PWPW
POLSKA WYTWÓRNIA
PAPIERÓW WARTOŚCIOWYCH

CUZ [TRUST SERVICE CENTRE] Sigillum Terms and Conditions

Status: Actual

PWPW S.A.

Ver. 1.2

Table of contents

1. General provisions

1.1 Centrum Usług Zaufania [Trust Services Centre] Sigillum has been entered under no 3 to the register of qualified entities providing certification services and under no 5 to the register of entities providing time stamping services. Thanks to the obtained entries, CUZ Sigillum may issue qualified certificates and provide certification services, including the time stamping service. CUZ Sigillum also issues commercial certificates for electronic signature which are not qualified certificates.

1.2 CUZ Sigillum operations associated with the issuing and processing of digital certificates is the Act of September 26th 2016 on Trust Services and Electronic Identification (Journal of Laws of the Republic of Poland of 2016 item 1579), executive ordinances for this act, as well as CUZ Sigillum Policies Included in the Trusted Services Policy Document no. O.I.D. 1.2.616.1.113725.0.0.0.1 by CUZ Sigillum containing O.I.D.-s of relevant trust services.

1.3 CUZ Sigillum uses its own OIDs in the issued certificates:

- For qualified certificates for signature (EIDAS structure):
  1.2.616.1.113725.0.0.3 id-qcp-natural-qscd
- For qualified seal certificates:
  1.2.616.1.113725.0.0.4 id-qcp-legal-qscd
- In the issued tokens of qualified timestamps,
  1.2.616.1.113725.0.0.5 id-qtsu

1.4 All trust services are subject of audits for compliance with eIDAS Regulation

1.5 Whoever makes a qualified signature with data used for making an electronic signature, which was assigned to another person, is subject to a fine or deprivation of liberty for up to 3 years or both these penalties jointly.

1.6 Complaints about the operating of Registration Points and the operating of CUZ Sigillum are examined by the CUZ Sigillum Manager.

1.7 CUZ Sigillum undertakes to provide Certification Services pursuant to the terms and conditions stipulated in the Agreement.

1.8 CUZ Sigillum runs its activity in a reliable manner, without breaching the provisions of the Act of September, 29th 2016 on Trust Services and Electronic Identification (Journal Of Laws of the Republic of Poland of 2016, item 1579) and the executive ordinances to the Act.

1.9 In case of the introduction of new Policy versions, which are effective for Certificates issued prior to the said new Policy versions entering into force, CUZ Sigillum shall immediately inform the Subject electronically or in writing about the introduction of the new Policy versions. If an Agreement on Provision of Certification Services has been concluded with a Subscriber, CUZ Sigillum shall also inform the Subscriber about the introduction of new Policy versions.

1.10 In matters associated with the execution of the Agreement and making complaints, the Subject / Subscriber should contact CUZ Sigillum at the address: Polska Wytwórnia Papierów Wartościowych S.A. [Polish Security Printing Works PLC], ul. Sanguszki 1; E-mail: **sigillum@pwpw.pl**, phone **+48 22 464-79-79**.

1.11 Concerning the suspension, unsuspension and revoking the Certificate, the Subject / Subscriber should contact the e-mail address **dyspozycja_certyfikat@pwpw.pl** or call

the number 0-801 64 00 33. Charge for each commenced minute of the call as for one impulse, regardless of the place in the Republic of Poland from which the call is made - compliant with the rates of the local operator.

1.12 The Agreement concerning the providing of Certification Services enters into force on the day it is signed and remains in effect for the period of Certification Services providing.

1.13 In case of revoking the Certificate, the Agreement shall be terminated.

1.14 The records of the event logs and employees' activity logs are kept and archived for a period of at least 3 years.

1.15 Information about:

- activity of its employees;
- events taking place in the ICT system which are associated with the security of the trust services provided;
- all qualified certificates and certification documents issued by CUZ Sigillum;
- events associated with time stamps issuing;
- all CRL lists issued by CUZ Sigillum;
- agreements on the provision of certification services;
- documents referred to in the eIDAS…

are kept for a period of 20 years of being created. For CUZ Sigillum certificates and the Relying party certificates, the period of storage is counted from the moment the certificates expire. After the period of storage, the archived information is destroyed in the presence of a commission, in a secure manner.

1.16 According to article 13 sections 1 and 2 of Regulation 2016/679 CUZ Sigillum informs that:

- CUZ Sigillum headquartered in Warsaw at the following address: ul. Sanguszki 1, 00-222 Warszawa shall be the administrator of Subscriber's personal data, within the meaning of Regulation 2016/679.
- CUZ Sigillum has appointed the Personal Data Inspector who can be reached by e-mail at iod@pwpw.pl in any matter concerning the processing of Ordering Party's personal data.
- Ordering Party's personal data shall be processed for marketing purposes, in particular to contact the Ordering Party by phone or by e-mail to inform the Ordering Party on services, products, and events held with participation of CUZ Sigillum, under article 6 section 1 letter a) of GDPR;
- Ordering Party's personal data may be disclosed to:
  a) entities that cooperate with CUZ Sigillum and that perform specific tasks in connection with activity conducted by CUZ Sigillum, including to entities that process personal data for the benefit of CUZ Sigillum under agreements on entrusting the processing of personal data,
  b) entities authorized to receive personal data under the rules of law.
- Ordering Party's personal data shall not be disclosed to a third country or to any international organization.

- The Ordering Party shall be entitled to access Ordering Party's data and to correct, delete, limit the processing of and transfer such data, as well as to object against the processing of such personal data.
- Within the scope of Ordering Party's approval to process personal data, the Ordering Party shall be entitled to revoke the approval to process personal data. Revocation of the approval shall not affect legality of the processing performed before the revocation of the approval.
- The Ordering Party shall be entitled to lodge a complaint with a supervisory authority, i.e. with the President of the Office for Personal Data Protection, responsible for protection of personal data, if the Ordering Party finds that the processing of Ordering Party's personal data violates Regulation 2016/679.
- Ordering Party's personal data shall not be used for profiling or for making automatic decisions.
- Ordering Party's personal data shall be processed during a period necessary to perform the task for which the data have been gathered. In case of granting the approval by the Ordering Party to process the data, until the approval is revoked.
- Disclosure of Ordering Party's personal data by the Ordering Party is voluntary. However, if the Ordering Party decides not to disclose Ordering Party's personal data or to revoke the approval to process personal data, it shall not be possible to process personal data for the marketing purposes specified herein above.

2. Signature, seal certificates and timestamp service

2.1 CUZ Sigillum certificates may not be used for acts breaching mandatory provisions of law. Digital certificates may be revoked in case of actions incompliant with a policy or rules and regulations. CUZ Sigillum shall be liable for transactions with the use of certificates up to the limit transaction value.

2.2 A qualified electronic signature verified by means of a qualified certificate has legal effects stipulated by the act, if it was made within the validity period of the certificate. An electronic signature made in the period of suspension of the qualified certificate used for its verification has legal effects from the moment the suspension is abrogated.

2.3 Data in electronic form bearing a qualified electronic signature verified by means of a qualified certificate has the same legal effects as documents bearing handwritten signatures, unless provided otherwise elsewhere.

2.4 A qualified electronic signature verified by means of a valid qualified certificate assures integrity of data bearing the signature and an unequivocal identification of the qualified certificate, in such manner that all changes of the said data and changes of the identification of the qualified certificate used to verify the said signature, made after making the signature are recognizable.

2.5 A qualified electronic signature verified by means of a valid electronic certificate constitutes evidence of that the signature was made by the person indicated in the certificate as making the electronic signature.

2.6 It may not be invoked that an electronic signature verified by means of a valid qualified certificate was not made by means of qualified devices and data subject to exclusive control of the person making the electronic signature.

2.7 Electronic seal means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.

2.8 Qualified electronic seal means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal.

2.9 Electronic seal may not be denied legal effect or admissibility as evidence in legal proceedings solely because the seal is electronic or does not meet the requirements for qualified electronic seals.

2.10 A qualified electronic seal uses presumption of data integrity and the authenticity of the origin of the data with which the qualified electronic seal is associated.

2.11 A qualified electronic seal based on a qualified certificate issued in one Member State of the European Union is recognized as a qualified electronic seal in all other Member States of the European Union.

2.12 Time stamping by a qualified entity providing certification services has in particular the legal effects of a certified date in the meaning of the Civil Code provisions.

2.13 An electronic signature time stamped by a qualified entity providing certification services is deemed to have been made no later than at the moment the service is executed. This presumption exists until the date the certification document used for verifying the time stamp expires. Extension of the existence of the presumption requires another time stamping of the electronic signature together with the data used for
the previous verification by the qualified entity providing the service.

2.14 Validity and effectiveness of an electronic signature may not be refused solely based on that it exists in the electronic form or that the data used for verifying the signature do not have a qualified certificate or that it was not made with a qualified device used for electronic signature making.

2.15 In case of issuing certificates which are not qualified certificates, information is provided that an electronic signature verified with the said certificate does not have legal effects equivalent to a handwritten signature.

2.16 Scope of qualified Time Stamping service

- Under the Policy CUZ Sigillum issues qualified time stamps for the Subscribers. The certified services Subscribers realized hereunder may be natural persons, legal persons and organizational units without legal personality. CUZ Sigillum reserves the right to make decisions concerning the groups of users entitled to obtain time stamps, in particular through defining the entities providing certification services (including services of an internal character), whose certificates shall be recognized. CUZ Sigillum reserves moreover the right to refuse to terminate the providing of a service for specific users, in particular in case of the users failing to pay the fees for the certification services provided.

2.17 Sending timestamp request

- In order to obtain a time stamp, the Subscriber should send a time stamping demand, compliant with RFC 3161 and ETSI EN 319 421. The demand should be

electronically signed by the Subscriber and contain their certificate, used for signature verification. The demand does not contain the time stamped document - only its abbreviation, which must be determined by the application used by the Subscriber. The same procedure and data formats are used for time stamps maintenance, as upon obtaining the original time stamp.

2.18 Issuing a timestamp

- CUZ Sigillum issues the time stamp after the reception of a time stamp, positive verification of the signature made under the said time stamp and positive verification of the Subject's authority to receive a time stamp. The time stamp contains the date and time (UTC) of the moment of issuing the time stamp, which may not be the same as the moment of the time stamp demand reception.

2.19 Reception of a time stamp

- After the time stamp is issued, it is sent to the user within the same session of the network connection, in compliance with RFC 3161 and ETSI EN 319 421. The attested time stamp request profile and the profile of the time stamp server response has been included in chapter 6.4 and 6.5. of CUZ Sigillum Trust Services Policy. If the time stamp may not be issued, information about the reason to refuse the performance of the service shall be sent instead.

2.20 Time stamp validity period

- The time stamp end certificate is issued for 5 years and is renewed no later than 3 years from the date of its issue.

3. Rights and obligations of parties

3.1 The Subject / Subscriber are obliged to get acquainted with the terms and conditions of Certification Services Provisioning by CUZ Sigillum to the extent of their choice, including the terms and conditions of using Certification Services and the legal effects of making
a Qualified Electronic Signature verified with a Qualified Certificate.

3.2 The Subject / Subscriber is obliged to get acquainted with the CUZ Sigillum Certification Policy and they accept all the provisions thereof.

3.3 Publishing the Subject's Certificates in the Repository shall take place in accordance with their will expressed in the Form.

3.4 The Subject gives consent to placing in the qualified certificate of one of the identifiers: PESEL [Personal ID number], NIP [Tax Identity Number], ID card number, passport number.

3.5 In case a change of the data concerning the Subject, or the Subscriber recorded in the Certificate, the Subject shall be obliged to immediately report this fact to CUZ Sigillum for the purpose of revoking the Certificate and generating a new Certificate with the correct data.

3.6 Every time upon receiving a Certificate, the Subject shall be obliged to immediately check the correctness of data included therein. In case there are any errors in the data included in the Certificate and concerning the Subject and / or the Subscriber, the Subject shall be obliged to immediately report this to CUZ Sigillum for the purpose of revoking the Certificate and generating a new Certificate including the correct data. The

control of the correctness of the Certificate must be performed prior to the first use of the Private Key associated with the Certificate. However not later than within 7 days of receiving the Certificate. After the lapse of the seven days' term, the Subject shall be entitled to place a claim at a registration point run by a Partner or by CUZ Sigillum or to the e-mail address: **sigillum@pwpw.pl**

3.7 The Subject undertakes to confirm the reception of the data storage device associated with the Certificate by signing the Components Hand-over Report.

3.8 In case of Certificates handed over in the form of a pkcs#12 file, the Subject shall be obliged to change the password of the file protecting the Certificate no later than 1 day prior to the first day of the Certificate's validity.

3.9 CUZ Sigillum is liable towards the Subject / Subscriber for all damage caused by the non-performance or undue performance of its obligations regarding Certification Services provided Under the Agreement, unless the non-performance or undue performance
of the said obligations is a result of circumstances, for which CUZ Sigillum bears no responsibility and which it could not have been prevented despite exercising appropriate care. CUZ Sigillum liability for damages in such a case shall be limited by the amount of cover, stipulated in a relevant Policy.

3.10 CUZ Sigillum shall bear no liability towards the Subject / Subscriber for any damage resulting from causes different than the non-performance or undue performance by CUZ Sigillum or by authorized entities acting on its behalf of its duties, in particular CUZ Sigillum shall bear no liability for:

a. Hardware environment and system software installed on the Subject's computer;
b. The effects of incorrect use of the Subject's private key;
c. The effects of the use of the Subject's private key by an unauthorized person;
d. The results of the loss of security of the cryptographic algorithms used by CUZ Sigillum, subject to the use of the said algorithms not being compliant with the Policy or mandatory provisions of law;
e. The results of disclosing by the Subscriber to third party's information such as: PIN codes, access security measures for a file associated with the Private Key Certificate;
f. The results of a statement of will made by the Subject using a Certificate containing errors or omissions resulting from causes attributable to the Subject;
g. Towards the recipients of Certification Services for damage resulting from Certificate use exceeding the scope defined in the relevant Policies, including in particular damage resulting from exceeding the Highest Transaction Limit Value if it was indicated in the Form.

3.11 Regarding the providing of Certification Services, CUZ Sigillum acts through Registration Points referred to as Partners, for the acts and omissions of whom CUZ Sigillum shall be liable as for its own acts or omissions. A list of CUZ Sigillum Partners is available at the website **www.sigillum.pl**

3.12 If changes in Policy affect terms of this document, changes will be updated

3.13 CUZ Sigillum reserves the right to introduce now Policy versions regarding the providing of Certification Services. The place the new Policy versions are published is the Repository – www.sigillum.pl.

3.14 The provisions of new Policy versions enter into force the day they are published in the Repository and are effective for Certificates issued after the said day.

3.15 CUZ Sigillum may decide, in cases justified by requirements of the security of information protected by means of the Certificates issued so far, that the new Policy versions shall be effective also for Certificates issued prior to the new Policy versions entering into force.

3.16 If the Subject / Subscriber raise no qualifications to the new Policy versions, it shall be deemed that they got acquainted with the contents thereof, that they accept it and undertake to observe the provisions thereof.

3.17 Should the Subject not accept the new Policy versions, they may terminate the Agreement by delivering a written notification containing their statement of will.

3.18 CUZ Sigillum shall be entitled to terminate the Agreement without notice period in case the Certificate shall be revoked in situations stipulated in the Act.

3.19 Should CUZ Sigillum initiate a procedure of terminating its activity, the Subject / Subscriber shall grant their consent to hand over all data gathered in the process of handling and issuing the certificate to another Trust Centre or to an Entity exercising supervision over Trust Services.

3.20 The Agreement may be signed by the Subject / Subscriber using a Qualified Certificate issued by CUZ Sigillum held by them. In such case the person representing CUZ Sigillum shall also sign the Agreement using a valid Qualified Certificate.

3.21 The Subject / Subscriber is obliged to pay to CUZ Sigillum or the Partner fees due for the providing of Certification Services stipulated in the Agreement and for the technical components associated with the Certification Services, according to the calculations done based on the up to date Price List in power on the day the Agreement is signed, constituting an Attachment to the Agreement.

3.22 Relying Party obligations:

- Upon verifying the validity of a secure electronic signature or qualified timestamp Time stamp validity is examined based on the validity of the certification document issued to the qualified entity by the ministry of digital affairs or by an entity authorized by the minister.
- For the purpose of verifying the validity of time stamps issued hereunder, the Relying Party is obliged to use the public key placed on the TSL list as the Point of Trust.
- The Public Key constituting a Point of Trust must be downloaded in a manner assuring its authenticity and integrity (e.g. directly from the owner of the key or a Registration Point acting on their behalf or pursuant to a procedure assuring the verification of the public key fingerprint).
- The Relying Party shall be obliged to protect the integrity of the public key being a Point of Trust. In case of any doubt concerning the integrity and authenticity of the public key, the Relying party shall be obliged to confirm it, for example by comparing the fingerprint of the public key they have with a fingerprint published by the Supervisor Body or an authorized entity.

4. A record of changes in the document

Description of the amendment	Version	Date
Document creation	1.0	01.06.2017
Document publication	1.0	01.07.2017
Personal data update	1.0	09.06.2018
Document update	1.1	12.09.2019
Document review	1.2	14.10.2020