of a signer.

This definition contains general norm of compromise and two detailed definitions of evident and non-evident compromise. Such approach will allow to fulfill socially dangerous unlawful acts with use of personal key of electronic signature.

It is important to emphasize, that a crime, like any other violation of a law, is a human act. But unlike other human acts, a crime by its very social nature is an attack on those relations that have come of in society, reflects its most important interests, and thus are being protected by a law Personal key compromise of electronic signature should be considered as conscious willful act of a person, consisted in concrete action or inaction Public danger of personal key compromise of electronic signature, as a material element of a crime, consists in that action or inaction inflicts harm to relations, protected by a law, or contains a real possibility of infliction of harm This is objective quality of a crime, real violation of relations, that exist in society in the field of electronic signature.

Significance of public danger of personal key compromise of electronic signature as a material element of a crime lies in the fact that it, firstly, is the main objective criteria for adjudication of illegal act; secondly, allows to classify crimes according to degree of criminal act; thirdly, determines boundary between a crime and other violations of a law; fourthly, is one of the general principles of individualization of liability and punishment [22].

In addition, definition "evident compromise" will promote opportunity for legal assessment of actions of a signer, an owner of a private key, as well as third parties, who have stolen it and use illegally. At the same time, use of notion "evident compromise" will allow to classify more thoroughly socially dangerous acts, that are being committed relative to a personal key of a signer or with its use in the light of provisions of the Criminal Code of Ukraine, that regulate social relations in the field of information activity, including electronic signature, and outline special type of crime, connected with illegal use of modern information technology and means of computer equipment. Personal key compromise of electronic signature should be referred to consequences of commission of crimes, provided by the Criminal Code of Ukraine – leakage, loss, forgery, blocking of information, creation of its processing or violation of established order of its routing [23].

Conclusions. Taking into account analyzed approaches to definition of private key compromise, its types and specific features, it is possible to draw conclusion that, the lack of legal response of such socially dangerous act as "a personal key compromise" in the field of law affects stability of state information resources and their security.

Thus, providing clarity of legislative language and the certainty of legal norms, new legislative definition "personal key compromise of electronic signature" will promote legal regulation of public relations, connected with use of electronic digital signature, clear classification of crimes and violations of a law, committed with use of electronic digital signature, and will also increase confidence to reliability of such signatures and electronic documents signed by them, electronic services, agreements and treaties, concluded in electronic form with use electronic signatures, will stimulate development of cross-border e-commerce and services.

REFERENCES

1. Belov S., Martynenko S. Models of national infrastructure construction of key certification centers and their risks. URL: http://www.itsway.kiev.ua/pdf/Model-CA_Risks.pdf.

2. Pogorelov B., Cheremushkin A., Chechet S. About definition of basic cryptographic concepts. *Report at the Conference "Mathematics and Security of Information Technologies"" (MABIT-03), Moscow State University, October 23–24, 2003.*

3. Model Law of UNCITRAL on Electronic Signatures. URL: http://zakon0.rada.gov.ua/laws/show/995_937.

4. FIPS PUB 140–2. Security Requirements for Cryptographic Modules. *Federal Information Processing Standards Publication 140–2.* U.S. Department of Commerce, 05/2001.

5. Recommendation for Key Management. *Special Publication 800-57.* Part 1. Rev. 3. NIST. 05/2014.

6. NIST SP 800-130. Framework for Designing Cryptographic Key Management Systems. URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/ NIST.SP.800-130.pdf.

7. On Trust-worthy Services : Law of Ukraine dated 05.10.2017 № 2155–VIII. URL: http://zakon2.rada.gov.ua/laws/show/2155-19.

8. Sun TSI 1.1–003–99. Terminology in the field of protection of information in computer systems from unauthorized access. *Approved by order number 22 DSTSZI SBU from 28.04.1999.* URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/doccatalog/list?currDir=41640.

9. On approval of the Regulation of procedure of development, production and operation of cryptographic protection of confidential information and open information with use of electronic digital signature: the order of the DSSIA of Ukraine dated 20.07.2007 № 141. (Registered by the Ministry of Justice of Ukraine, July 30, 2007, № 862/14129). URL: http://zakon2.rada.gov.ua/laws/show/z0862-07.

10. Resolution of Leninsky District Court of Kirovograd, October 19, 2011 in the case № 1–463/11. *Uniform State Register of Judgments :* website. URL: http://www.reyestr.court.gov.ua/Review/20422029.

11. Investigation 12016040730000533. *The only registry of pre-trial investigations :* website. URL: http://www.gp.gov.ua/ua/erdr.html.

12. Decree of Ivano-Frankivsk city court of Ivano-Frankivsk region, March 9, 2017 in case № 344/3171/17. *Unified state register of court decisions :* website. URL: http://www.reyestr.court.gov.ua/Review/65214508.

13. Verdict of Pechersk District Court of Kyiv, March 14, 2017 in the case № 757/10916/16-k. *Uniform State Register of Judgments :* website. URL: http://www.reyestr.court.gov.ua/Review/56854252.

14. Factorization of 768-bit RSA Modules, version 1.4 / T. Kleinjung et al. February 18, 2010. URL: https://eprint.iacr.org/2010/006.pdf.