Katarzyna Samulska
The Jacob of Paradies Academy in Gorzów Wielkopolski, Poland

The Safe Electronic Signature in Administrative Proceedings

Summary

This article explains some of the important issue of electronic signature. Discussed are the dynamic changes in the use of electronic signature, the introduction of its various types, as well as its significance and consequences under European Union legislation and as a consequence of Polish legislation, and its current legal status and context. Various types of electronic signatures are described, with a particular emphasis on qualified electronic signatures.

Keywords: electronic signature, secure electronic signature, modern technologies, digitalization, computerization

Introduction

The development of modern technologies has enforced their implementation on the administration. Computerization is understood as improvement in the quality of processes correlated with the use of technological progress and use of computers[1]. Implementing the principles and means of electronic communication as tools of its computerization to the public administration has resulted in the introduction of provisions on electronic documents as an equivalent written form[2].

To be valid, electronic documents must be labeled with a secure electronic signature.

Due to the dynamic changes in the use of the electronic signature, introduction of its various types, as well as significance and results as part of the European Union legislation and as a consequence, Polish legislation, the current legal status in this area should be further observed.

This article is intended to analyze issues related to terminology regarding a secure electronic signature and its use as part of administrative proceedings.

[1] P. Adamczewski, *Computer Dictonary*, Gliwice, 2005, p. 81.

[2] B. Adamiak, *Commentary to Art. 107 of the Administative Procedure Code*, [in:] B. Adamiak, J. Borkowski, *Commentary to the Administrative Procedure Code*, Legalis, 2017.

1. Types of electronic signatures

By virtue of the Act of 18 September 2001 on electronic signature[3], the concept of electronic signature was introduced into the legal system of Poland. The Act was in force from 18 August 2002 until 7 October 2016[4].

In Art. 3, point 1 of the Act, the definition of an electronic signature was formulated, defining it as data in electronic form, which together with other data to which they were enclosed or with which they are logically connected are used to identify the person submitting the electronic signature. The above concept of an electronic signature is often referred to as ordinary electronic signature.

By formulating the definition of an electronic signature, the Polish legislation implemented Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures[5].According to Art. 2, para. 1 of the above-mentioned directives, an electronic signature means data in electronic form added to other electronic data or logically related to them and used as an authentication method.

When analyzing the above definitions, one can point to a different purpose to be served by the electronic signature. The Polish legislation indicated that an electronic signature serves to identify a person that is putting their signature. According to the EU legislation, the electronic signature is an authentication method.

The Polish dictionary defines the term "authenticate" as:

1) making something credible,
2) verifying the authenticity of a document or copy, compliance with the right of some legal action,
3) providing someone with documents stating entrusting them with a diplomatic function[6].

In the light of the above, it may be concluded that the notion of authentication is a concept that is broader than identification.

The Polish legislation used the concept of a person submitting an electronic signature, stating in Art. 3 of the Act, that it is a natural person who has a device

[3] OJ of 2001, No. 130, item 1450.

[4] The Act of 18 September 2001 on electronic signature has lost its force pursuant to Art. 141 of the Act of 5 September 2016 electronic identification and trust services for electronic transactions. OJ of 2016, item 1579.

[5] Dziennik Urzędowy L 013, 19/01/2000 P. 0012-0020, http://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:31999L0093&from=PL.

[6] PWN Polish Dictionary, https://sjp.pwn.pl/sjp/uwierzytelnic;2533983.html, accessed on12 February 2018.

used to create an electronic signature, who acts on their own behalf or on behalf of a natural or legal person or an organizational unit without legal personality[7].

At this point, the concept of a device used to create an electronic signature should be cited, which according to Art. 5 of the Act on electronic signature, means equipment and software configured in a way that allows a copy or electronic certificate to be deposited using data used for the signature or electronic certification[8].

In addition to the electronic signature called "ordinary," the Polish legislation has provided for a secure electronic signature in the discussed Act on electronic signature. According to Art. 2,Sec. 2 of the above-mentioned Act, a secure electronic signature is such an electronic signature, that: a) is assigned exclusively to the person submitting the signature, b) is prepared by means of electronic signature equipment and electronic signature data for the exclusive control of the person submitting the electronic signature, c) is linked to data to which it has been attached in such a way that any subsequent change of this data is recognizable.

Art. 5, Sec. 1 of the Act on the electronic signature formulates a concept of a secure electronic signature verified using a qualified certificate. A qualified certificate is understood as a certificate that meets the needs set forth in the article, issued by a qualified subject providing certification services, which meets the requirements provided for in the act.[9]. Putting a secure electronic signature on data verified by means of a valid qualified certificate is equivalent in terms of legal effects to documents bearing handwritten signatures[10].

Article 6 of the discussed legal regulation additionally specifies that a secure electronic signature verified by means of a valid qualified certificate is evidence that it has been submitted by a person specified in this certificate as submitting an electronic signature. This will not apply if the period of validity of the certificate expires or since the date of its cancellation and during the suspension period, unless it is proven that the signature was submitted before the expiry of the certificate or before its annulment or suspension.

The necessary condition for recognizing the correctness of a complex secure signature is to use secure devices and data subject to exclusive control of the person who submits the electronic signature.

---

[7] The EU legislatotion in Art. 4 of Directive 1999/93/EC clarified that the person putting an electronic signature is a person possessing a device used to put a signature and acting on their own behalf or on behalf of natural or legal persons or another entity which they represent. Therefore, the EU did not limit this concept only to natural persons, thus limiting the group of electronic signatures to natural persons, as the Polish legislation did.

[8] Article 6 of Directive 199/93/EC provides that a device used to create an electronic signature means configured software or hardware used to implement data support for the electronic signature.

[9] Article 3 sec.12 of the Act on electronic signature.

[10] Article 5, Sec. 2 of the Act on electronic signature.

It is worth emphasizing that the already mentioned Directive No. 199/93/EC also introduced the concept of an advanced electronic signature. An advanced electronic signature means an electronic signature that meets the following requirements: a) it is assigned only to the signatory; b) it enables identification of the signatory; (c) it is created by means which the signatory may have under exclusive control; (d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.

In force from 1 July 2016 is Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, called eIDAS and repealing Directive 1999/93/EC11. This new regulation introduced common legal and technical standards on the single digital market of the European Union. It applies directly in all EU Member States.

The Polish legislature, with a view to applying the above mentioned eIDAS regulation, has passed the Act of 5 September 2016 on trust services and electronic identification[12]. By virtue of this act, the law on electronic signature has been repealed. This act redefined the existing secure electronic signature verified by means of a valid qualified certificate as a qualified electronic signature[13] understood as an "advanced electronic signature, which is submitted by means of a qualified device for submitting an electronic signature and which is based on a qualified electronic signature certificate"[14].

---

[11] EU Journal of Laws 257, of 28.08.2014.

[12] OJ of 2016, item 1579.

[13] Art. 3, Sec. 12 of the eIDAS regulation.

[14] Art. 3, Sec. 15 of the eIDAS Regulation states that a qualified electronic signature certificate "means an electronic signature certificate that is issued by a qualified trust service provider and meets the requirements set out in Annex I; Eligible certificates for electronic signatures contain the following information:

a) indicating – at least in the form allowing for automatic processing – that the given certificate was issued as a qualified electronic signature certificate;

b) a set of data unambiguously representing a qualified trust service provider that issues qualified certificates, including at least the Member State where the supplier is established, and – in reference to a legal person: the name and, if applicable, the registration number in accordance with the official register, in reference to a natural person: name and surname of that person;

c) at least the name of the signatory or his or her pseudonym; if a pseudonym is used, this fact is clearly indicated;

d) data used to validate the electronic signature, which correspond to the data used for the electronic signature;

e) data regarding the beginning and end of the certificate's validity period;

f) the certificate's identification code, which must be unique for the qualified trust service provider;

g) an advanced electronic signature or an advanced electronic seal of the issuer of the qualified trust service provider;

h) place where a certificate attached to an advanced electronic signature or an advanced electronic seal referred to in point (g) is available free of charge;

According to Art. 131 of the Act on trust services and electronic identification, a secure electronic signature verified by means of a valid qualified certificate within the meaning of the Act of 18 September 2001 on electronic signature is a qualified electronic signature. Qualified electronic signature in accordance with Art. 25, Sec. 2 and 3 of the eIDAS regulation have a legal effect equivalent of a handwritten signature and if issued in one Member State, it is also recognized in the other Member States. In connection with the above, public administration authorities in Poland, from July 2016 on, are obliged to recognize qualified electronic signatures issued by other member countries.

It should be emphasized that certificates issued before the entry into force of the eIDAS regulation remain valid. Every electronic signature created after 1 July 2016 with the use of the same devices and software that were used to create secure electronic signatures in accordance with the Polish act of 18 September 2001 on electronic signature and verified – using a qualified electronic signature certificate issued after 1 July 2016 under new provisions (eIDAS) – or by means of a qualified certificate issued before 1 July 2016 under the then applicable Polish law on electronic signature has the status of a qualified electronic signature under the new regulations (eIDAS) and has a legal effect equivalent of a handwritten signature, i.e., the same legal effect of a secure electronic signature verified by means of a qualified certificate within the meaning of the Polish Act on electronic signature.

However, due to low public interest the use of secure electronic signatures (currently qualified), the Polish legislatitive has also introduced other institutions allowing the authentication of users of the ICT system.

According to Art. 20a, para. 1 of the Act of February 17, 2005 on computerization of the activities of entities performing public tasks[15], authentication of users of the ICT system using online services provided by entities specified in Art. 2 – among others, government administration bodies, state control and law enforcement bodies, courts, prosecution organizational units, as well as local government entities and their bodies, requires: data verified by means of a qualified electronic signature certificate or an ePUAP trusted profile. From September 29, 2018 on, an alternative will also be the use of the notified electronic identification means, adequately to the level of security required for services provided under these systems. A public entity that uses public teleinformation systems to perform

i) a place of services that may be used to submit a request for the validity status of a qualified certificate;
j) in the case where data used to create an electronic signature associated with the data used to validate the electronic signature are located in a device qualified for submitting an electronic signature, an appropriate indication of this fact at least in a form allowing automatic processing.

[15] I.e., OJ of 2017, item 570.

public tasks may allow users identification in this system through the use of other technologies, unless separate provisions provide for the obligation to perform activities at the premises of a public entity[16].

It should be clarified that ePUAP is an electronic platform for public administration services[17]. According to Art. 3, Sec. 15 of the Act of February 17, 2005 on computerization of entities performing public tasks[18], a signature confirmed by the ePUAP trusted profile is: an electronic signature submitted by the user of the ePUAP account, to which the identification information contained in the ePUAP trusted profile has been attached, as well as: a) an unambiguously indicating trusted ePUAP profile of the person who submitted the signature, b) containing the time at which the signature was submitted, c) niquely identifying the ePUAP account of the person who submitted the signature, d) ePUAP account authorized by the user, e) stamped and protected with an electronic seal used in ePUAP to ensure integrity and authenticity of operations performed by the ePUAP system.

The legal effects of the signature confirmed by the ePUAP trusted profile are regulated by Art. 20b Computerization: A signature confirmed by the ePUAP trusted profile has legal effects if it was created or submitted during the period of validity of this profile (par. 1). Data in electronic form bearing a signature confirmed by the ePUAP trusted profile are equivalent in terms of legal consequences to a document bearing a handwritten signature, unless the separate provisions provide otherwise (par. 2). The validity and effectiveness of a signature confirmed by the ePUAP trusted profile cannot be denied only on the grounds that it exists in electronic form or that other data than those used to confirm the trusted profile have been changed (par. 3). The signature confirmed by the ePUAP trusted profile is to constitute an alternative to a qualified electronic signature due to the fact that it is free of charge as opposed to the latter type of signature.

2. Safe electronic signature in administrative proceedings

Administrative proceedings regulated in the Act of 14 June 1960 of the Administrative Procedure Code[19] provides for the possibility of submission and delivery of elec-

[16] Art. 20 a, para. 2 of the Act on computerization of activities of entities performing public tasks.

[17] Regulation of the Minister of Digitization of 5 October 2016 on the trusted profile of an electronic platform for public administration services (OJ of 2016, item 1633) specifies the terms and conditions for confirming, extending validity, use and revocation of the trusted electronic platform for public administration services.

[18] I.e., OJ of 2017, item 570.

[19] I.e., OJ of 2017 item 1257, as amended.

tronic documents in administration and through administration, and provides for the possibility of communication by electronic means. An electronic document within the meaning of the act on computerization of entities performing public tasks is a separate set of data, arranged in a specific internal structure and stored on an IT data carrier[20].

When analyzing the provisions of the Administrative Procedure Code, it should be pointed out that cases in administrative proceedings can be dealt with in addition to the classical form – written – also in the form of an electronic document[21], delivered by electronic means of communication[22]. The means of electronic communication may be used only if the party demands it or explicitly agrees in response to the offer made by the authority[23]. Therefore, the party to the administrative proceedings obtained the right to submit the application, request, explanation, appeal, complaint, by e-mail. The date of initiation of proceedings at the request of the party brought electronically is the day the request is entered into the ICT system of the public administration authority[24]. According to Art. 63, para. 3a, the Administrative Procedure Code states that the application submitted in the form of an electronic document should:

1) bear a qualified electronic signature or signature confirmed by an ePUAP trusted profile, or authenticated in a way that ensures the ability to confirm the origin and integrity of the verified data in electronic form;
2) contain data in a fixed format, included in the application template specified in separate regulations, if these provisions require applications to be submitted in accordance with a specific pattern;
3) include the electronic address of the applicant.

The Voivodeship Administrative Court in Warsaw, in its decision of 25 June 2015, considered that the e-mail did not meet the requirements of a procedural document in administrative proceedings, if it was not signed in the form accepted by the provisions of the Administrative Procedure Code. The application submitted in the form of an electronic document should be authenticated using mechanisms specified in Art. 20a, para. 1 or 2 of the Act of February 17, 2005 on computerization of activities of entities performing public tasks[25].

---

[20] Article 3, Sec. 2 of the Act on computerization of activities of entities performing public tasks (i.e., OJ of 2017, item 570).

[21] According to Art. 3, Sec. 2 of the Act of February 17, 2005 on computerization of activities of entities performing public tasks (i.e., OJ of 2017, item 570) an electronic document constituting a separate semantic whole, a set of data arranged in a specific internal structure and stored on an IT data carrier.

[22] Article 14, para. 1 of the Act of 14 June 1960 of the Administrative Procedure Code.

[23] B. Adamiak, *Commentary to Art. 39 (1) of the Administrative Procedure Code*, [in:] B. Adamiak, J. Borkowski, *Administratice Procedure Code. Commentary,* 2017, Lex.

[24] Art. 61, para. 3 a of the Administrative Procedure Code.

[25] Decision of the Voivodeship Administrative Court in Warsaw of 25/06/2015, II SAB/Wa 326/15, Legalis.

In the administrative procedure, the form of an electronic document with a qualified electronic signature or a signature confirmed by a trusted profile may also take the form of a power of attorney[26]. If a copy of the power of attorney or copies of other documents showing authorization have been drawn up in the form of an electronic document, they are authenticated by supplementing the document with copies bearing a qualified electronic signature or a signature confirmed by the ePUAP trusted profile.

At this point, it is worth noting the judgment of the Voivodeship Administrative Court in Szczecin of 1 February 2012[27] in which the court ruled that if the power of attorney sent by email (the proxy sent a scan of the power of attorney) in performing the obligation to remove the lack of a formal appeal by attaching the power of attorney, was considered inappropriate by the authority – the party shall be notified of this fact and called to sign the appeal or call the attorney to submission of a proper power of attorney. Failure to do so by the appeal body constitutes an infringement expressed in Art. 9 of the Administrative Procedure Code of the principles of duly and fully informing the parties on the factual and legal circumstances that may affect determination of their rights and obligations being the subject of investigation.

In the course of administrative proceedings, a public administration body also has the right and obligation to use legal institutions requiring a secure electronic signature. This signature can be used both in activities and documents directed outside the public administration body – to the party to proceedings or other participants of the proceedings, but also as part of the documentation of the body's activities. As part of the activities of the public administration body addressed to the officially non-subordinate entities, authorities may call for participation in the activities undertaken and to provide explanations, among others in the form of an electronic document. Such a request should be accompanied by a qualified electronic signature of the employee of the requesting authority[28].

The authority also has the right to certify compliance with the original document made in the form of an electronic document. It does so by using a qualified electronic signature or signature confirmed by an ePUAP trusted profile[29].

Copies of files of the case given to the body of higher instance in the event of a reminder being lodged by the party may be made in the form of an electronic

[26] Art. 33, Sec. 2 and 2a of the Administrative Procedure Code.

[27] Judgment of the Voivodeship Administrative Court in Szczecin of 1.02.2012, reference No. SA/Sz 1223/11, Legalis.

[28] Art. 54 of the Administrative Procedure Code.

[29] Art. 76 a, para. 2 a of the Administrative Procedure Code.

document[30]. The body conducting the proceedings is obliged to forward the body of higher instance without undue delay, no later than within seven days of its receipt.

In the course of the proceedings, in order to consolidate the activities carried out, the public administration body may make annotations in the form of an electronic document[31].

It is important to give the form of an electronic document to individual administrative acts issued in the course of administrative proceedings – that is, the provisions and at the end of the case – administrative decisions. Both the administrative decision and the order issued in the form of an electronic document shall still contain the same elements as the decision or the written order, and to ensure authenticity of this act they must be accompanied by a qualified electronic signature[32]. The direction of changes is clear and unambiguous – as a result, there was a constant to strengthen requirements regarding the form of a written administrative decision, which fully applies to electronic documents, the use of which also falls within the general rule formulated in Art. 14,para. 1. The decision, as well as the provisions, shall be delivered to the parties in writing or by electronic means of communication. The legislation has adopted two equivalent ways of communicating the will of the body externalized in the administrative decision (omitting verbal announcement of the decision).These methods are delivery in paper form and delivery of an electronic document, which is a decision, with the help of electronic means of communication. Each of these methods leads to an effective delivery of a decision, that is, after which the party has the opportunity to become acquainted with the content of the administrative decision[33]. However, it follows from the jurisprudence of administrative courts that even if a party makes a request for delivery of a decision in the form of an electronic document, this does not justify accepting that only in this form will the delivery of the decision be allowed. In a situation where the authority does not have technical capabilities to address the party's task in this regard, the delivery of the decision by post will be a legally justified way of delivering the decision of the authority[34].

The legislation also provided for the form of an electronic document to prepare a settlement concluded in the course of the administrative proceedings. The settlement prepared in this form requires a qualified electronic signature

[30] Art. 37, Sec. 4 of the Administrative Procedure Code.
[31] Art. 72 of the Administrative Procedure Code.
[32] Art. 107, para. 1, sec. 8 of the Administrative Procedure Code and Art. 124, para. 1 of the Administrative Procedure Code.
[33] Judgment of the Voivodeship Administrative Court in Wrocław of 18/09/2013, reference No. Act II Sa/Wr 420/13, Legalis.
[34] Judgment of the Supreme Administrative Court of Poland of 06.06.2014, reference No. II SK 2297/13, Legalis.

of the parties and an authorized employee of the public administration body[35]. For a guarantee that settlement elements will not be included in the settlement without the will of the parties, it is required to read the drafted content of the settlement, unless the settlement has been prepared in the form of an electronic document. In this case, the parties should familiarize themselves with the content of the settlement made to protect their legal interests[36].

Computerization of administration introduced the possibility of issuing certificates in the form of an electronic document. The certificate, as an official confirmation of facts or legal status, takes the form of an official document drawn up in a specific form by an authorized entity[37]. The certificate shall be issued in the form of an electronic document with a qualified electronic signature, if requested by the person applying for the certificate[38].

The certificate may be issued in the form of an electronic document only at the request of the person who applies for it. From the provision of Art. 217, para. 4 of the Administrative Procedure Code, it follows that the basic form remains a written document, and the choice of electronic form belongs only to the person who requests the issuing of a certificate and at the same time determines his/her desired specific written form. The certificate in the form of an electronic document must be accompanied by a qualified electronic signature ensuring the credibility of the document and individualizing the signatory. Certificate on tacit settlement of the matter referred to in Art. 122f of the Administrative Procedure Code can also be issued in the form of an electronic document, as provisions of Art. 217, para. 4 of the Administrative Procedure Code apply[39]. The literature also allows the possibility of obtaining an electronic certificate stored on an IT data carrier[40]. The certificate issued in the form of an electronic document may be used – as an official document – only in electronic trading. The printout of the electronic certificate will only constitute a copy of this document[41].

In a judgment of 7 September 2015, the National Appeal Chamber accepted that a certificate issued in electronic form bearing a secure electronic signature by a person indicated by name and surname in the certificate, verifiable using a signature

[35] Art. 117 of the Administrative Procedure Code.

[36] B. Adamiak, *Commentary to Art. 117 of the Administrative Procedure Code*, op. cit.

[37] K. Celińska-Grzegorczyk, "Commentary to Art. 217 of the Administrative Procedure Code," in*Administrative Procedure Code,* edited by R. Hauser, M. Wierzbowski, Warszawa, 2017, Legalis.

[38] Art. 217, para. 4 of the Administrative Procedure Code.

[39] S. Gajewski, *Kodeks postępowania administracyjnego. Nowe instytucje.* Commentary to chapters 5a, 8a, 14 and sections IV and VIII a of the Administrative Procedure Code, 2017, Legalis.

[40] R. Kędziora, Commentary to Art. 217 of the Administrative Procedure Code, [in:] Administrative Procedure Code. Commentary. 2017, Legalis.

[41] Ibidem.

verification software, is issued in accordance with the procedure provided for in the act(Art. 217,para. 4 of the Administrative Procedure Code), in the form equivalent to the written form (in accordance with Art. 14 of the Administrative Procedure Code). Thus, it is an official document, drawn up in the prescribed form by the state authorities appointed for this purpose in their scope of operation and constitutes evidence of what has been officially identified in it (Art. 76, para. 1 of the Administrative Procedure Code). In the opinion of the Chamber, it has no impact on the assessment of a document issued in electronic form equated with the written form and its later printing, which actually constitutes the materialization of an electronic document for submission in a public procurement procedure. Until the printing of such a document, it remains only in electronic circulation, and its printing does not affect the change in form in which it was drafted, and thus its effectiveness[42].

Conclusion

Changes in regulations regarding the secure electronic signature in administrative proceedings are aimed to build trust to the online environment among citizens. Computerization of administrative proceedings has become a fact.

Building trust to electronic services is also aimed to increase implementation of new services provided by the administration in this form. Making the administration more effective, more efficient, more flexible, and faster. Modern methods of managing administration and satisfying the needs of citizens are to bring a metamorphosis of its organizational structure, increase the quality of services provided, and guarantee reliable operation of bodies in which highly qualified staff is employed[43]. The adopted legislative solutions are aimed at increasing trust in electronic transactions not only within services provided in Poland but also within services provided in other European Union countries by ensuring a common basis for safe electronic interactions between citizens, enterprises, and public authorities.

Bibliography

1. Adamczewski, P., *Computer Dictonary*, Gliwice, 2005.
2. Adamiak B., *Commentary to Art. 107 of the Administrative Procedure Code*, [in:] B. Adamiak, J. Borkowski, *Commentary to the Administrative Procedure Code*. Legalis, 2017.

[42] Judgment of the National Appeal Chamber of 7.09.2015, National Appeal Chamber 1860/15, No. 131620, Legalis.

[43] See also A. Haręża, *Introduction to the electronic problems of public administration*, „Kwartalnik Naukowy Prawo Mediów Elektronicznych" 2011, No. 1, pp. 26-33.

3. Cegielska-Grzegorczyk, *Commentary to Art. 217 of the Administrative Procedure Code*, in *Administrative Procedure Code*, ed. R. Hauser, M. Wierzbowski, Warszawa 2017, Legalis.
4. Gajewski S., *Administrative Procedure Code. New Institution. Commentary to chapters 5a, 8a, 14 and sections IV and VII a of the AdministrativeProcedure Code,* Warszawa, 2017, Legalis.
5. Horęża A., *Introduction to the electronic problems of public administration*, „Kwartalnik Naukowy Prawo Mediów Elektronicznych" 2011, No. 1.
6. Kędziora R., *Commentary to Art. 217 of the Administrative Procedure Code*, [in:] *Administrative Procedure Code, Commentary*, Legalis, 2017.