PWPW
POLSKA WYTWÓRNIA
PAPIERÓW WARTOŚCIOWYCH

CUZ [TRUST SERVICE CENTRE] Sigillum Terms and Conditions

Status: Current

PWPW S.A.

Ver. 1.4

Table of contents

1. General provisions

1.1 Sigillum Trust Services Center has obtained an entry in the register of qualified trust service providers. With the obtained entry, Sigillum CUZ can provide the following services.

- Issuing qualified certificates for electronic signature and qualified certificates for electronic seal
- Creation of qualified electronic signature online and creation of qualified electronic seal online
- Qualified management of remote electronic signature devices and remote electronic seal devices;
- Creation of qualified electronic time stamps;

CUZ Sigillum also issues commercial certificates for electronic signature that 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 Suspension, revocation of suspension and cancellation of the Certificate, the Subscriber/Orderer should carry out using the functionality provided by the Sigillum system after logging into his account or report to the registration desk. In case of problems, he/she can contact at the e-mail address dyspozycja_certyfikat@pwpw.pl or at telephone number 0-801 64 00 33.

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 Subscriber 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 trust service provider certificates 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 and associated private and public keys 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 7.4 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.

2.21 The validity periods of Sigillum's CUZ certificates and Subscribers' certificates, are no more than:

- 11 years for CUZ Sigillum certificates;
- 3 years for certificates of Subscribers
- 1 hour, for certificates issued for the issuance of a remote one-time signature

2.22 Information on certificate revocations:

- The list of revoked certificates is generated and published no less frequently than every 12 hours, regardless of whether revocations or suspensions have occurred;
- If a certificate revocation or suspension or revocation of a certificate suspension has occurred since the generation of the last CRL, the CRL is generated and published immediately after the event.

- Sigillum CUZ provides methods for verifying the status of a certificate through the OCSP service or verifying the status of a certificate in the CRL.
- Revocation status information published via CRLs is made available until the certificate is valid. Therefore, the CRL list does not contain the ExpiredCertsOnCRL extension.
- Revocation status information published via the OCSP service is made available for a period longer than the validity period of the certificate. Therefore, the OCSP response contains an ArchiveCutOff dilution with the date set to the “notBefore” time and date value of the CA certificate.
- For short-term certificates with a confirmed validity period of less than 24 hours, no revocation functionality is provided. Consequently, these certificates have the validity guarantee extension id-etsi-extvalassured-ST-certs (OID: 0.4.0.194121.2.1). Despite the inability to revoke these certificates, the OCSP service allows verification of the status of these certificates.
- In case of compromise of CUZ Sigillum keys:
  - all certificates of sunscribers and trust service provider certificates on the certification path associated with the compromised authority are revoked;
  - the latest CRL will be generated with the “nextUpdate” field set according to ETSI EN 319 411-2 to “99991231235959Z”, which will be kept intact and available for inspection, guaranteeing the availability of an information service on the status of certificates for at least 10 years.
- In the event of termination of CUZ Sigillum, the issuance of new certificates will be halted and the activities described in Section 5.8 of the CUZ Sigillum Service Provision Policy and the CUZ Sigillum Termination Plan will be carried out. In addition:
  - Certificate revocation service will be maintained until Sigillum's CUZ authority certificate is revoked;
  - All subscribers' certificates will be revoked, a final CRL will be generated with the “nextUpdate” field set according to ETSI EN 319 411-2 to “99991231235959Z”, which will be kept intact and available for inspection.
  - OCSP service will be maintained until the end of Sigillum's CUZ certificate validity.
  - CUZ Sigillum shall transfer the documents and data referred to in Article 17(1) of the Law of September 29, 2016 on Trust Services and Electronic Identification, including the latest CRL, to the Minister of Information Technology, who shall keep the data until the end of the period, in accordance with Article 20(2) of that Law.

3. Qualified signature and seal creation service provided through a qualified service for managing remote electronic signature and seal creation devices

3.1 The remote signature service is available only to adults

3.2 After the remote signature is executed, the time for downloading the signed document is limited. It will be possible to download the document during the browser session and through the provided link. When the availability time expires, the file will be deleted. The availability time of the file will be configurable within the framework of partner agreements or specified in the product details.

3.3 For one-time signatures, a single identity verification will be used for both the issuance of a short-term certificate as well as the creation of a signature

3.4 Available signature formats:

- CAdES (CMS Advanced Electronic Signatures) - Electronic signature format based on the CMS standard (Cryptographic Message Syntax, RFC 5652).

  Characteristics:

  A binary signature that can be attached to any type of file (e.g., documents, binary data).

  Applications:

  Popular for signing general-purpose files and documents. Often used in ePUAP systems, e-documents, archiving.

  Features:
  Supports long-term extensions (timestamp, OCSP/CRL), flexible and widely used.
- XAdES (XML Advanced Electronic Signatures) - An electronic signature format based on XML Signature (XMLDSig).

  Characteristics:

  Signature is embedded in XML structure, which allows easy integration with XML systems, e.g. e-invoices, XML documents, web services.

  Applications:

  Typical in e-government, XML document exchange systems (e.g., e-invoices, e-procurement).

  Features:

  Allows signature verification and validation of XML data, supports extensions such as timestamp, OCSP/CRL
- PAdES (PDF Advanced Electronic Signatures) - A signature format dedicated to PDF documents.

  Characteristics:

  Signature is embedded directly into the PDF file, allowing text, images and document structure to be signed.

  Applications:

  Common in signing electronic PDF documents - e.g. contracts, invoices, reports.

  Features.

  Allows integration of signature with visual representation (e.g. visual signature on document), supports long-term extensions.

  1 hour, for certificates issued for the issuance of a remote one-time signature
- JAdES (JSON Advanced Electronic Signatures) - A JSON-based electronic signature format.

Characteristics:

Signature in JSON format, ideal for modern web applications, APIs and REST services.

Applications:

Increasingly popular in systems integration, JSON message signing, e-health, e-government environments.

Features:

Lightweight, machine and human readable, works well with web technologies, supports signature extensions according to ETSI.

The above list of signature formats for the user performing the signature is limited by the agreement with the partner or the terms and conditions accepted by the user and the type of service purchased.

3.5 Signature documents must be provided in binary form in a suitable format compatible with the signature format or in abbreviated form.

3.6 The supported parameters of the qualified signature and seal creation service are as follows:

- Signature format - In what form the signature will be saved: CAdES, XAdES, PAdES, JAdES;
- Signature level

  B-B (Baseline - Basic) The simplest level of signature.

  Includes: Electronic signature. Signer's certificate.

  Use: Short-term validity, e.g. invoices, internal documents.

  Verification: Only possible if the certificate is still valid and has not been revoked.

  B-T (Baseline - Timestamp) - Extension of the B-B level with a timestamp.

  Includes: Everything from the B-B level. A cryptographic timestamp that confirms the existence of a signature at a specific point in time.

  Use: Documents that require confirmation of the date of the signature.

  Verification: Possible even after the certificate has expired, thanks to the timestamp.

  B-LT (Baseline - Long Term) - Long-term signature with full verification data.
  Includes: Everything from the B-T level.

  Verification data:

  Certificates (including chain of trust),

  Revocation data (CRL, OCSP),

  Timestamp certificates.

  Use: Documents that need to be verifiable for many years.

  Verification: possible without internet access, as all data is embedded in the signature.

  B-LTA (Baseline - Long Term Archival) - The highest level of signature, providing archival durability. Includes: Everything from the B-LT level.

Document timestamp (document timestamp), which confirms the existence of the entire data set at a given time.

- Signature type:
  - Enveloped - The signature is inside the document being signed.;
  - Detached - The signature is a separate file, independent of the document being signed.
  - Enveloping - The document is inside the signature - the signature contains the entire document as part of its structure.

3.7 The qualified signature and seal creation service was based on a certified QSCD device managed by CUZ Sigillum.

3.8 Qualified signature and seal creation service allows presenting documents for signature that are saved in PDF/A-1a format.

4. Rights and obligations of parties

4.1 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.

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

4.3 The subscriber is obliged to provide the TSP with accurate and complete information to register the subscriber.

4.4 The Subscriber/Ordering Party is obliged to use the certificate keys in accordance with all the obligations and limitations presented.

4.5 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, if he orders a certificate with such an identifier. For corporate customers, there is also an option to order certificates with a different subscriber identifier (other than PESEL number, NIP, ID card number, passport number) - generated by Sigillum.

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

4.7 If the subject's private key has been lost, stolen or potentially compromised, control of the subject's private key has been lost as a result of compromised activation data (e.g., PIN), or for other reasons, the Subscriber is obliged to stop using the key and immediately notify CUZ Sigillum of this fact in order to invalidate the Certificate and issue a new one containing correct data

4.8 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**

4.9 For certificates issued on physical media, the Subject undertakes to confirm the reception of the data storage device associated with the Certificate by signing the Components Hand-over Report.

4.10 The subscriber shall use the private key(s) only for cryptographic functions within a secure cryptographic device

4.11 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.

4.12 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.

4.13 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, security access to files associated with the Private Key Certificate, the user's credentials for his/her individual account in the Sigillum System, access to the authenticator device and application for confirming key use operations;;
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.

4.14 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**

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

4.16 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.

4.17 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.

4.18 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.

4.19 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.

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

4.21 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.

4.22 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.

4.23 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. For remote services, the contract can also be concluded electronically in the form of acceptance of the terms and conditions.

4.24 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.

4.25 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.

5. Availability of services

5.1 The repository is available 24 hours a day, all days a year. Any unavailability time of the repository shall not exceed 2 hours each time, and the minimum availability on a monthly basis is 99% of the time.

5.2 CUZ Sigillum provides certificate status verification service, free of charge continuously 24 hours a day, 7 days a week.

5.3 Response times

Name of System	**Name of Subsystem**	**Response time**	**Repair time/time to set up replacement solution**
Trust Services Center	CA/OCSP/UZC	Up to 1 hour	Up to 8 hours
	REPO/Archive	Up to 1 hour	Up to 8 hours
EPR	EPR	Do 1 godziny w dni pracujące	Up to 8 hours on working days
Service for creating electronic signatures and electronic seals		Up to 1 hour on working days	Up to 8 hours on working days
Trust Services Center - Certificate Issuance Hotline	Certificate Revocation Hotline	Up to 1 minute	Up to 30 minutes

6. 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
Document update	1.3	01.07.2025
Document update	1.4	27.11.2025