

Regulation of the mSzafir seal service of Krajowa Izba Rozliczeniowa S.A.

The Regulation set out the rules for the use of the mSzafir seal service provided by Krajowa Izba Rozliczeniowa S.A. in Warsaw, ul. rtm. W. Pileckiego 65 02-781 Warsaw, entered in the Register of Entrepreneurs kept by the District Court for the Capital City of Warsaw, XIII Commercial Division of the National Court Register, under the KRS number 0000113064, fully paid-up share capital of PLN 5,445,000, NIP number: 526-030-05-17, hereinafter referred to as "KIR".

§ 1.

Definitions

1. Terms used in the Regulation mSzafir seal service, hereinafter referred to as Regulation have the following meanings:
 - 1) Mobile application - an IT tool used for Authorization;
 - 2) Authorization - the electronic process that enables the identification of the Customer for the purpose of gaining access to the Private Key;
 - 3) eIDAS - Regulation (EU) No. 910/2014 of the European Parliament and of the Council of July 23, 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
 - 4) Customer - an entity that has placed an Order, in particular a Subscriber;;
 - 5) Consumer - a Customer who is a consumer within the meaning of Article 221 of the Civil Code;
 - 6) Private Key - the data used to create an electronic seal;
 - 7) Authorized Person - a person authorized by the Customer to receive the certificate and activate the first Mobile Application;
 - 8) mSzafir Portal - an IT system of KIR that provides functionality of affixing an electronic seal to documents
 - 9) Regulation - this Regulation;
 - 10) RODO - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation);
 - 11) Subscriber - an entity whose data has been entered into the certificate;
 - 12) mSzafir Seal Service - a trust service involving the issuance of a qualified certificate and the generation, storage and management of a Private Key, including the handling of Authorization, for the purpose of submitting a qualified electronic seal;
 - 13) User - an entity to which the Subscriber has directly or indirectly made available a mechanism to perform Authorization for the purpose of submitting an electronic seal on behalf of the Subscriber, in particular by activating an instance of the Mobile Application;
 - 14) Order - an order to a trust services agreement covering the use of the mSzafir seal Service.

2. Terms appearing in the Regulations that are not defined in this paragraph shall be understood in accordance with the definitions contained in the KIR Certification Policy for Qualified Trust Services.
3. The Regulations set out the rules for the provision of the mSzafor Seal Service only and shall not affect the provision of other services under contracts for the provision of trust services.
4. The Regulations do not determine the rules for the conclusion of contracts. Contracts are concluded regardless of the acceptance of the Regulations.

§ 2.

General rules

1. The mSzafor seal service is a trust service regulated by the Law of September 5, 2016 on Trust and Electronic Identification Services, hereinafter referred to as the "Law", and its accompanying implementing acts and eIDAS.
2. The Customer and the Subscriber shall be obliged to comply with the provisions of the Regulations.
3. KIR shall use the Polish language in its relations with the Customer and the Subscriber.
4. The Regulations do not specify the principles of incurring the costs of data transmission over the Internet, related to the use of the mSzafor seal Service.
5. The person authorized to use the mSzafor seal service, including, in particular, the creation of an electronic seal, is only the Subscriber acting by the User.
6. The granting and revoking of User privileges shall be performed by the Subscriber or another User only using the mechanism provided in the Mobile Application.
7. The Customer shall be obliged not to provide to mSzafor Portal content prohibited by law, e.g. content that promotes violence, defamatory content or content that violates the personal rights and other rights of third parties.
8. The Code of Good Practices referred to in Article 12 paragraph 1 item 15 of the Law of May 30, 2014 on Consumer Rights shall not apply to the provision of the Service seal mSzafor.
9. The mSzafor seal service is a service provided electronically within the meaning of the Act of 18 July 2002 on the provision of electronic services.
10. Due to its nature, the use of the mSzafor seal Service shall not be anonymous, except that KIR may not verify the identity or identify the User's data.
11. KIR shall endeavor to ensure the greatest possible availability of the mSzafor seal Service and to promptly rectify failures, as well as to make technical interruptions as inconvenient as possible for the Subscribers.

§ 3.

The orders

1. In order to execute the Order, it is required to provide the Subscriber's data for the production of the certificate and to indicate the Authorized Person.
2. The rules of use and licensing of the Mobile Application are specified in the license document in the Mobile Application, which the Subscriber should become familiar with before installing it.

§ 4.

Presenting data for the certificate

1. In order to execute the Order, the Customer is obliged to present in a reliable manner verified data for the certificate and the authorized person.
2. A qualified certificate contains the data specified in the KIR Certification Policy for qualified trust services.
3. Confirmation of data for the certificate shall require sending a confirmation of the Order submitted by persons authorized to represent the Subscriber and verification of its correctness by the KIR.
4. If the presented data referred to in Clause 3 is incomplete or incorrect, or the Subscriber fails to send a confirmation of the Order referred to in Clause 3 or fails to confirm the accuracy of such data, KIR shall contact the Customer for clarification.
5. If it is not possible to contact the Customer or to clarify the irregularities, or the Customer fails to provide data or the Subscriber fails to submit a confirmation of the Order within 30 days from the date of placing the Order, then KIR shall refuse to execute the Order and shall not produce a qualified certificate, and shall refund the payment using the same payment method used by the Customer.
6. KIR accepts only the following methods of confirming the identity of the Authorized Person :
 - 1) use of a qualified certificate of electronic signature;
 - 2) personal appearance.
7. Confirmation of identity in the mode referred to in paragraph 6.1 shall consist in signing the certification request with a qualified electronic signature.
8. Confirmation of identity in the mode referred to in paragraph 6(2) shall consist in personal verification of the identity of the Authorized Person at an KIR facility.
9. Confirmation of identity shall be made within 30 days from the date of placing the Order. If the identity of the Authorized Person is not confirmed within the deadline then KIR will refuse to execute the Order and will not produce a qualified certificate, and will refund the payment using the same payment method used by the Customer.

§ 5.

Cancellation, termination or dissolution of the Agreement (The Order) by the Consumer

1. Pursuant to Article 27 of the Act of May 30, 2014 on Consumer Rights (Journal of Laws of 2020, item 287, as amended), a Consumer who has concluded a contract (the Order) at a distance or off-premises may withdraw from it within 14 days without stating a reason and without incurring costs. This right may be exercised by any Consumer.
2. Pursuant to the law referred to in paragraph 1, a Consumer may not withdraw from an agreement (the Order) in the case of, among other things:
 - 1) the provision of services, if KIR has performed the service in full with the express consent of the Consumer, who was informed before the performance began that after the performance by KIR he or she will lose the right to withdraw from the agreement (the Order);
 - 2) in which the subject of performance is a non-refabricated item, produced to the consumer's specifications or serving to satisfy his or her individualized needs;
 - 3) the provision of digital content that is not recorded on a tangible medium, if the performance has begun with the express consent of the Consumer before the expiry of the deadline for withdrawal from the contract (the Order) and after KIR has informed him of the loss of the right to withdraw from the contract (the Order).
3. The mSzafor seal service will be fully performed as soon as the qualified certificate is created in the KIR system, and the qualified certificate is completely individualized for the Consumer. As of that moment - pursuant to Article 38 (1), (3) or (13) of the Law of May 30, 2014 on Consumer Rights - the Consumer will lose the possibility to withdraw from the Order. KIR - at the latest before confirming the data for the certificate - will warn the Customer that the Customer agrees to start performing the mSzafor seal Service before the deadline, and thus will lose the possibility to withdraw from the Order after its execution.
4. The Order shall be terminated and the Customer shall be entitled to a refund of remuneration in the case:
 - 1) referred to in § 4 section 5;
 - 2) failure to complete the process of confirming the identity of the Person authorized by the date referred to in § 4 paragraph 9.
5. The course of the period for withdrawal from the Order shall begin from the moment of its delivery, except that from the moment referred to in paragraph 3, the Consumer shall not have the right to withdraw.
6. In order to exercise the right of withdrawal, the Consumer should submit a statement of withdrawal. The Consumer may use the model withdrawal form. Use of the template is not mandatory.
7. The statement of withdrawal should be sent to the Department of Customer Contact and Operations of KIR in writing to the address: Suraska 3A Street, 15 - 950 Bialystok or by e-mail to: kontakt@kir.pl.
8. In the case of cancellation of an Order placed remotely, the Order shall be deemed not to have been placed.

9. KIR shall immediately, no later than within 14 days from the date of receipt of the Consumer's declaration of withdrawal from the Order, return to the Customer all payments made by the Customer.
10. KIR shall refund the payment using the same method of payment used by the Customer.

§ 6.

Complaint procedure

1. Complaints should be submitted to the address of the Customer Contact and Operations Department, Krajowa Izba Rozliczeniowa S.A., 3A Suraska St., 15-950 Białystok, or to e-mail: kontakt@kir.pl.
2. When submitting a complaint, you should provide all information or elements necessary to start the process of processing the complaint.
3. KIR shall consider the complaint within 30 days from the date of submission of the complaint.
4. KIR does not provide for other out-of-court ways of processing complaints.
5. KIR does not provide for other out-of-court means of claim investigation or rules of access to these procedures.
6. The Customer shall be entitled to technical assistance for problems related to the use of the mSzafr seal Service.
7. KIR shall make every effort to ensure that the problem reported under technical assistance is resolved as soon as possible.
8. Technical assistance shall be provided on the days and hours of operation of the Helpline and at the Helpline number indicated on the website www.elektronicznypodpis.pl.

§ 7.

Privacy policy and data protection

1. Pursuant to Article 13(1) and (2) and Article 14(1) and (2) of the RODO, KIR informs that:
 - 1) the administrator of personal data is Krajowa Izba Rozliczeniowa S.A. with its registered office in Warsaw, 65 rtm. Witolda Pileckiego Street, 02-781 Warsaw, KRS 0000113064;
 - 2) the contact details of the Data Protection Officer at KIR are: IOD@kir.pl;
 - 3) personal data will be processed on the basis of:
 - a) the legal obligation referred to in Article 6(1)(c) of RODO, resulting from Article 24 of eIDAS ;
 - b) Article 6(1)(b) of the RODO in order to conclude and perform a contract;
 - c) the legitimate legal interest of the NCI referred to in Article 6(1)(f) of the RODO, in connection with Article 19(1), Article 24(2)(g) and Annex II(1)(c) of eIDAS, to ensure the security of the trust service provided and to prevent data forgery;
 - 4) if the service, e.g. for identity verification, is provided by a Partner, then personal data may be transferred to the Partner; a list of Partners can be found at: www.elektronicznypodpis.pl;

- 5) personal data will be stored for the period necessary for the provision of trust services, and with regard to the data referred to in Article 17(2) of the Act of September 5, 2016 on Trust Services and Electronic Identification (Journal of Laws of 2020, item 1173, as amended) for the period required by law, which is currently 20 years, except that in the case of the occurrence of other legal grounds authorizing the NCI to process personal data, this period may be changed according to the duration of such grounds;
 - 6) data is subject to profiling pursuant to Article 6(1)(f) of the RODO in conjunction with Article 19(1), Article 24(2)(g) and Annex II(1)(c) of eIDAS, in order to ensure the security of the service provided and to prevent data falsification. If, as a result of profiling, the NIR obtains a reasonable suspicion of a possible breach of the security of the trust service, it may stop the process of generating a certificate or revoke a certificate already generated;
 - 7) everyone has the right to access the content of their data and the right to rectify, delete, limit processing, the right to data portability, the right to object to the processing of personal data, the right to withdraw consent at any time without affecting the legality of the processing performed before its withdrawal, except that the exercise of this right may be limited by mandatory provisions of law;
 - 8) everyone has the right to lodge a complaint with the President of the Office for Personal Data Protection if he/she considers that the processing of personal data concerning him/her violates the provisions of the RODO or other regulations on personal data protection;
 - 9) providing personal data is necessary for the issuance of a certificate, if not provided, the service cannot be provided.
2. KIR - in connection with the mSzafer seal Service - processes the following personal data:
 - 1) data entered in the certificate, in particular name and address;
 - 2) data necessary for User Authorization;
 - 3) data of the Authorized person:
 - a) first and last name,
 - b) PESEL,
 - c) data of the identity document: series and number, issuing authority,
 - d) date of birth data provided for invoicing;
 - 4) data provided in connection with the handling of complaints.
 3. If the personal data referred to in paragraph (2) are not the Customer's data, the Customer shall provide them to the NCI after informing the data subject of the principles of personal data processing specified in paragraph (1) (Article 14 RODO).

§ 8.

Information for Customers

1. KIR shall be entered in the register of trust service providers under the Law.

2. A qualified electronic seal shall enjoy a presumption of data integrity and authenticity of origin of those data with which the qualified electronic seal is associated
3. An electronic seal shall not be denied legal effect or admissibility as evidence in legal proceedings solely on the grounds that the seal is in electronic form or that it does not meet the requirements for qualified electronic seals.
4. The rules for the issuance and revocation of qualified certificates, as well as the scope and limitations of the use of certificates, are defined in detail in the policies for the provision of services, in the "KIR Certification Policy for Qualified Trust Services" made available on the Internet at www.elektronicznypodpis.pl. The publication address is subject to change.
5. In the case of electronic sealing using the mSzafir Portal or the Mobile Application only KIR shall store documents for which an electronic seal is to be affixed and documents bearing the seal for a period of no more than 24 hours from the time they are stored in the KIR systems.
6. The mSzafir Seal Service is structured in such a way that:
 - 1) The User has the ability to affix an electronic seal using all Subscriber's electronic seal certificates issued for the same identifier in the KIR system,
 - 2) The User - during the period referred to in Section 5 - has access to all documents referred to in Section 5 bearing the Subscriber's electronic seal referred to in Section 1, regardless of which of the Users has submitted it.
7. The Subscriber shall be obliged - before granting User rights - to make sure that a given User is to be authorized to access the Private Key and the documents referred to in paragraph (6)(2), or to limit them in direct relation to the User. KIR shall not be liable for damages related to the abuse of the User's rights.
8. The identifier referred to in paragraph 6(1) may be: NIP and KRS number.
9. Pursuant to Article 21 of the Act, KIR shall not be liable for damages resulting from non-compliance by the Customer, Subscriber, or User with the rules set forth in the KIR Certification Policy for qualified trust services.
10. Revocation of a qualified certificate may be requested by the Subscriber, the Customer, or another person, provided that it results from the KIR Certification Policy for qualified trust services, the agreement, or other obligations of KIR.
11. A Certificate that has been revoked may not subsequently be recognized as valid.
12. The application for revocation of the Certificate is published on the KIR website www.elektronicznypodpis.pl.
13. Detailed rules for certificate revocation are set forth in the KIR Certification Policy for Qualified Trust Services.

14. Disputes arising from the use of an advanced electronic signature shall be resolved by the competent ordinary courts.

§ 9.

Technical requirements

1. The necessary technical requirements for the use of the mSzafor seal Service are as follows:
 - 1) a computer or mobile device with access to the Internet;
 - 2) Mobile Application;
 - 3) a web browser.
2. Meeting the above requirements is necessary, but does not guarantee successful use of the mSzafor seal Service. Detailed technical requirements, including in particular supported operating systems and computer hardware configurations, are available on the KIR website www.elektronicznypodpis.pl.
3. KIR reserves the right to temporarily refuse to provide the mSzafor Service, in particular within the scope of enabling to affix electronic signature online and Authorization to affix electronic signature in case the Subscriber fails to meet provisions of section 1 or 2, as well as in other cases, in particular if they could threaten a security breach of trust services, personal data protection principles or interests of trusting parties.
4. Electronic sealing using the mSzafor Portal or using the Mobile Application only may be limited to document formats supported in them. KIR guarantees that they support at least the Adobe Acrobat document format.

§ 10.

Authorization Rules

1. Authorization to the Private Key for seal will be based on the mechanisms provided in the Mobile application.
2. Upon successful Authorization User may affix an electronic seal.

§ 11.

Change of the Regulation

1. KIR reserves the right to unilaterally amend the Rules.
2. KIR shall inform about amendments to the Rules by publishing them on the website podpiselektroniczny.pl.

§ 14.

Final provisions

3. To all matters not covered by this Regulation, the relevant provisions of Polish law shall apply, in particular the provisions of eIDAS, the Act, the Civil Code and the Act of May 30, 2014 on Consumer Rights.
4. This Regulation shall apply from the 21st of March 2024.