PWPW
POLSKA WYTWÓRNIA
PAPIERÓW WARTOŚCIOWYCH

CUZ SIGILLUM TRUST SERVICES POLICY

Date: 15.06.2018

Status: Actual

PWPW S.A.

Ver. 1.1

Table of contents

1. Introduction

1.1. Dictionary

1) The Act of September, 5th 2016 on trust services and electronic identification. (Journal of Laws of 2016 item 1579) of the Act, henceforth referred to asthe Act.
2) The Ordinance of the Minister of Digitisation of October, 5th 2016 on the national trust infrastructure (Journal of Laws of 2016 item 1632), henceforth referred to as The Ordinance.
3) Regulation of the European Parliament and the Council (EU) no 910/2014 of July, 23rd 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, henceforth referred to as Regulation.
4) Policy - this Trust Service Policy
5) PKI - Public Key Infrastructure
6) Centrum Usług Zaufania Sigillum [Sigillum Trust Services Centre] — it is an electronic certification centre with separated organisation, operating within the structures of the Polska Wytwórnia Papierów Wartościowych S.A. [Polish Security Printing Works], henceforth referred to as 'PWPW SA', providing certification services to the extent covered by the Policy, henceforth referred to as 'CUZ Sigillum'.
7) Rada Zatwierdzania Polityk Certyfikacji [*Certification Policy Approval Council*] PWPW SA - the body responsible for approving Certification Policies, henceforth referred to as RZPC PWPW SA
8) Registration Point - an organisational unit of CUZ Sigillum or another organisational unit acting on its behalf, performing certain functions associated with the provision of certification services, pursuant to the Policy.
9) RSA Algorithm - a cryptographic algorithm, defined unequivocally by an object identifier „{ joint-iso-ccitt(2) ds(5) module(1) algorithm(8) encryptionAlgorithm(1) 1 }".
10) Key - a number, symbol or a sequence of numbers of symbols, unequivocally determining the cryptographic transformation among the transformation family defined by the cryptographic algorithm.
11) RSA algorithm pair - two keys (private key and public key), determining the mutually reverse transformation among the family of transformations defined by the RSA algorithm.
12) Signing key - a private key used for making an electronic signature; the signing key constitutes data used for making an electronic signature within the meaning of the Act.

13) Signature verifying key - a public key used for verifying an electronic signature; a key verifying a signature constitutes data used for verifying an electronic signature or used for verifying an electronic attestation within the meaning of the Act.
14) Infrastructure keys - cryptographic keys of cryptographic algorithms used for purposes other than making or verifying a secure electronic signature or the verification of a secure electronic signature or electronic attestation and in particular keys used:

a) in key negotiating or distribution protocols, assuring the confidentiality of data,

b) for assuring, during transmission or storage, the confidentiality and integrity of certification applications, user keys, event logs,

c) for verification of access to devices, verifying or signing software.

15) Certificate of the signature verifying key - electronic certificate, with which a signature verifying key is assigned to a person making an electronic signature which makes it possible to identify the person; the signature verifying key certificate is a certificate within the meaning of the Act.
16) Public key certificate - certificate of the key verifying the signature.
17) Qualified electronic signature certificate - an electronic signature certificate issued by a qualified trust services provider and meeting the requirements stipulated in Attachment I to Regulation no 910/2014.
18) Qualified electronic seal certificate - an electronic seal certificate issued by a qualified trust services provider and meeting the requirements stipulated in Attachment III to Regulation no 910/2014.
19) Qualified electronic time stamp - means an electronic time stamp meeting the requirements stipulated in art. 42 of the Ordinance.
20) Electronic attestation - data in electronic form, which together with other data, to which it was added or logically associated with, make it possible to identify the entity providing certification services or the authority issuing certification documents and meeting the following requirements:
    a) it is prepared by means of secure devices used for making electronic signatures remaining under the exclusive control of an entity providing certification services or an authority issuing certification documents and with data used for making an electronic signature,
    b) any change of certified data is recognisable.
21) Polish Security Printing Works Hereinafter called in the document PWPW SA
22) GDPR/RODO - Regulation of the European Parliament and of the Council (EU) 2016/679 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 (hereinafter referred to as Regulation 2016/679).

23) Certificate - an electronic certificate with which data used for the verification of electronic attestation is associated with an entity providing certification services or the minister in charge of the economy and which makes it possible to identify the entity or authority.
24) Certification path of the signature verifying key - an ordered sequence of certificates or certificates and a qualified certificated, created in such a way, that with data used for the verification of electronic attestation and names of the issuer of the first certificate on the path it is possible to prove that for each of the two directly subsequent certificates or the certifying document and certificate the electronic attestation contained in one of them was prepared by means of data used for making an electronic attestation associated with the other one; data used for the verification of the first electronic certificate are a 'Point of trust' for the verifier.
25) Point of trust - see 'Certification path of the signature verifying key'.
26) CRL List - list of revoked and suspended public key certificates issued by a given entity providing certification services and possible of revoked certificates issued by the entity. The list is electronically certified by the entity providing certification services.
27) ARL list - a list of revoked certificates issued by a given entity providing certification services. The list is electronically certified by the entity providing certification services. An entity does not have to issue an ARL list, if CRL list it issues contains information concerning the revoked certificates.
28) Subject - a natural person, who concluded with PWPW SA an agreement on providing certification services.
29) Relying party - a natural person, legal person or an organisational unit without legal personality, which may act based on a certificate or certificate document within the limits defined in the certification policy. A Subject is also a relying party if they perform actions based on a certificate or certificate document issued pursuant to the Policy.
30) Subscriber - a legal person or an organisational unit without legal personality, which may finance certification services provided for a given Subject. Data of the Subscriber may be included in the Subject's certificate. The Subscriber is entitled to revoke the Subject's certificate (art. 21 item 2 paragraph 5 of the Act).
31) Qualified Certification Services - certification services provided by an entity holding a record in the register of qualified entities providing certification services, pursuant to the Policy corresponding to the record.
32) Technical Component - hardware used for the purpose of generating or utilising data used for the making of a secure electronic signature or electronic attestation.

33) Key Module - a device cooperating with the Technical Component, storing infrastructure keys or data used for making qualified electronic signatures or electronic attestations or keys protecting the data, or storing parts of these keys or data.
34) Qualified device used for the verification of an electronic signature - a devices used for the verification of an electronic signature meeting the requirements stipulated in the Act and Ordinance.
35) Highest limit transaction value - a pecuniary amount defining the limit of the highest value of a transaction for which a Certificate may be used. The amount of the limit transaction value is defined by the Subscriber / Subject.
36) Certification Request - a file in the PKCS#10 format, containing among others a name identifying the Subject and the public key. Terms used in the Policy and not defined hereinabove should be interpreted pursuant to the definitions provided in the Act and Ordinance.
37) Trust service - means an electronic service normally provided for remuneration which consists of:
    a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
    b) the creation, verification and validation of certificates for website authentication; or
    c) the preservation of electronic signatures, seals or certificates related to those services;
38) TTP – see Trusted Third Party
39) Trusted Third Party - A logical PKI Party that uses an electronic signature mechanism and a certificate to authenticate specific content trusted by the other parties in that model
40) QSCD - Qualified Signature Creation Device - means an electronic signature creation device that meets the requirements laid down in Annex II of eIDAS Regulation
41) Qualified Electronic Seal Creation Device' means an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II of eIDAS Regulation
42) Secure Signature Creation Devices - which the conformity has been determined in accordance with Article 3(4) of Directive 1999/93/EC shall be considered as qualified electronic signature creation devices under this Regulation.

1.2. Introduction

This document is the certification Policy of PWPW SA, for the electronic certification centre, created within the PWPW SA organisational structures, called Centrum Usług Zaufania 'Sigillum', henceforth referred to as CUZ Sigillum, concerning the providing of a qualified trust service

comprising the issuing of qualified electronic signature certificates and qualified electronic seal certificates.

This Policy is effective for certification services regarding the issuing of qualified certificates issued in compliance with the requirements stipulated by the Regulation of the European Parliament and of the Council (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/EC. The Policy is protected by PWPW SA intellectual property rights.

CUZ Sigillum has been designed and implemented in a manner allowing for meeting the requirements imposed on providers of qualified trust services providing services of issuing qualified certificates under Regulation no 910/2014 and the national act on Trust Services and relevant ordinances, as well as the requirements of other mandatory provisions of law and existing international standards regarding the creation and operating of PKI systems, in particular taking into account the recommendations included in RFC 3647 'Certificate Policy and Certification Practices Framework'.

CUZ Sigillum assures that all the Subjects' private keys, whose public keys are certified in compliance herewith, are stored in devices which meet the requirements imposed by the Commission Implementing Decision (EU) 2016/650 of April, 25th 2016, laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

To ensure the best possible access to the services for persons with disabilities., CUZ Sigillum offers technical support via helpline on +48 22 464 -79-79 and visit of RA Inspector in place indicated by the Client after setting all the terms and dates.

1.3. Name of the document and its identification

Identifier of this Certification Policy, registered in the KRIO [National Register of Object IDs]

Name of the Policy	CUZ SIGILLUM TRUST SERVICES POLICY
Policy version	1.1
Version status	Actual

Reference number / OID (Object Identifier)	{ iso(1)member-body(2) PL(616) organisation(1) pwpw(113725) id-sigillum(0)id-qtso(0)id-qtsp-doc(0)id-qtsp-doc-version(1){1}}
Date of entry into force	15.06.2018
Expiry date	Until further notice

This Trust Service Policy is a collection of policies and regulations:

- used by CUZ Sigillum for the issuance of qualified certificates. Each qualified certificate issued by CUZ Sigillum contains the identifier of the Certificate Policy used to issue this certificate.
- used by qualified time stamp service. Each issued timestamp token contains the policy ID of the time stamp service

CUZ Sigillum certification policies for qualified certificates are based on the requirements defined in ETSI EN 319 411-2 Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates:

- For qualified certificates for signature - on the QCP-n-qscd (Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)) policy
- For qualified seal certificates - on the QCP-l-qscd (Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal-qscd (3)) policy

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

- 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

Policy of providing qualified time stamping is based on the requirements defined in ETSI EN 319 421 Policy and Security Requirements for Trusted Services Providers, issuing

Time-Stamps, identified as BTSP itu-t (0) identified-organization (4) etsi (0) time-stamp Politician (2023) policy-identifiers (1) best-practices-ts-policy (1)

CUZ Sigillum in the issued tokens of qualified time stamps uses its own OID: 1.2.616.1.113725.0.0.5 id-qtsa

1.4. PKI Participants

The PKI system operated by CUZ Sigillum, which performs its services based on the entry to the Register of Qualified Trust Services Providers, comprises:

- Certification Authority

- Time Stamp Authority

- Registration Points

Next to the CUZ Sigillum domain, there is an NCCert (National Certification Authority) managed by the NBP (National Bank of Poland) that issues certificates to TSP and publishes their data on the national TSL list.

The PKI hierarchy of NCCert 2016 is:

Level	**Parameter**	**Content**
Level 1 - Root CA	DN Name	2.5.4.97=VATPL-5250008198, CN=Narodowe Centrum Certyfikacji, O=Narodowy Bank Polski, C=PL
	Serial number	40 f8 f7 8a b0 e3 64 10 56 91 c8 d9 e0 2c f8 c1 c6 40 0a 46
	Key identifier	29 b3 c8 c4 df a3 87 f8 66 05 12 58 fd 46 2a b8 98 0d 79 87
	Fingerprint [SHA-1]	89 ce c4 84 2f af 40 1b 48 d0 f2 1d 80 43 e9 a6 3e 7c 02 d5
Level 2 - Sub CA	DN Name	2.5.4.97=VATPL-5250001090, CN=CUZ Sigillum - QCA1, O=Polska Wytwórnia Papierów Wartościowych S.A., C=PL
	Serial number	76 2d 27 ca b5 00 27 e8 c9 e9 e0 77 67 e7 04 8b f4 e6 8d 75
	Key Identifier	42 fa 4f 86 36 81 9d 28 a1 9e 2d 1a b5 50 bb aa 27 f2 9c b4
	Fingerprint [SHA-1]	38 8e 94 d9 5d f7 d0 40 d6 63 1f 07 d2 78 3e bb 20 db 6c 48
Level 3 – OCSP	DN Name	2.5.4.97 = VATPL-5250001090 CN = CUZ Sigillum - QOCSP1 O = Polska Wytwórnia Papierów Wartościowych S.A. C = PL
	Serial number	62 be 70 95 fa 47 fc 0d

	Key Identifier	ac 75 11 49 48 ae c9 20 99 30 36 00 79 ea 01 76 99 28 7a 30
	Fingerprint [SHA-1]	74 86 7f 51 d5 a7 bd 47 9b 2a ed 98 77 59 c3 a1 c9 e5 a8 4a
Level 2 - UZC	DN Name	2.5.4.97 = VATPL-5250001090 CN = CUZ Sigillum - QTSA1 O = Polska Wytwórnia Papierów Wartościowych S.A. C=PL
	Serial number	02 37 16 df b8 0b 52 88 b2 b7 e0 88 e1 07 c5 b9 eb c4 9d ab
	Key Identifier	73 12 32 67 84 48 76 79 fe 77 ca 88 70 c3 6b e6 45 5d 17 ab
	Fingerprint [SHA-1]	9f 76 27 fe 88 f6 60 5a 2c f2 e5 25 e4 7b 17 df 72 c0 58 01

1.4.1. Certification Authority

CUZ Sigillum as a certification authority is issuing qualified certificates for qualified electronic signatures and qualified electronic seals certificates, with a structure resulting from the ETSI standards concerning certificates' structure.

The Authorities operate in compliance with the requirements of:

- Regulation of the European Parliament and the Council (EU) no 910/2014 of July, 23rd 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
- Act on Trust Services and Electronic Identification of September, 5th 2016 (Journal of Laws of the Republic of Poland of 2016, item1579).
- Ordinance of the Minister of Digitisation of October, 5th 2016 (Journal of Laws of the Republic of Poland of 2016, item1632).
- The standards resulting from the COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of April, 25th 2016, laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
- The qualified certificates issued meet the requirements of the following standards:
    - ETSI EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
    - ETSI EN 319 411-2 Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

The authorities issue certificates:

- For the purposes of building a certification path (overlapping certificates used for renewing the authority certificate)
- For the needs of verification of the status of issued certificates (OCSP service certificate)
- Qualified electronic signature for natural persons
- Qualified electronic seal for legal persons

Time in certification systems is synchronized with UTC at least once a day.

1.4.2. Time Stamp Authority

A time stamping service has been commissioned within the CUZ Sigillum Qualified Certification Authority, operating in compliance with the requirements of the Regulation and the Act.

Time stamp tokens are compliant with the requirements of RFC 3161 and the ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles standard.

The private key of the time stamping service is used solely for certifying time stamp tokens. Tokens are issued only if the CUZ Sigillum system had embedded service certificate issued by National Certification Center (NCCert). Tokens issuance service will be stopped when certificate expires.

The time stamping service uses mechanisms assuring time synchronisation with two international time references, with an accuracy of 1 second. The synchronised time is compared with an internal time source of high precision. In case a time difference larger than 1 second is discovered, timestamps issuing is stopped and the event is logged.

The internal time source correctly performs the handling of the leap second.

Time in time stamp systems is synchronized with UTC at least once a day.

1.4.3. Registration Points

The CUZ Sigillum Certification Authority cooperates with Registration Points (RP). They represent certification authorities in contacts with subjects and have privileges delegated to them by the certification authority concerning the confirmation of identity during the registration of a current of future subject. The CUZ Sigillum may confirm the identity of a person applying for a certificate without their personal presence at the registration point, based on a notarial confirmation of identity. CUZ Sigillum may also appoint other persons confirming on their behalf the identity of an applicant and authorised to accept applications and conclude agreements on the provision of certification services.

The Registration Point tasks are described:

1) In the Registration Point rules and regulations constituting an internal document of CUZ Sigillum – if the Registration Point is an organisational Unit of PWPW SA or

2) in an agreement between PWPW SA and an entity operating a Registration Point.

An up to date list of Registration Points is presented at the CUZ Sigillum website at the address:

http://sigillum.pl/kontakt.html

1.5. Obligations of the parties

1.5.1. Subject's obligations

Prior to filing an application for a public key certificate and signing an agreement on the provision of certification services, the Subject is obliged to get to know the contents of the Policy and the Terms and Conditions of Providing Services.

If the Subject uses certificates issued pursuant to the Policy, it means that they are acting as a Relying Party. Upon performing the said actions, they are bound by all the conditions set forth in chapter 1.2.6.

The Subject is obliged to use private keys associated with the qualified certificates issued pursuant to the Policy solely in a secure device for making qualified signatures, within the meaning of the Act.

The Subject is obliged to keep confidential the private keys associated with the public key certificates issued pursuant to the Policy. The Subject bears full responsibility for the secure storage of their private key. In case the keys are stored in technical components or key modules secured with passwords or PIN codes, the Subject is obliged to store the password or PIN code securely, separated from the used technical component or key module.

In case of loss of the private key associated with the public key certificate issued hereunder and in case of disclosing the key or a reasonable suspicion that such disclosure may have taken place - the Subject is obliged to report the fact of such event taking place immediately to CUZ Sigillum in order to suspend or revoke the public key certificates associated with the lost or disclosed keys.

The Subject is obliged to provide in the agreement on the provision on certification services and the certification application true and complete data of an extent required by the agreement or certification application, as the case may be.

In case of an application of a Subscriber for the placing of the Subscriber data in the Subject's public key, the Subscriber makes a proper declaration on a CUZ Sigillum form.

After receiving a public key certificate the Subject is obliged to verify its correctness. In case of any irregularities, in particular, incorrect values of the fields determining the Subject's identity, they will be obliged to report this fact immediately to CUZ Sigillum for the purpose of revoking the public key certificate and generating a new public key certificate with correct data.

In case a change of the data concerning the Subject recorded in the public key certificate, they will be obliged to immediately report this to CUZ Sigillum for the purpose of revoking the public key certificate and possibly generating a new public key certificate with the correct data.

The Subject is obliged to bear the costs of the provision of certification services according to the price list valid at CUZ Sigillum on the day of signing the agreement on the provision of certification services - unless the costs are borne by the Subscriber or CUZ Sigillum may not obtain the costs from the Subscriber.

In case of generating keys by the Subject, the Subject will be responsible for the compliance of the process with the requirements of the Act and the Ordinance.

1.5.1.1. TimeStamping Service Subject's obligation

Prior to sending a demand to issue a time stamp, the Subject is obliged to get acquainted with the contents hereof.

The Subject is obliged to pay the fees for the provided certification services according to the price list in place at CUZ Sigillum on the day of issuing the time stamp and in accordance with the rules defined in the agreements concluded.

For the purpose of obtaining a time stamp, the Subject is obliged to send a demand for time stamping in the format and in the manner defined herein. The demand must be electronically signed by the Subject.

Extension of the time stamp validity prevents to expiry of the time stamp as a result of the revoking or expiry of the certification document used by CUZ Sigillum upon issuing the primary time stamp.

The Subject is obliged to assure the time stamp validity, except if the data for which the time stamp was issued lose validity or for other reasons for which it will not be important for the Subject to possess evidence of the existence of the said data at a given time.

The time stamp validity extension may be performed by the same entity providing qualified time stamping certification services, at which the original time stamp was obtained (after a change by this entity of the data used for time stamping) or by another qualified entity.

The time stamp validity extension should be performed prior to the expiration of validity of the certification document, used by the entity providing the qualified time stamping certification services.

The time stamp validity extension comprises the obtaining of a new time stamp confirming the existence at a given moment of:

1) Time-stamped data,

2) the previous time stamp.

Attention should moreover be drawn to the fact, that in case of extending the validity of a time stamp obtained due to the possibility of verification of the validity of a qualified electronic signature, it may be necessary to time-stamp also the materials, based on which the signature validity is examined, that is the qualified certificate and relevant CRL, ARL lists, OCSP responses, electronic certificates or stamps.

1.5.2. Obligations of the Subscriber

The Subscriber is obliged to appoint a duly authorised representative / representatives, responsible for the supervision over the process of correct granting and revoking of the rights to use the Subscriber data in public key certificates issued hereunder.

The Subscriber gives written consent for placing the Subscriber's data in the public key certificate issued hereunder, by concluding with CUZ Sigillum an agreement on the provision of certification services.

Prior to giving the consent for placing the Subscriber's data in the public key certificate, a representative of the Subscriber is obliged to get to know the Policy and the Terms and Conditions of Providing Services and accept the provisions stipulated therein.

In case a change of the data concerning the Subscriber recorded in the public key certificate, the Subject is obliged to immediately report this to CUZ Sigillum for the purpose of revoking the public key certificate and possibly generating a new public key certificate with the correct data.

The Subscriber is obliged to bear the costs of the provision of certification services according to the price list valid at CUZ Sigillum on the day of signing the agreement on the provision of certification services - if the Subscriber included an obligation to bear the said costs therein.

The Subscriber and PWPW SA must be independent entities, except for the situation in which PWPW SA issues qualified certificates for its employees.

1.5.3. 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 minister of Digital Afairs or by an entity authorised 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 is 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 is obliged to confirm it, for example by comparing the fingerprint of the public key they have with a fingerprint published by the minister in charge of the economy or an entity authorised by the minister.

1.5.4. Obligations concerning the use of qualified certificates

Upon verifying the validity of a secure electronic signature, the Relying Party is obliged to perform the following procedure:

1) obtain from the qualified entity providing certification services a correct time stamp, confirming the existence at a given time of a document bearing the qualified electronic signature, whose validity is to be verified.

2) verify the validity of the qualified certificate, which is to be used for the verification of the secure electronic signature, with the following conditions:

a) validity of the qualified certificate is verified based on the proper certification path of the signature verifying key.

b) the signature verifying key certification path must be correctly verified only if all certification documents and qualified certificates contained therein are valid at a given time (i.e. the date on which the certification document or qualified certificate is expired remains in the validity period of the certification document or qualified certificate and the certification document or qualified certificate is not included in the relevant CRL or ARL list) and they bear Policy identifiers from a Policy set defined by the verifier.

c) the signature verifying key certification path contains a certification document issued to a qualified entity by the Minister of Digital Affairs- art. 27 item 2 of the Act.

d) the CRL and ARL list used to verify the validity of qualified certificates and certificate documents located on the signature verifying key certification path according to point b), have been issued by qualified entities providing certification services later than at the moment defined in the time stamp described in point 1), however not later than the date of issuing the first CRL or ARL list, as the case may be, after the lapse of the validity term of the verified certificates and certification documents.

3) verification of the secure electronic signature, which the document bears, using the qualified certificate verified in the manner described hereinabove. Additional conditions associated with the verification of a secure electronic signature have been described below, in the paragraph titled ‘Additional conditions of secure electronic signature verification’.

The Relying Party is not obliged to obtain the time stamp mentioned in point 1) above, if another entity has previously obtained the time stamp, issued by a qualified entity providing certification services and delivered the time stamp to the Relying Party and the Relying Party may confirm the validity of the said time stamp. In such a case the condition defined in point 2)d) refers to the time stamp received by the Relying Party.

The time stamp discussed above may confirm solely the existence of a secure electronic signature, whose validity is being verified - it does not have to be directly associated with the signed document.

The Relying Party is obliged to prolong the time stamp validity discussed above, pursuant to the procedure defined by the Policy of the entity issuing the time stamp. The time stamp prolongation is not necessary if the signed electronic document has lost its validity and the Relying Party accepts the loss of the possibility to verify the electronic signature's validity.

The Relying Party may use a simplified procedure of secure electronic signature verification, without obtaining the abovementioned time stamp (or other evidence substituting the time stamp) and without meeting the condition discussed in point 2)d). Such a procedure may only be used however subject to the responsibility of the Relying Party. In such a case the Relying Party bears:

1) the risk associated with the fact that the qualified certificate or certification document (and thus also the qualified electronic signature) is not valid at the time of verification - in case of not using the CRL and ARL lists or using CRL and ARL lists not meeting the condition stipulated in point 2)d.

2) the risk associated with the fact that the qualified certificate or certification document (and thus also the qualified electronic signature) is not valid at the time of verification - even though it is not listed on the CRL or ARL list which the Relying Party uses - in the case of not meeting the condition defined in point 2)d above.

3) The risk associated with the fact that the qualified electronic signature, valid at the time of verification, may lose its verifiability at any time (and those lose evidential effect) - in case the Relying Party does not have a valid time stamp or other evidence substituting the time stamp.

Additional conditions of secure electronic signature verification

The Relying Party is obliged to use a secure device for signature verification (comprising software and possibly a technical component), meeting the requirements of the Ordinance, for the verification of qualified electronic signatures with the use of qualified certificates issued hereunder.

The secure device used by the Relying Party for the verification of secure electronic signatures must have the ability to correctly interpret the extensions of the qualified certificate defining

the highest limit value of a transaction, which may be confirmed in one operation using the said qualified certificate and the correct presentation of this value to the Relying Party.

The Relying Party may assume that the qualified electronic signature verified with the use of a qualified certificate issued hereunder is valid only if the secure signature verification device returns a verification result corresponding to 'positively verified' and the Highest Limit Transaction Value which may be confirmed once with the said qualified certificate - if it has been defined in the qualified certificate - does not exceed the value of the given transaction. In case the secure signature verification device returns a verification result corresponding to the meaning of 'incompletely verified, the Relying Party may repeat the attempts at verifying the signature at a later time, however until the possible obtaining of a 'positively verified' verification result, the Relying Party may not assume the signature to be valid.

1.5.5. Obligations concerning the protection of the integrity of the public key being a Point of Trust

In order to verify the validity of public key certificates issued hereunder, the Relying Party is obliged to use as Point of Trust the public key of the minister in charge of the economy (published under art.23 item 3 of the Act), the CUZ Sigillum public key or a public key of another qualified entity providing certification services concerning the issuing of certificates (within the meaning of the Act). The public key of an entity which does not publish a cryptographic digest (also called a fingerprint) of the key in a form allowing for controlling the integrity of the public key used by the Relying Party may not be used as a 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 must 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 will be obliged to confirm it, for example by comparing the fingerprint of the public key they have with a fingerprint published by the Minister of Digital Affairs, CUZ Sigillum or another entity providing certification services, as the case may be.

1.6. Scope of application of certificates

CUZ Sigillum issues certificates of signature verifying keys hereunder.

Certificates of signature verifying keys, issued by CUZ Sigillum pursuant to the Policy,

Are qualified certificates.

The number of certificates issued to a single Subject is unlimited.

1.7. Organisational structure

Centrum Usług Zaufania Sigillum [Sigillum Trust Services Centre] is an electronic certification centre with separated organisation, operating within the structures of PWPW SA

The PWPW SA Management Board have appointed a team within the CUZ Sigillum services, responsible for:

- Operating the system,
- Administering the system,
- Security of the system.

The CUZ Sigillum Manager is the person responsible for coordinating the works. The Manager is also a member of the PWPW SA Certification Policy Approval Council, appointed by the PWPW SA Management Board

1.8. Contact and legal registry data

Contact data:

Polska Wytwórnia Papierów Wartościowych S.A. [*Polish Security Printing Works PLC]*

Centrum Usług Zaufania Sigillum

00-222 Warszawa ul. Sanguszki 1,

e-mail: sigillum@pwpw.pl,

Phone: (+48) 22,464 79 79

www.sigillum.pl

Legal registry data:

NIP: 525-000-10-90

KRS: 0000062594

District Court for the City of Warsaw, 12th Commercial Department of the Polish Business Register

2. Publishing and repository

2.1. Repository

Acting within its obligations, CUZ Sigillum maintains a repository available for the recipients of certification services.

The repository is available in the Internet through the LDAP, OCSP protocols via http and http and WWW. In order to assure high service availability, CUZ Sigillum utilises two Internet connections from independent providers.

Public key certificates and CRL lists are made available with the LDAP protocol, the other documents listed in chapter 2.2 except the data from point d) with the http protocol.

Information about the certificate status will be available by the OCSP protocol on request of the Relying party. Certificate statuses on the current CRL list will be fully compliant with the statuses returned by the OCSP service, taking into account the time necessary for generating and publishing the CRL lists.

The repository is available 24 hours a day, on all days of the year. The possible time of unavailability of the repository may not exceed 2 hours per occurrence and the minimum monthly availability is 99% of time.

2.2. Publishing in the electronic version

The Policies are published electronically in the form of PDF format files at the CUZ Sigillum website.

The following documents are published electronically:

a) all versions of the Policy, with the time they were in power given (in PL and EN versions),
b) Extract of the Trust Service Policy (PKI disclosure statement),
c) Electronic signature certificates and electronic public key seal certificates of:
    a. the CUZ Sigillum authority, used for the verification of public key certificates and electronic seals issued hereunder,
    b. Electronic seal issued hereunder by PWPW CC,
    c. Electronic seal of the OCSP service,
    d. Electronic seal of the Time Stamp Authority,
    e. End users issued hereunder, if the Subject, whose data is included in the certificate or the electronic seal, subject to their consent.

d) an up to date list of revoked public key certificates and certification documents (CRL), issued hereunder,
e) agreement template / agreement templates on the provision of certification services (in PL and EN versions),
f) Terms and conditions of providing services (in PL and EN versions),
g) test certificate in the PKCS#12 format,
h) price list,

2.3. Frequency of publishing

The list of revoked certificates is generated and published at least every 24 hours, regardless of whether any certificates have been revoked or suspended.

In case a certificate is revoked, suspended or unsuspended in the period since the list was last generated, the CRL list is generated immediately after his has taken place. In the event of revoking a certificate upon the request of a Subject, Subscriber or other authorised persons, the CRL list is drafted and published immediately, however not later than within 1 hour of the reception of the request to revoke the certificate.

New versions of Policies, Rules and Regulations, Terms and Conditions of Providing the Service and PDS are published immediately after they are accepted.

In case the certificate Recipient and / or Subscriber agree to the certificate being published, the said certificate, issued hereunder, are published immediately, however not later than within 1 day of the moment of generating the certificate.

The seal of the authority, seals of the Time Stamp Authority, OCSP services - from time to time, immediately, when a new certificate or seal is issued.

2.4. Access control

The CUZ Sigillum repository is publicly available in a 'read only' mode, for the purpose of downloading the data or documents published therein.

Access control is effected, preventing the introduction of unauthorised changes of the status of certificates or other documents placed in the repository.

It is possible to limit access to specific services to individual users, if the CA is able to prove that the user is abusing the system.

3. Identification and authentication rules

Registration inspectors verify identity during a visit and authenticate other attributes of certificate applicants, prior to dispatching a certificate request to the CA. CUZ Sigillum prepares and supervises the use of documented verification and authentication procedures of clients applying for certificates.
An application filed in person at an RP concerning the administration of a certificate issued by the CA is authenticated by the Registration Inspector prior to it being realised.

Recipients of the certificates can be:

- issuing a qualified electronic signature certificate:
  - Subject is a natural person, Subscriber is a natural person,
  - Subject is a natural person who is a representative of a legal person , Subscriber is a representative of a legal person,
  - Subject is a natural person authorized by a representative of a legal person , Subscriber is a representative of a legal person,
  - Subject is a natural person authorized by a representative of a legal person , Subscriber is a natural person authorized by a representative of a legal person,

- issuing a qualified seal certificate:
  - Subject is a legal person, Subscriber is a representative of a legal person,
  - Subject is a legal person, Subscriber is a natural person authorized by a representative of a legal person.

3.1. Name giving principles

The Certificates issued at CUZ Sigillum is X.509v3 certificates, created in compliance with the requirements of RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate

Revocation List (CRL) Profile, taking into account the requirements of European standards ETSI EN 319 412-(1 to 5).

The construction of identity numbers of natural and legal persons is compliany with the syntax defined in the ETSI EN 319-412-1 standard.

3.1.1. Types of names

The identifier file of the 'subject' entity makes it possible to define an entity associated with the public key, placed in a file of a the public key of the certificate issued. The 'subject' file must contain a non-empty name identifying the entity. The contents of the Receiver file of the certificate is compliant with the instructions of the ITU-T X.520 Recommendation.

3.1.2. Necessity to use distinguished names

A certificate recipient may act under a pseudonym. In order to assure the possibility to unequivocally identify the certificate Recipient, at least the following attributes must be present in the identifier file of the 'subject' entity:

- For a natural person
    - countryName
    - Either: (givenName and surname) or pseudonym
    - commonName
    - serialName – may be present to assure the uniqueness of the Recipient's name in the domain of the certificate issuer

    Additionally, if a natural person acts in connection with a legal person, and in certificate is indicated a link with the Subscriber, then at least the following attributes may occur:
    - organizationIdentifier
    - organizationName

- For a legal person
    - countryName
    - organizationName
    - organizationIdentifier

- commonName

3.1.3. Rules of interpreting different forms of names

The certificate issuer is the final decision maker regarding the allowable DN contents, the Subject is entitled not to agree to the contents of the proposed DN. The meaning of individual attributes of names identifying certificate Recipients has been defined herein.

3.1.4. The use of pseudonyms in the name

A certificate recipient may act under a pseudonym. The issuer of certificates, in the registration process, assures unequivocal verification of the identity of the owner of a certificate containing a pseudonym. Data gathered during the registration process must be available at the certificate issuer for the period stipulated in the provisions of law.

3.1.5. Uniqueness of names

CUZ Sigillum assures the uniqueness of names in the certificate issuer domain, through the verification already at the level of users' registration, so that different recipients are not registered with the same range of data in the identifying name of the certificate (DN). A DN name once used may not be used by another certificate Recipient throughout the whole lifetime of the certificate issuer.

CUZ Sigillum settles disputes concerning the rights to use a pseudonym in the DN identifier contained in certificates issued in the certificate issuer domain for the benefit of a person, who already has a certificate including the said pseudonym issued by PCCE Sigillum.

3.1.6. Recognition, authentication and role of trademarks

CUZ Sigillum is not verifying rights of persons to use trademarks.

3.2. First registration

The notion of first registration covers the actions taken by CUZ Sigillum prior to generating a certificate for a Subject, who may be a natural or legal person, in case the Recipient does not have a valid qualified certificate issued hereunder.

Prior to issuing a certificate, CUZ Sigillum performs verification of the Subject's identity (if the Subscriber is a natural person), at least to the extent described in chapters 3.2.1 and 3.2.2, and of other attributes, which are gathered in the registration process.

In case the Subject is a natural person associated with a Subscriber, the Registration Inspector verifies the veracity of the legal person's data, the authorisation of the Subject associated with the legal person, as well as all other attributes necessary to obtain a confirmation of the association between the Subject and the legal person. If the legal person's data is to be included in the certificate attributes, both parties must confirm their consent thereto.

Notarial confirmation of the identity of the Subject and / or Subscriber is allowable. In such a case the Subject and / or Subscriber put their handwritten signature on the required documents in the presence of a notary public, which the notary public confirms and next the Subject and / or Subscriber file the thus prepared set of documents to the CUZ Sigillum.

At least two authorized representatives of CUZ Sigillum participates in the registration process.

The CA prepared and supervises the use of documented verification and authentication procedures of clients applying for certificates. The said procedures describe the scope of evidence gathered, not excessing the data necessary to confirm the veracity of data and attributes which are included in the certificate.

3.2.1. Authentication of legal persons

In order to identify and authenticate and organisation, which applies for a certificate, at least the following must be verified:

- Documents confirming the registration of the organisation in compliance with the national law.

- Documents confirming the authorisation to represent the organisation
- Documents confirming the relation between the Subscriber and the organisational unit, whose data is to appear in the certificate.

During the verification of the organization, it is also determined and verified:

- All representatives of a legal person, on the basis of the records of the founding documents
- Authorized representatives of the legal person on the basis of the authorization and the previously verified data of representatives of the legal person.

At least the following data must be verified: full name of the organisation and identity number.

3.2.2. Verification of natural persons' identity

In order to identify and authenticate a person applying for a certificate, the identity of the person is verified based on a document confirming identity. At least the following data must be verified: surname, name, date and place of birth and the national unique identity number, if it exists in a given country and the number and serial number of an identity document.

For the purpose of identity verification, a Natural Person must visit in person, at least once a Registration Point or a notary public.

The authentication process is performed by authorised persons based on the documents presented and comprises the verification of identity and, in case the physical person is associated with an organisation, the confirmation of power of attorney and / or authorisation, as well as verifying the scope thereof.

CUZ Sigillum prepared a detailed procedure describing the registration process. Documents including among others the said procedure are internal documents made available solely to a specific group of employees and partners performing the registration process.

3.2.3. Concluding the agreement

Prior to issuing a certificate, the Subject is obliged to sign an agreement on the provision of certification services with CUZ Sigillum. If a Subscriber participates in the process, it also is obliged to sign a relevant agreement. The agreement may be signed in a paper or electronic form, with the use of a qualified electronic signature. An authorised Registration Inspector signs the agreement on behalf of PWPW SA

Templates of the agreements with a Subject and Subscriber are placed in a publicly available repository at the CUZ Sigillum website.

3.3. Issuing another certificate

In the case of exchanging the key of a user, who is already registered and had a certificate qualified by CUZ Sigillum issued, filing the application without appearing in person is allowable, subject to the application for issuing a new certificate being signed with the use of a private key verified with a valid qualified certificate issued by CUZ Sigillum. The Registration Point operator must verify the validity of the available information concerning the applicant's identity and other attributes included in the certificate. If necessary, the Applicant must be requested to provide relevant documentation.

If the exchange of the key takes place due to the revoking of the qualified certificate, the identification and authentication process of the Applicant takes place in the same manner as during the first registration.

3.4. Certificate suspension and revoking

The administration of a certificate takes place electronically, over the phone or through a personal visit of Subject / representative of the Subscriber at a Registration Point, after authentication with the data agreed with the Subject / Subscriber representative, - if the said data has been defined. Providing correct authenticating data is sufficient for making an administrative order.

If the data used for the authentication of an order to administer of a certificate had not been defined at the stage of registration / issuing the certificate, or the person who intends to issue an order does not know the data, making an order is possible solely at a Registration Point

after the person is authenticated and their authority to make such administrative orders is verified.

The authentication of the person making an order and their authority takes place in accordance with the rules described in chapters 3.2.1 and 3.2.2.

3.5. Data collection

According to article 13 sections 1 and 2 of Regulation of the European Parliament and of the Council (EU) 2016/679 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 (Regulation 2016/679) CUZ Sigillum informs that:

1. 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.

2. CUZ Sigillum has appointed the Personal Data Inspector who can be reached by e-mail iod@pwpw.pl in any matter concerning the processing of Subscriber's personal data.

3. Subscriber's personal data shall be processed in order to conclude and perform the agreement under article 6 section 1 letter b) of Regulation 2016/679 according to which processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

4. Subscriber's personal data may be disclosed to:

1) entities that cooperate with PWPW S.A. and that perform specific tasks in connection with activity conducted by PWPW S.A., including to entities that process personal data for the benefit of PWPW S.A. under agreements on entrusting the processing of personal data,

2) entities authorized to receive personal data under the rules of law.

5. Subscriber's personal data shall not be disclosed to a third country or to any international organization.

6. The Subscriber shall be entitled to access Subscriber's data and to correct, delete, limit the processing of and transfer such data.

7. The Subscriber shall be entitled to lodge a complaint with a supervisory body, i.e. with the President of the Office for Personal Data Protection responsible for protection of personal data, if the Subscriber finds that the processing of Subscriber's personal data violates Regulation 2016/679.

8. Subscriber's personal data shall not be used for profiling or for making automatic decisions.

4. 9. Subscriber's personal data shall be processed during a period necessary to perform the task for which the data have been gathered.

4. Requirements concerning the services provided

The Certification Centre issues certificates based on a verified and authenticated certification request, after authenticating the Subject and, if there is one, the Subscriber and after signing the agreement on issuing the certificate. Moreover, in the process of registering the Subject and the Subscriber, the following should be presented or collected, among others:

- Terms and Conditions of the service, concerning the use of the certificate, which should be made available using durable means of communication
- An obligation of the Subject and the Subscriber to use a secure device
- Consent for the recording of data gathered in the registration process, future certificate administration orders and for transferring them to a third party company in case of a termination of the activity of the Certification Centre.
- Consent for publishing of the certificate in the Certification Centre repository

4.1. Certificate application

A natural person, a legal person, a natural or a natural or legal person managing hardware or a system, for which the certificate is to be issued may apply for a certificate

This Policy does not allow the issuing of certificates for Subject keys stored in a service allowing for remote signing.

4.2. Processing a certificate application

Each certification application which is to be realised by the Certification Centre, must originate from a trusted registration channel. Registration data is transferred in a secure manner after the authentication of the registration service provider is performed.

The registration point operator identifies the Recipients and Ordering Parties, verifies and authenticates the data and information provided and next initiates the certificate generating process.

4.3. Issuing a certificate

Upon receiving a certification order from a Registration Point, the certification authority verifies the correctness of the order and generates a certificate for the Subject based on the positively verified certification orders.

The generated certificate is recorder in the data base and transferred to the Registration Point for the purpose of placing it on a cryptographic card, on which the private key associated with the public key of the certificate is placed.

In case the certificate is generated based on an order delivered by a client, the certificate is transferred to the Subject or a person authorised by them.

The Subject and the Subscriber are notified of the fact of issuing the certificate if they are separate entities.

The Certification Centre registers in the log all significant events associated with issuing the certificate.

4.4. Certificate acceptance

After receiving the certificate the Subject and the Subscriber are obliged to immediately verify the contents thereof. In case they notice any errors whatsoever, in particular, associated with the Certificate Recipient's identity, they are obliged to immediately report the fact to CUZ Sigillum, for the purpose of revoking the certificate.

If the certificate contents are correct, the Subscriber confirms this fact by signing a respective statement. The certificate is published in the Certification Centre repository, subject to the Subject and / or Subscriber's consent.

The Certification Centre notifies the Subject and / or Subscriber and the Registration Point, from which the certification application has been sent, about the fact of issuing a certificate.

The control of the correctness of the certificate must be performed prior to the first use of the private key associated with the certificate. The Subject may face legal liability if they fail to meet this obligation and use a key associated with an incorrect qualified certificate.

4.5. Principles of using the certificate and pair of key

Certificates and private keys should be used by the Subject in compliance with the principles, particularly:

- The algorithm and length of the key should be compliant with those allowed hereby.
- The pair of keys must be used solely in compliance with the requirements communicated to the Subscriber and the Subject.
- The Subject must avoid unauthorised use of the private key.
- The private key must be used exclusively under the sole control of the Subject.
- The private key must be generated, recorded and used solely in a qualified digital signature or stamp device.
- CUZ Sigillum issues qualified signature and seal certificates only on cryptographic cards owned by him.
- CUZ Sigillum issues qualified seal certificate on HSMs for creating qualified seals using only QSCD devices
- In the case of an HSM device, being in the possession of the ordering party, intended for servicing qualified seal certificates, its prior verification by the CUZ Sigillum team is necessary.
- The Subject and / or Subscriber are obliged to inform the Certification Centre about cases of:
    - Loss, theft or suspected compromising of the private key
    - Loss of control over the private key due to the disclosure of activation data or for other reasons
    - Incorrect data in the certificate or of a change of data included in the certificate
- In the case of compromising the Subject's private key, cessation of the private key use for a purpose other than decrypting data.
- Cessation to use the private key after receiving information about the revoking of the Subject's certificate or the authority certificate
- If the private key is a signature certificate, the private key may be used solely for making a signature
- If the private key is a stamp certificate, the private key may be used solely for making a stamp

The Relying party is obliged to verify the public key certificate status, associated with the private key, which was used to sign or stamp an electronic document they receive, using one of the certificate status verifying methods described herein.

4.6. Certificate renewal

The certificate renewal process is performed the same way as issuing a new certificate.

4.7. Certificate renewal with key exchange

The certificate renewal process with key exchange is performed the same way as issuing a new certificate.

4.8. Certificate contents modification

The certificate contents modification process is performed the same way as issuing a new certificate.

4.9. Suspension, un-suspension and revoking of a certificate

A certificate must be suspended by the initiative of CUZ Sigillum, in case there is reasonable suspicion that there are grounds to suspend the certificate. In particular, the reception by CUZ Sigillum of information over the phone, electronically or through a personal visit of Subject / representative of the Subscriber at a Registration Point of a request to suspend the certificate, authenticated with the data agreed with the Subject / Subscriber, if such data has been established, must be sufficient grounds.

The revocation of a certificate suspension is initiated by CUZ Sigillum if they ascertain that the reasons for suspension no longer exist. In particular, if the suspension took place upon the reception by CUZ Sigillum of information from the Subject / representative of the Subscriber, the revocation of a certificate suspension may take place upon a telephone request, a request sent electronically by the Subject or a representative of the Subscriber, authenticated with the data agreed with the Subject or the representative of the Subscriber - if such data has been established, or through a personal visit of the Subject / representative of the Subscriber at the Registration Point.

Certificate Revoking takes place:

1) Upon the request of the Subject,
2) upon the request of the Subscriber or another person, whose data is included in the certificate,

3) upon the request of a third party, upon the obtaining of a confirmation from the Subject or Subscriber,
4) upon the request of a Supervisory Authority
5) on CUZ Sigillum initiative

The revoking of a certificate upon a Subject ’s request takes place on the basis of:
1) telephone notification, including an order of the Subject to revoke the certificate, authorised with the data agreed with the Subject - if such data has been agreed upon, or
2) the original copy of the document bearing a handwritten signature of the Subject, made in the presence of an authorised representative of CUZ Sigillum, after confirming the identity in compliance with the principles stipulated in chapter 5.1, or
3) an electronic document, bearing a valid qualified electronic signature made by the Subject

Revoking the certificate upon the request of the Subscriber or another person, whose data is included in the certificate, takes place on the basis of:
1) telephone notification, including an order of the Subscriber or another person, whose data is included in the certificate, authorised with the data agreed with the Subscriber or the said person - if such data has been agreed upon, or
2) the original copy of the document bearing a handwritten signature of the Representative of the Subscriber or another person, whose data is included in the certificate, made
in the presence of an authorised representative of CUZ Sigillum, after confirming the identity in compliance with the principles stipulated in chapter 5.1 and upon producing an original copy of the document authorising the person to represent the Subscriber or
the said other person, or
3) an electronic document bearing a valid, qualified electronic signature made by the representative of the Subscriber or another person, whose data is included in the certificate, Subject to CUZ Sigillum being able to confirm the authorisation of the said person to act on behalf of the ordering party or the said other person based on other documents (e.g. the agreement on the provision of certification services concluded with
the Subscriber)

The revoking of a certificate upon a request of a Third Party takes place based on:
1) original copy of a document, comprising information about the reason to make the order (e.g. a report of an incident indicating the possibility of an unlawful use of a private key), bearing a handwritten signature of the Third Person, made in the presence of an authorised

representative of CUZ Sigillum, after confirming the identity pursuant to the rules stipulated in chapter 5.1, or
2) original copy of a document, comprising information about the reason to make the order (e.g. a report of an incident indicating the possibility of an unlawful use of a private key), bearing a valid, qualified electronic signature made by the Third Party, after confirmation with the Certificate Administrator that the order made should be realised.

The revoking of a certificate upon a request of the Supervisory Authority takes place based on:
1) an original copy of the document bearing a handwritten signature of minister in charge of Informatisation (or an authorised representative of the minister), or
2) an electronic document bearing a valid, qualified signature of the Minister of Digital Affairs(or an authorised representative of the minister).

Immediate revoking of a qualified certificate by CUZ Sigillum takes place after the expiration of 7 days from the moment of suspending the certificate in case it is not possible to explain the reasons for suspending the qualified certificate. The original date of suspension is used as the date of revocation. In case the circumstances of suspending a qualified certificate are explained, CUZ Sigillum is be obliged to revoke the suspension.

If CUZ Sigillum concludes with the Subscriber or solely with the Certificate Recipient an agreement on the provision of certification services, requirements other than those described above may be stipulated therein, concerning the manner of authenticating the Certificate Recipient acting on behalf of the Subscriber or another person, whose data is included in the certificate upon certificate suspension or revoking of suspension.

Time from receiving certificate disposition to decision of publishing new status of the certificate is up to 24 hours.

The disposition of a certificate must be realised without undue delay, no later than within an hour of making the decision concerning the realisation of the disposition. The CRL list must be generated and published immediately.

The Certification Authority, applicant and administrators of the certificate must be informed both of the realisation of the disposition l and the refusal to realise the disposition, along with the grounds for the refusal.

The main and recommended to the parties method of verifying the status of a certificate which remains in its validity period indicated in the certificate is to use the online status verification service (OCSP). In case of a need to verify a certificate after it expires, it will be necessary to use the CRL lists, in which information about all revoked certificates issued by this Authority must be recorded.

The list of revoked certificates is generated and published at least every 12 hours, regardless of whether any certificates have been revoked or suspended.

A certificate, which has been revoked, may not be activated again.

CUZ Sigillum does not provide a certificate status verification method other than the OCSP service or certificate status verification on the CRL list.

Time on systems involved in the certificate disposition process is synchronized with UTC at least once a day.

4.10. Certificate Status Verification Services

CUZ Sigillum continuously provides the certificate status verification service free of charge. The status may be verified:

- In the OCSP service, available at the address indicated in the certificate
- In the CRL list, available at the address indicated in the certificate

4.11. Terminating the use of the service

The recipient of certification services may terminate the use of the certification service through revoking the certificate. At the moment the certificate expires, in case it is not renewed, the Recipient's use of the certification service terminates.

4.12. Keys storage

CUZ Sigillum does not store private keys of the Recipients and does not provide a deposit service for the Subjects' private keys.

4.13. Time stamping service

4.13.1. Scope of qualified TimeStamping service

Under the Policy CUZ Sigillum issues qualified time stamps for the Subscribers. The certified services Subscribers realised hereunder may be natural persons, legal persons and organisational 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 will be recognised. 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.

4.13.2. 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.

4.13.3. 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.

4.13.4. 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.

If the time stamp may not be issued, information about the reason to refuse the performance of the service must be sent instead.

5. Physical, organisational and personal security measures

In order to assure the maximum security level for the provided trusted services, CUZ Sigillum utilises among others physical, organisational and operational security measures. This chapter contains a description of the security measures utilised by CUZ Sigillum and the methods of controlling them.

All IT system resources used for the provision of trust services are placed in separate rooms, with limited and controlled access, protected against damage or unauthorised modifying. Moreover, CUZ Sigillum takes up activities aimed at:

- preventing the occurrence of an emergency situation, threatening the security of the data processed, particularly the data concerning vital interests of the Relying Party.
- minimising the effects of a possible disturbance of the system operation.

The whole CUZ Sigillum activity associated with the provision of trust services is monitored and controlled. This concerns both the activities of persons associated with the services provided and the operating of the whole IT system, working environment (energy, water, air conditioning) and access to rooms and the IT system.

CUZ Sigillum got certified in information security management in compliance with the ISO IEC 27001 standard for the purpose of its activity.

5.1. Physical security controls

The following systems associated with physical security are in place at CUZ Sigillum:

- Access control and intruder prevention;
- Fire protection and automatic fire extinction;
- Environment control - temperature, humidity and flooding;
- Emergency power supply.

Monitoring systems, associated with physical security, automatically notify the security service. If necessary, also the persons performing respective roles at the provision of trust services at CUZ Sigillum are also notified.

Systems monitoring the work of persons employed at the provision of trust services and systems monitoring the operating of IT systems are also used at CUZ Sigillum.

Alls monitoring systems work in a continuous manner, that is 24 hours a day.
Regular inspections and maintenance of all monitoring and support systems are performed for the purpose of assuring their uninterrupted operation, in compliance with legal requirements, service agreements and the policy adopted at PWPW SA.

5.1.1. Premises location and building

The organisational unit providing trusted certification services labelled CUZ Sigillum is located in the secure zone at the premises of PWPW SA. This concerns the primary and backup facilities. The facilities are located at a considerable distance from each other. The backup facility is capable of taking over the full functionality of the primary facility.

The buildings' structures meet the requirements of high security level zones. The room, at which trust services are provisioned and in which various ICT infrastructure elements used for the provisioning of these services are located is equipped with lock control. Moreover, CUZ Sigillum uses additional, separated zones in the form of cages and safes for the protection of resources associated with trust services.

The rooms in which trusted services are provided, are divided into the following zones:

- administration and operator rooms;
- IT system rooms.

Apart from the primary facility, CUZ Sigillum is in possession of a backup facility, which takes over the operation in case the operation of the primary facility is limited or impossible. Tests associated with switching operations to the backup facility and the correctness of its operation take place regularly, at scheduled times.
Access to rooms and the whole IT system of CUZ Sigillum for persons performing trusted roles in the system is assured 24 hours a day, for the purpose of assuring continuous trust services provisioning.

5.1.2. Physical access

Physical access control to CUZ Sigillum is assured by standard access protection procedures in place at the PWPW SA premises and through additional measures, assuring the possibility of access to CUZ Sigillum solely to authorised persons. All information assets brought into or out of the PWPW SA. Premises are also subject to control.

Physical access to CUZ Sigillum rooms is guarded by an internal security service and an access control system (ACS). Only authorised persons have physical access to the secure zones, where authentication takes place based on an electronic access card and a PIN number.

Persons, who are not authorised to enter CUZ Sigillum rooms may enter them solely under supervision of CUZ Sigillum staff.

5.1.3. Power supply and air-conditioning

CUZ Sigillum rooms in which technical elements are located, are equipped with emergency power supply systems and air conditioning systems.

In case of a breakdown of the primary power supply system, power supply is automatically switched to emergency power supply - an electricity generator or UPS.

The air conditioning system assures stable temperature in all rooms, which are monitored in terms of temperature and humidity. Exceeding the assumed threshold values causes automatic notification to CUZ Sigillum staff.

5.1.4. Water supply

There is no water supply within the critical rooms of CUZ Sigillum.

The CUZ Sigillum rooms are protected and monitored against flooding with water. Server rooms in the primary and backup facilities are monitored with flooding sensors. The appearance of water in these rooms causes automatic notification to the CUZ Sigillum staff and security services.

5.1.5. Fire prevention

The CUZ Sigillum rooms are protected and monitored against the occurrence of fire, in compliance with the mandatory provisions of law. An automatic fire extinguishing system is installed in the server rooms of the primary and backup facilities.

Hydrants are located next to the rooms where trust services are provisioned and the rooms are equipped with fire extinguishers allowing for extinguishing fires of electronic devices.

The CUZ Sigillum staff are regularly trained in the area of fire protection and there are regular staff fire drills at PWPW SA.

5.1.6. Usage of data storage devices

Data storage devices kept by CUZ Sigillum are protected against the impact of environment factors, such as temperature, humidity and magnetic field. Storage devices of data critical for the provisioning of trust services are kept in fire-resistant safes in the rooms of the primary facility. Copies of the said data storage devices are kept in the backup facility rooms, also in fire-resistant safes.

Only authorised data storage devices may be used in the ICT system, the use of data storage devices is allowed solely by authorised users.

All data storage devices, on which information associated with the provisioned trust services are recorded, are Subject to being recorder and controlled.

Access to these data storage devices is limited to authorised persons.

5.1.7. Disposal of data storage devices

Paper-based documents and data storage devices containing elements subject to physical protection are destroyed after the storage period. The destruction takes place under supervision.

Physical destruction takes place in compliance with the rules adopted at PWPW SA and is confirmed with a relevant destruction record.

After the data storage devices, both paper and electronic, are destroyed, there is no possibility to recover the information previously recorder on them.

5.1.8. Storage of backup copies outside the CUZ Sigillum premises

CUZ Sigillum developed and implemented procedures assuring the storage of two identical sets of backup and archive copies: one at the primary and the other one at the backup facility. All information associated with the trust services provided by CUZ Sigillum, required by the Act and Ordinance, is Subject to copying and storage.
Backup copies of cryptographic keys, PIN numbers, passwords, and the like are stored in special zones (outside the CUZ Sigillum premises) with limited access and protected against the results of various disasters.

5.2. Organisational security controls

Apart from physical security measures, CUZ Sigillum also utilises organisational safeguards allowing for maintaining the highest possible security level and assuring a high level of the trust services provided.

Pursuant to the Ordinance, the persons employed at CUZ Sigillum are allocated relevant roles in the provisioning of trust services. An employee's roles and scope of responsibility is registered in the Privileges and Responsibilities Sheet or in the Agreement on Providing of Services.

5.2.1. Trusted roles

In order to distribute the responsibility of persons performing the trusted roles at CUZ Sigillum, pursuant to the executive regulations associated with the Act, the following personnel roles are defined:

1. CUZ Sigillum Manager is responsible for the correct operating of CUZ Sigillum, defines the directions of its development and implements the Certification Policy (SM);
2. The persons supervising the implementation and use of all procedures of secure operation of IT systems used for the provisioning of trust services, henceforth referred to as 'Security Inspectors' (SI);

3. The persons who confirm the Subject's identity and approve the prepared certification applications, henceforth referred to as 'Registration Officers' (RO);
4. The persons who perform certificate revoking at the request of an authorised entity, henceforth referred to as 'Revoking Inspectors' (Rev.I);
5. Persons, who install, configure and manage the system and IT network, henceforth referred to as 'System Administrators' (SA);
6. Persons, who perform continuous IT system operations, including the creation of backup copies, henceforth referred to as 'System Operators' (SO);
7. Persons, who analyse the logs of events recorded in the IT systems used for the provisioning of trust services, henceforth referred to as 'Audit Inspector' (AI).

The persons who perform trusted roles must meet the requirements stipulated in the Act.

5.2.2. Number of persons required for a task

CUZ Sigillum defines in its security procedures the numbers of persons necessary to perform individual tasks. In many cases the tasks performed by the operators (SO) or administrators (SA) are supervised by the Security Inspectors (SI).

The processes of generating keys used by CUZ Sigillum for signing: certificates, OCSP responses, CRL lists and time stamps are subject to particular supervision. The Security Inspector, System Administrator, System Operator, Audit Inspector and observers, among others, take part at generating the keys.

Moreover, CUZ Sigillum uses the principle of shared access to numerous operations or resources of the system working for the purpose of trust services provisioning. This concerns primarily administrative tasks, verifying event logs and making backup copies.

5.2.3. Authentication and authorisation of each role

Each person employed at the provisioning of trusted services, depending on the performed role, has precisely defined privileges concerning the access to:

- Rooms, in which trusted services are provisioned or in which the hardware or documentation used for the provisioning of such services are located;
- The IT system used at CUZ Sigillum;
- Operations performed on the software and data.

Each of the persons employed at the provisioning of trust services has an individual account, which allows for strict accountability of the person and with which strictly defined privileges are granted. Logging in to accounts allowing for direct certificate issuing, requires the use of a certificate stored on a cryptographic card secured with a PIN.

The reviewing of accounts and privileges at CUZ Sigillum takes place in compliance with the rules adopted at PWPW SA. Unused accounts are immediately blocked and the privileges taken away.

Software supervising the work of individual persons is also installed at CUZ Sigillum. Access to this software and the information it records is granted solely to the persons, for whom it results from the role performed in the trusted services provisioning system.

The rule of 'minimum privileges' is used at CUZ Sigillum, i.e. Persons with access to rooms or the IT system have only the privileges needed for proper performance of their work. The duties and scopes of responsibility are divided into individual organisational units at PWPW SA.

5.2.4. Separation of duties for each of the roles.

The functions described in points 1 and 3 as well as in points 1 and 4 of Chapter 5.2.1 may not be connected. The function referred to in point 5 may not be connected with any of the other functions listed in Chapter 5.2.1.

5.3. Personnel management

CUZ Sigillum employs workers with qualifications required for the provisioning of trust services and meeting the requirements stipulated in the Act. The employment takes place based on a labour contract or a civil-law contract, which defines the role the person will perform in the trust services provisioning system. This way both information security and a high level of the trust services provisioning are assured.

5.3.1. Requirements associated with qualification, experience and verification of the personnel

There are procedures for employment and selection of personnel in place at PWPW SA, taking into account the preparation, qualifications, professional experience and requirements for the work at a given position. Moreover, methods of verifying a person employed for a position associated with the performed trusted role are used.

Each person employed at PWPW SA, regardless of the form of employment, has a strictly defined range of duties and privileges associated with the role they perform in the system. The range must be signed with a handwritten signature by the employed person.

The duties and privileges a given employee has determine the extent of the person's access to rooms and the IT system of CUZ Sigillum.

Prior to starting to perform their duties associated with the provisioning of trust services, the employed person must undergo the trainings associated with the performed duties as required by the law, in particular, concerning the Act, personal data protection and fire prevention.

Employees with managerial positions have experience or training regarding the provided trust service. These persons demonstrate the knowledge of security procedures for the staff reporting to them, they are responsible for security of information and risk assessment and they have sufficient knowledge to perform management functions.

Each employee supposed to perform a trusted role at CUZ Sigillum, must be accepted by the managers of the PWPW SA organisational unit in charge of trust services provisioning.

5.3.2. Employee work preparation control

Control of the preparation for work at a given position associated with the performance of a trusted role is performed for each new employee, prior to allowing them to perform duties and in the course of employment. CUZ Sigillum verifies the qualifications and professional experience and requires a statement concerning a clean criminal record.

Special emphasis is placed on the knowledge of issues associated with the certificates technology and provisioning of services concerning the electronic signature and time stamp. The persons employed at CUZ Sigillum are also required to have the knowledge and skills associated with the operating of hardware and software used for electronic, automatic processing of data in networks and ICT systems.

The persons employed at the provisioning of trust services must sign relevant statements associated with non-disclosure of confidential information prior to starting their work.

Employees do not gain access to performing trusted functions until all necessary controls are finished.

5.3.3. Training Requirements

All CUZ Sigillum employees performing trusted roles in its structure, are trained in particular in the area of:

1. Automatic data processing in networks and IT systems;
2. Security mechanisms of networks and IT systems;
3. Cryptography, electronic signatures and public key infrastructure;
4. Hardware and software used for electronic data processing;
5. Acts and ordinances regulating the operations of CUZ Sigillum;
6. Policies, rules and regulations and operational procedures used at CUZ Sigillum.

The completed trainings should be confirmed with relevant certificates or diplomas.

5.3.4. Training repetition requirements

The director of the organisational unit in charge of trust services provisioning must determine the training plan, assuring the maintenance by the CUZ Sigillum personnel of a high level of knowledge. The plan covers both repeated trainings, those supplementing knowledge and gaining new skills.

5.3.5. Frequency and manner of position turnover

CUZ Sigillum does not implement planned turnover of positions of its employees.

5.3.6. Sanctions for unauthorised actions

Due to the fact that all actions performed upon the provision of trust services are controlled and documented, it is possible to detect and prove the possible unauthorised actions of the persons employed at CUZ Sigillum.

CUZ Sigillum may impose penalties on its employees penalties under the Work Rules and Regulations at PWPW SA, the Labour Code or the Act for unauthorised actions.

In case members of the CUZ Sigillum staff perform unauthorised actions, they must also face sanctions stipulated in other provision, including among others the Act on Fighting Unfair Competition, Act on the Protection of Personal Data and the Criminal Code.

PWPW SA may also pursue damages for the losses incurred in civil law court proceedings.

5.3.7. Requirements for independent contractors

In case of performing any works for CUZ Sigillum by independent contractors, who are not CUZ Sigillum employees, the following are required:

(1) Concluding a civil-law contract precisely defining:
   (a) The scope of works performed;
   (b) Time and place of performing the works;
   (c) Conditions for the acceptance of the works performed (date of the acceptance, qualitative and quantitative criteria);
   (d) Sanctions for improper performance or non-performance of the conditions of the contract;
   (e) the possibility of audit and monitoring the contractor's personnel;
   (f) Damages for damage caused by the actions of the contractor's staff;
   (g) Other provisions associated with information security or the quality of trust services provided.
(2) Obligations of the contractor to meet the security regulations in place at CUZ Sigillum.
(3) Signing by the independent contractor of a representation concerning keeping confidential all information associated with the works performed and a representation that the contractor recognises the information about punitive sanctions attached to breaching the confidentiality clause. If there are more persons working for the independent contractor, the said representations should be signed by each of the said persons.

If needed, CUZ Sigillum must communicate to the independent contractor the principles of access to information and the allowed use of information. The contractor should also be acquainted with the policies, procedures or documents associated with information security and the trust services provided in place at CUZ Sigillum.

The acceptance of works performed by an independent contractor should be Subject to the condition of signing without reservations by the management of CUZ Sigillum of the protocol of performance and acceptance.

5.3.8. Documentation supplied to personnel

CUZ Sigillum personnel has continuous and direct access to:

1. Any and all documentation, pertaining to CUZ Sigillum, of hardware and software used for the provisioning of services labelled CUZ Sigillum;
2. Policies, Rules and Regulations;
3. Operational procedures and procedures assuring operations continuity in force at CUZ Sigillum;
4. Templates of agreements, applications and the like used for provisioning of services.

The access includes both current and archival documentation.

5.4. Event control procedures

All events, significant from the point of view of the security of the trust services provided, are logged, stored and audited by CUZ Sigillum. Events Subject to the logging procedure originate both from the individual components of the system itself and the actions performed by CUZ Sigillum employees.

Event logs are kept and stored, in particular for the purpose of:

1. Assuring service provisioning continuity;
2. Making users and employees accountable for their actions;
3. Controlling workers with regards to their actions;
4. Providing evidence in court proceedings. The information is stored in electronic form.

The following procedures concerning the security of the conducted activity have been implemented at CUZ Sigillum:

1. Monitoring the IT system;
2. Operating the event logs;
3. Proceeding in case of an information security infringement.

CUZ Sigillum assures the confidentiality of information gathered in the logs through the use of physical, organisational and procedural security measures.

After the required period of storage, the event logs are destroyed under the supervision of a commission, in compliance with procedures adopted at PWPW SA

5.4.1. Types of events logged

All important elements of CUZ Sigillum infrastructure keep audit logs for the purpose of assuring accountability of the operators' and administrators' actions, registering errors and other events concerning information security in order to support the processes of event and security incident management, configuration, capacity and detection of events which may have an influence on systems' availability. Access to event logs is Subject to access control Logs and session records are Subject to protection.

Event logs records cover at least:

1. all events associated with registration, including filing applications concerning the obtaining of a certificate, updating keys or certificate renewal;
2. A demand to provide certification services which are typically made available by the system or services not provided by the system and information concerning the provision or non-provision of a service and the reason of non-performance.
3. significant events associated with changes in the system environment, including in the keys and qualified certificates management subsystem, in particular the establishing of accounts and type of privileges granted;
4. all events associated with time stamps issuing;
5. events associated with time stamp authority key and certificate life cycle;
6. new software installation or updated;
7. Initiating and breaking event logging functions;
8. Changes to the configuration of the event logging functions, including in particular any modification or synchronization of the system time;
9. Time of making backup copies;
10. Time of archiving event logs;
11. Shutting down, opening and restarting after shutting the system down.
12. Unexpected events in software and hardware operating;
13. Negative test results;
14. events concerning network communication;
15. All reports concerning the revoking of a qualified certificate and all messages associated therewith, in particular the sent and received communications about calls sent in the relation between the qualified certificate holder with the qualified entity providing certification services.

All records in event logs are time-stamped with a precision of one second. Time used for logging events in the register is synchronized with the UTC at least once a day. Events are logged continuously.

At least the following are logged for individual events:

1. Event type;
2. Its identifier;
3. the date and time of occurrence;
4. Information associated with the reason of occurrence;
5. Defining the effects of the occurrence of the event.

Entries associated with logging events are archived.

5.4.2. Frequency of event logs reviews

Events recorded in logs are revived by operators (SO) together with auditors (SA) or inspectors (SI) at least once a day, except for Saturdays, Sundays and bank holidays. The fact of performing the review is logged in the events' review logs.

If necessary, e.g. the occurrence of an incident, more frequent overviewing of the event logs is required. Event logs overview is focused mainly on identifying adverse events in terms of the security or quality of the provisioned trust services. Results of the event log reviews are recorded in the 'Logs Review Registers'.

Events from CUZ Sigillum infrastructure elements' logs are sent to a central system, where rules of correlating events from various devices have been defined. Anomalies in system operating generate notifications to the personnel responsible for system monitoring.

In case of noticing events, which are significant from the point of view of the services provided, the Security Inspector together with the System Operator or Administrator take action to explain the event. If the noticed event is associated with system security or threatens the continuance of the provided services - additionally they draft a written 'Post Incident Report', in compliance with the rules in place at PWPW SA

The Audit Inspector (AI) verifies the completeness of records in the 'Logs Review Registers' after the end of the month. The results of this verification are documented in the form of a 'Security Report'.

Authorised persons perform a review of the event log particularly in terms of attempts at:

1. Preventing or interrupting the CUZ Sigillum activity regarding the provisioning of trust services;
2. Unauthorised access to the ICT system;
3. Unauthorised access to the database;
4. Unauthorised access to CUZ Sigillum rooms.

5.4.3. Period of event logs storage

The event logs are stored in the place where they originate, for a period of at least two years and they are available on-line. After the said period the event logs are archived and made available in the off-line mode.

The archived events are stored for a period of a minimum Of 3 years of the date of making an entry. After this period the event logs are destroyed in compliance with the procedures in place at CUZ Sigillum.

5.4.4. Prevention of the event logs

Event logs, like other information associated with the security of the services provided, are Subject to protection on the same level as all other information associated with the CUZ Sigillum activity.

For the purpose of protecting the event log against modification, deletion, loss of integrity or other such events, a rule has been adopted at CUZ Sigillum, that none of the persons listed in Chapter 5.2.1 hereof may have access to the event log on their own. Thus the administrators or operators have access to the event logs solely in the presence of one of the two persons: inspector or auditor.

Access to the event logs is possible solely in the reading mode.

5.4.5. Procedures of creating backup copies of event logs

Security procedures concerning the handling of event logs require copying the records according to the adopted schedule - at least once a month. If required by the situation, e.g. Switching off a server, software or database update, event logs are downloaded and copied prior to performing the required operations.

At least two of the persons listed in Chapter 5.2.1 hereof are present upon the creation of backup copies.

5.4.6. Event logging system (internal and external)

Event logs from the ICT system are created automatically. They originate from the following sources: the operating system, databases and the software used.
Additionally logs of subsystem operation and event logs review records are kept in a paper-based form. Entries in these documents are made by the proper, authorised persons.
All records associated with the registers kept are stored in two counterparts. One counterpart is located in the primary facility, in which the trust services are provided, the other one outside the primary facility.

5.4.7. Notification of event-causing subject

CUZ Sigillum has implemented and uses a system of monitoring and notifying of adverse events, which have influence on the security of the trust services provided. The system is operated 24 hours a day by the System Operators. If necessary, depending on the degree of criticality, also System Administrators and Security Inspectors are notified.

The task of the notified persons comprises getting acquainted with the situation in detail, analysing it and taking the right decisions aimed at preventing the results of adverse events.

5.4.8. Vulnerability assessment

CUZ Sigillum has a certificate compliant with the ISO ICE 27001 standard for issuing and handling certificates.

According to the said standard's requirements, CUZ Sigillum performed the qualification of all its assets used for the provisioning of trust services. Furthermore, in accordance with the requirements thereof, an analysis of the assets' vulnerability to threats has been performed and the risks associated with them have been assessed. A risk management plan has been implemented and accepted by the CUZ Sigillum management.

PWPW SA maintains: an internal audit unit, whose responsibility is among others to assess the compliance of CUZ Sigillum with the requirements of the ISO IEC 27001 standard, as well as an

ICT security unit, whose responsibility is among others to assess and analyse vulnerability and reactions to incidents.

5.4.9. Risk management

Risk management is a regular and continuous process of threat identification and minimising vulnerability and the effects of the occurrence of those threats. Risk management is intended to support decision making processes at PWPW SA, with the purpose of selecting the measures aimed at diagnosing causes, limiting and effective reaction to the results of breaches in the area of resources and processes realised at CUZ Sigillum.

Risk assessment is performed once a year or after introducing significant changes in the process (including in the ICT infrastructure used in it).

Risk assessment results from the context of the organisation and business needs of the process of issuing and processing certificates, which means, that risks identified during the assessment must be associated with the business goals of the process.

The list of potential threats is drafted based on:

- Information gathered from an earlier risk analysis session,
- Internal audit results.
- External audit results,
- Reports concerning the reported security incidents,
- Organisational changes (e.g. organisational structure changes, new services),
- Technical changes (e.g. new ICT systems, new functional scope),
- New security threats.

Detailed methodology of performing the risk analysis and the manner of handling the risk are described in PWPW SA internal procedures.

5.5. Archiving logs

All events, significant from the point of view of providing trust services and those required by the law, are archived and copied at CUZ Sigillum in two counterparts on external data storage devices.

CUZ Sigillum has developed and implemented archive procedures, procedures of storage and access to archive data.

The events archive is created automatically, whereas information concerning the recording of events and the review of correctness of the copy made is maintained with the so-called reports in the paper-based form.

The audit inspector is obliged to review the records associated with the archiving process at least once a month. The fact of performing such a review is registered in the Event Log Review Register'.

5.5.1. Types of archived records

CUZ Sigillum maintains an archive comprising the records associated with:

- 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.

Records associated with the employees' activity and events taking place in the ICT system are made automatically.

5.5.2. Retention period for archive

The records of the event logs and employees' activity logs are kept and archived for a period of at least 3 years. Information listed in point 5.5.1 is 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.

5.5.3. Protection of the archive

Data storage devices containing the archived data are protected by means of physical and electronic access control methods. They are also protected against the impact of environment factors, such as temperature, humidity and magnetic field.

The archives' integrity is assured with the use of electronic signatures made by means of infrastructure keys.

Only the persons associated with performing trust functions in the CUZ Sigillum system have access to the archives.

Access to the archived information is possible solely in the reading mode.

5.5.4. Procedures of creating backup copies of the archive

CUZ Sigillum has developed and implemented procedures of creating archival resources and managing them. In particular, the said procedures concerns:

1. Resources' classification
2. Information processing;
3. Assuring security for the archives.

5.5.5. Requirements for dating records

There are no defined requirements concerning the dating of the archive records. This does not prejudice the obligation to record the date of each event, in the manner stipulated in Chapter 5.5.1.

5.5.6. Archive gathering system (internal and external)

Archival copies are made by the System Operators and recorded on external write once data storage devices (WORM) in two counterparts.

All records associated with the archives kept are stored in two counterparts. One counterpart is located in the primary facility, in which the trust services are provided, the other one outside the primary facility.

5.5.7. Procedures of access and verification of the archived information

In order to verify the correctness of archiving information on external data storage devices, correctness of the records made is performed at CUZ Sigillum. The operation is performed daily by a System Operator under the supervision of a Security Inspector on randomly selected objects. Information about the correctness of making a record and its readout is logged in the relevant registers.

Selected information from the archive may be made available to the proper bodies solely based on art. 15 paragraph 4 of the Act.

5.6. Key changeover

The key changeover at CUZ Sigillum is not performed automatically. The keys expire in compliance with the expiry date of the certification document issued for CUZ Sigillum by the minister in charge of informatisation.

The keys are exchanged sufficiently in advance of the expiry date, so that the expiry date of none of the certificates issued with the use of these keys exceeds the expiry date of the keys. It must also be necessary to obtain a new certification document from the Minister of Digital Affairs or an entity appointed by the Minister.

After the certification document containing the old CUZ Sigillum public key expires, the private key associated with it is destroyed by means of the relevant procedures adopted at CUZ Sigillum.

After the exchange of keys, CUZ Sigillum uses for the provisioning of services solely the new private key.

5.7. Security breach of the authority keys and disaster recovery

CUZ Sigillum has developed and implemented a detailed operational continuity procedure covering the situation of compromising the CUZ Sigillum private key, hardware, software and communication lines breakdown and natural disasters such as fire and flood. Also, the documentation describing the basic configuration of hardware, operating systems, software applications, anti-virus software and specific PKI software has been developed.

CUZ Sigillum also has relevant backup and archive copy handling procedures and procedures for data storage outside of its premises.

CUZ Sigillum also performs regular training of its personnel concerning the contingency procedures for situations with a negative impact on its activity and tests of switching to the backup facility.

Regardless of the procedures associated with maintaining operational continuity, also procedures for notifying supervisory authorities and Subjects of such events are prepared at CUZ Sigillum.

All events which may contribute to the occurrence of an incident are continuously monitored and controlled.

5.7.1. Incident handling procedures

The incident handling procedure defines the principles of handling incidents associated with information security. Incident handling is aimed at taking up the necessary actions, which will remove or minimise the results of the incident taking place or will reinstate the condition from before the incident.

Potential threats, which may have a significant impact on the continuity of the trust services provided, have been identified and catalogued at CUZ Sigillum. These include, inter alia:

- The authority private keys compromising;
- Physical or logical damage to any element of the IT system used for trust services provisioning;
- Loss of external network services;
- Loss of computing power, software or data;
- Loss of power supply;
- Detection of the time that would be indicated in a time-stamp drifts or jumps over 1 second;
- Disasters resulting from natural reasons.

An operational continuity for the services provided has been developed at CUZ Sigillum for the purpose of handling threats, incidents and disasters. Procedures have been prepared, allowing for the operation of a part or whole of the system at the backup facility, procedures associated with archiving and copying the system and procedures regarding system recovery after events.

Incident handling procedures cover also the manner of reporting them. A special telephone line and an internal intranet site have been established for the purpose of reporting incidents.

In case of discovering a security breach or loss of integrity, which has significant impact on the service provided or the processed personal data, CUZ Sigillum will, without undue delay, not later than 24 hours after receiving information about the incident's occurrence, inform a supervisory authority of this fact and, in relevant cases, other proper entities.

5.7.2. Breakdown of computing power, software or data resources;

CUZ Sigillum has developed and implemented a document describing the basic configuration and procedures of making backup and archive copies. The activities in case of the occurrence of computing resources or software are defined by the procedures under the service agreements concluded by CUZ Sigillum.

For the purpose of minimising the breakdown results of its ICT resources, CUZ Sigillum has taken the following actions:

- Developing and implementing a procedure of notifying of incidents both the supervisory bodies and Subjects;
- It has a plan of operating in emergency situations and system recovery after a disaster procedures;
- It regularly creates copies (in two counterparts) of the whole system, which include system and application software as well as the data;
- It uses the number of keys adjusted to its needs, the keys are stored in various places;
- It regularly tests recovery plans of its operations and tests the possibility to recover it from backup and archive copies;
- All changes in the system, both concerning hardware and software, are documented and controlled;
- It has signed proper hardware and software maintenance agreements with their vendors or producers;
- It regularly and periodically performs auxiliary systems' reviews (power supply, air conditioning, etc.).

5.7.3. Procedures in case of compromising private keys

In case of compromising the private keys of the authorities providing trust services, CUZ Sigillum must initiate the relevant procedures, which include inter alia:

- Applying to for a new certification document to the national certification authority;
- Generating new private keys of the authority;
- immediately notifying all Subjects of the event that took place;
- Revoking the previous certification documents, associated with the compromised key;
- All certificates and certification documents, which are on the certification path associated with the compromised authority must be revoked;
- Ne certificates and certification documents must be generated and sent to the Subject at the expense of CUZ Sigillum to replace the revoked ones.

5.7.4. Operational continuity maintenance

CUZ Sigillum has developed and implemented:

- procedures for Business Continuity Plans
- procedures to generate backup and archive copiers and the rules of storage of the said copies outside the CUZ Sigillum premises.

CUS Sigillum has organised and maintains a backup facility, capable of taking over the functions of the primary facility in emergency situations. Private keys of authorities and services are imported to cryptographic devices in the primary and backup facilities and associated with the certificate of a given service or authority.

Both the possibility to recover information from backup copies and the operating of the backup facility are regularly tested.

After each recovery of the system after a disaster to the normal condition, the Security Inspector, together with the System Administrator must:

- Verify the completeness and correctness of system operation;
- Analyse the reasons and results of the disaster that happened;
- Inform the supervisory authority and Subjects about the disaster results;
- Verify and update the risk analysis associated with the provisioning of trust services;
- Review and update the relevant policies and procedures from the point of view of assuring information security in the future in case similar events occur.

5.7.5. Procedures in case of algorithms compromising

In case of compromising the algorithms used by CUZ Sigillum, relevant procedures must be initiated, comprising inter alia:

- immediately notifying all Subjects of the event that took place;
- All certificates and certification documents using the compromised algorithm are revoked.

5.8. Termination of CUZ Sigillum or Registration Points activity

If it turns out to be necessary to terminate the activity of CUZ Sigillum or one of trust services, it should be assured that the effects of this fact for the recipients of certification services be minimised to the extent to which it will be possible.

In order to minimise the effects of terminating the providing of trust services, CUZ Sigillum has developed and implemented an operational continuity plan, taking into account the situation in which CUZ Sigillum is removed from the register of qualified entities providing certification services. The plan includes the obligation to cease concluding agreements on the provision of certification services upon the reception of a decision to remove CUZ Sigillum from the register, within the scope of the Policy, which the decision will concern. The plan involves also the obligation to notify in advance the relevant supervisory authorities and Subjects about the termination of activity, so that they make take relevant action associated with the certificates held.

5.8.1. Actions to be performed by CUZ Sigillum

In case of a planned termination of the activity of CUZ Sigillum, it must immediately inform of this fact the Minister of Digital Affairs and the Registration Points, at least three months in advance, along with the communication of information about a possible successor that could take over the providing of services to the Subjects.

CUZ Sigillum must notify all Subjects associated with the authority terminating its activity about the intention to terminate it. Whereas those, who hold a valid certificate issued by the authority terminating its authority, at least three months in advance. In such a case the Registration Points may offer to Subjects support in applying for a certificate to be issued to the successor of CUZ Sigillum. Certification services of the same or another certification centre should be recommended to the Subjects, as soon as possible.

In case of an emergency termination of the CUZ Sigillum Activity, for example as a result of compromising the private key, CUZ Sigillum must inform of this immediately, no later than within 7 days of the date of the occurrence of the said situation, the minister in charge of

informatization. In such a case CUZ Sigillum must provide to the subordinate Registration Points the necessary information.

All certificates issued by CUZ Sigillum, after the certification document issued by the NCCert is revoked, must also be revoked. CUZ Sigillum must hand over the documents and data stipulated in art. 17 paragraph 1 of the Act to the minister in charge of informatisation, who stores the data until the end of the period stipulated in art. 17 paragraph 2 of the Act.

CUZ Sigillum must, to the extent possible, take all effort to make the termination of activity regarding the providing of services cause the minimum possible losses in the Subjects' activity. If possible, CUZ Sigillum must reimburse the costs of the certificate issued to the Subject, in the amount proportional to the period remaining to the expiry date of the issued certificate.

Pursuant to the requirements of the Act, CUZ Sigillum has a civil liability insurance for the event of causing damage to the recipients of trusted services.

5.8.2. Subjects' keys and certificates

In case CUZ Sigillum terminates its activity:

1. All certificates issued by CUZ Sigillum must expire;
2. Timestamp service certificate must be revoked;
3. Pursuant to mandatory provisions of law, it can't be possible to automatically 'transfer' Subjects to another Electronic Certification Centre.

CUZ Sigillum has developed and implemented an operational continuity plan, taking into account the situation in which CUZ Sigillum is removed from the register of qualified entities providing certification services.

The plan includes the obligation to cease concluding agreements on the provision of certification services upon the reception of a decision to remove CUZ Sigillum from the register, regarding the services, which the decision must concern.

Under the Act, after terminating the activity, data archives associated with the provisioning of certification services must be transferred to the Supervisor Body.

6. Technical security controls

6.1. Generating and installing key pairs

The security of generating and installing key pair is assured by operational procedures used at CUZ Sigillum.

6.1.1. Generating key pairs

Key pairs of all CUZ Sigillum authorities are generated in compliance with the documented generating procedure, assuring the integrity and confidentiality of keys. The generating of a pair of keys takes place at the CUZ Sigillum premises in a physically safe environment, in the presence of at least two authorised persons performing trusted roles, whereas at least one of them must be a Security Officer. A report of the operations performed in generating the keys is prepared and signed by all participants of the keys generating procedure. The Security Inspector certifies with their signature on the aforementioned, that the key generating process took place in compliance with the documented procedure of confidentiality and integrity of keys.
After keys generation, CUZ Sigillum applying for certificate of trusted service to Minister of Digital Affairs . After receiving the certificate, chain of trust and certificate are validated by CUZ Sigillum.

The pairs of keys of Registration Inspectors are generated under the supervision of a Security Inspector.

A pair of subject keys intended for cryptographic cards may be generated only by the Registration Officer during the registration process, in the presence of the Subject, on the QSCD device provided by CUZ Sigillum.

In the case of an HSM device intended for handling a qualified seal certificate for which a pair of keys is generated by the subject, the generating process must take place in the presence of representatives of CUZ Sigillum after verifying by them that the device on which the keys were generated meets the requirements of art. 30 para. 3 and / or art. 39 par. 2 of Regulation (EU) No 910/2014 of the European Parliament and of the Council. Key generation process

confirmed by a protocol signed by both parties. The report is drawn up in two identical copies, one for each party. CUZ Sigillum stores its copy in the archive.

Parameters of the generated keys must meet the requirements imposed in the ETSI TS 119 312 standard: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites" or in national provisions of law.

CUZ Sigillum assures that all the Subjects' private keys, whose public keys are certified in compliance herewith, are stored in devices which meet the requirements imposed by the Commission Implementing Decision (EU) 2016/650 of April, 25th 2016, laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market or meets the requirements of Article 51 (1) of EU Regulation 910/2014.

6.1.2. Delivery of the private key to the Subject

After generating the keys in CUZ Sigillum, it is delivered to the Subject along with information enabling the activation of the private key, the Subject is obliged to immediately change the data allowing the activation of the private key.

6.1.3. Delivering the public key to the certificate issuer

Public keys of Subjects are delivered from the Registration Point in the form of a certification application, signed by the Registration Inspector.

6.1.4. Delivery of the public CA key to Relying Parties

The CUZ Sigillum public key may be obtained by the Subject from the Registration Point, at the time of registering the Subject or it can be downloaded from the repository, subject to the Subject giving consent to the certificate being published in the repository. The authenticity and integrity of the qualified authority certificate may be verified using the certificate of the superior authority NCCert published at the website: http://www.nccert.pl

6.1.5. Parameters of keys

The qualified CUZ Sigillum authorities use the following keys:

- For the 'CUZ Sigillum' authority – CA1 qualified' key with a length of 4096 bits,

- OCSP service - key with a length of 4096 bits.

The qualified time stamping service uses keys with a length of 4096 bits.

Private keys used by CA and CUZ Sigillum are stored in cryptographic modules whose security level is specified in 6.1.19.

The length of keys used by the Registration Inspector is 2048 bits.

Unless provided otherwise by provisions of law, cryptographic algorithms used for generating keys should meet the minimum requirements stipulated in the ETSI TS 119 312 „Electronic Signatures and Infrastructures; Cryptographic Suites" document.

6.1.6. Public key generating parameters and quality control

The CUZ Sigillum authorities' keys are generated with hardware cryptographic modules, which assure proper quality of the obtained keys. Regardless of whether the public keys have been generated by CUZ Sigillum or by the Subject themselves, the key generating parameters must meet the requirements stipulated in the Ordinance.

6.1.7. Use of keys

The manner of using the key is defined in the *KeyUsage and ExtendedKeyUsage* field of the standard certificate extensions (X.509 v3). The field should be verified by applications using the certificate.
Authority keys are used solely for signing Subject's certificates and signing CRL lists.
OCSP keys are used solely for signing OCSP responses.
UZC keys are used solely for signing time stamps.

6.1.8. Protection, activation, deactivation and destroying keys

The Subject's private keys associated with qualified certificates are processed solely in qualified devices for making electronic signatures, compliant with the requirements of the Ordinance.

Private keys of all CUZ Sigillum authorities and services are stored in a technical component (cryptographic module).

6.1.9. Cryptographic module standards and control

A hardware cryptographic module meeting the requirements of class FIPS 140-2 level 3 and Common Criteria EAL4+ is used in the CUZ Sigillum authorities' infrastructure. The cryptographic module was delivered to CUZ Sigillum in the manufacturer's packaging with seals in an undamaged condition, as well as the serial number and firmware version confirmed by the manufacturer. Periodic control of the module comprises visual verification of the seals' integrity, control of the serial number and messages on the device's display. The device undergoes self-control upon every start-up of the cryptographic module.

6.1.10. Private key control by many persons

Private keys of all CUZ Sigillum authorities are protected by splitting the key into parts, so called secrets, pursuant to the requirements of the Ordinance. CUZ Sigillum uses an indirect method of splitting the key, in which the symmetric key, with which the private key is encrypted, is split into parts. A defined number of shared secrets is necessary to recover the key, constituting the so-called threshold. Shared secrets are recorded on electronic cards and password-protected.

6.1.11. Depositing the private key

It is not allowed to deposit the private keys of CUZ Sigillum authorities, Registration Inspectors, infrastructure private keys and Subjects into deposit.

6.1.12. Backup copy of the private key

CUZ Sigillum creates backup copies of the private keys of authorities for the event of an emergency key recovery procedure. The key backup copies are stored in a form encrypted with a symmetric key, which is split into shared secrets. The secrets are stored in safes in secure zones, only authorised personnel performing trusted roles have access to them. Access to the backup secret sets requires double control.

CUZ Sigillum does not create backup copies of private keys of: infrastructure, Registration Inspectors and Subjects.

6.1.13. Archiving the private key

It's not allowed to archive any private keys used for making an electronic signature or authorising with the use of infrastructure keys:

1. of the CUZ Sigillum private key used for confirming certificates, OCSP, CRL lists, time stamps;
2. Private keys of Registration Inspectors, used for signing certification applications;
3. Private keys of Subjects, associated with qualified certificates.

6.1.14. Private key transfer to / from the cryptographic module

A private key in an open form may only be processed in the cryptographic module. The transfer of private keys of the CUZ Sigillum authorities to the cryptographic module takes place in the key loading procedure. The key in the open form is not transferred outside the cryptographic module.

6.1.15. Storage of the private key in the cryptographic module

The private key is stored in the cryptographic module memory in an open form solely during an application session of the cryptographic module.

6.1.16. Manner of activating the private key

The cryptographic material containing keys is stored in the file system in an encrypted form. The activation of private keys of CUZ Sigillum authorities requires the cooperation of two persons performing trusted roles, whereas one of them must by a Security Inspector, holding shared secrets on electronic cards and the passwords for these cards.
The activation of the private keys of a Subject and a Registration Inspector requires the knowledge of the PIN code to the technical component they use. The PIN code is handed over to the Subject in a secure manner.

6.1.17. Manner of deactivating the private key

The deactivation of private keys of the CUZ Sigillum authorities takes place under the control of a Security Inspector. The deactivation of a private key comprises the ending of the operation of the cryptographic module application in the operating system.
The deactivation of the public key of a Subject or a Registration Inspector takes place as a result of ending the operation if the application using the key.

6.1.18. Manner of destroying the private key

The private keys of all CUZ Sigillum authorities and services are destroyed together with the physical destruction of the electronic cards containing the shared secrets. A report of the operations performed upon destroying the keys is prepared and signed by all participants of the destruction procedure.

The private key of a Subject and a Registration Inspector is destroyed together with the physical destruction of the technical component or key module, on which it is recorder, or through overwriting the memory of the technical component or key module with a string of zeros.

6.1.19. Security measures level offered by the cryptographic module

A hardware cryptographic module meeting the requirements of class FIPS 140-2 level 3 and Common Criteria EAL4+ is used in the CUZ Sigillum authorities' infrastructure.

6.1.20. Archiving the public key

All public keys are archived by CUZ Sigillum. Expired certificates are archived for a period of at least 20 years of the date of origin.

6.1.21. Validity period of certificates and pairs of keys

The validity periods of CUZ Sigillum certificates and Subjects' certificates are no longer than:

- 11 years for CUZ Sigillum certificates;
- 2 years for Subject certificates;

The starting time of CUZ Sigillum and Subject certificates may not be earlier than the time they are created.
The validity period of a private key may be shorter than that of the certificate.
The time stamp authority has only one active key for signing time stamp requests at all times.

6.1.22. CUZ Sigillum certificate renewal

CUZ Sigillum must apply to the Minister of Digital Affairs for issuing a new certification document appropriately in advance prior to the expiry of the current certification document. The generation of a new certification document takes place at least 2 years before the current certification document expires.

6.2. Activation data

Activation data is used by Subject, Registration Inspectors and authorised persons operating certification authorities. Activation data takes the form of PIN codes or passwords and is used for activating private key,

6.2.1. Generating and installing activation data

The data activating CUZ Sigillum shared secrets - in the form of password codes - is defined in compliance with the procedures developed and implemented by CUZ Sigillum.

The Subject keys activation data is:

1. Defined by the Subject - if they generate the pair of keys;
2. Defined by the Registration Inspector - if the pair of keys is generated at the Registration Point - in this case the data should be changed by the Subject as soon as this is reasonably possible.

6.2.2. Activation data protection

The persons authorised to use the data are responsible for the protection of activation data of CUZ Sigillum authority keys.

The Subjects and Registration Inspectors are responsible for the protection level of their activation password. The password should be stored in a place which is secure and unavailable to third parties. The password may not be communicated to third parties.

6.2.3. Other aspects concerning activation data

Not applicable.

6.3. Managing the information system security

The PWPW SA security policy is in force at CUZ Sigillum. The Detailed Information Security Policy at PWPW SA Document has been approved by the PWPW SA Management Board, published and communicated to the employees and the proper external parties through making it available at the official PWPW SA website. All changes to the policy document are made available to the interested parties. A Policy Review and inventorying takes place within the Integrated Management System. Changes to the Policy require the approval of the PWPW SA Management Board.

Reliable software and hardware is used in the CUZ Sigillum ICT system. A set of procedures assuring secure operations has been implemented.

6.3.1. Special technical requirements regarding the security of computers

Technical and environmental security mechanisms, concerning the security of computers specific for the CUZ Sigillum activity have been implemented. The security measures are realised in applications, operational systems, ICT network and physical security features.

6.3.2. Security measures level of computers

The computer security features used in the CUZ Sigillum infrastructure meet the requirements for systems operated at PWPW SA.

6.3.3. ICT network protection

The CUZ Sigillum ICT network has been divided into segments by means of network firewalls, on which additional intrusion detection modules have been set up. Rules on the network firewalls admit only defined traffic, through access control lists, other connections are rejected. Logs of network events are regularly monitored by personnel performing trusted roles.

Changing the rules on network firewalls requires a formal approval of an application for a change, which takes place pursuant to a documented change management procedure. Network firewalls management takes places in compliance with the four eyes principle (double control). Network firewall rules are reviewed by personnel performing trusted roles, not less frequently than once a quarter or after the occurrence of a security incident.

Communication between components included in CUZ Sigillum is secured by means of a two-sided SSL / TLS protocol with client authentication.

6.3.4. Privileges of users

Granting privileges to users in the CUZ Sigillum ICT system requires formal application approval in accordance with a documented privileges management procedure. Access rights configuration takes place based on the smallest privileges and division of roles principle. Accounts of users who changed positions or terminated employment are immediately modified or blocked.

6.3.5. Change Management

All changes in the ICT systems configuration and software are identified, logged, categorised, prioritised, evaluated, assessed, approved and implemented in compliance with the change management procedure. A decision about implementing a change is taken by the change

board (CAB), based on the opinions prepared by representatives of particular organisational units, including the IT security unit.

6.3.6. Protection against malware

Protection against malware is performed by technical security measures (systems' separation, antivirus software and preventing the installation of applications by unauthorised users) and organisational (increasing users' awareness, internal instructions describing the procedure in case of malicious code infection), which are aimed at limiting the risk of infection by malware.

6.3.7. Security updates management

The CUZ Sigillum ICT systems are regularly scanned for security gaps with vulnerability scanners. Moreover, the systems are Subject to penetration tests prior to commissioning and after significant changes. The identified vulnerabilities are Subject to assessment, after which the proper measures are taken for the purpose of countering the risk according to the developed and implemented vulnerability management instruction. Response time for identified critical vulnerabilities is up to 48 hours.

6.4. Security management of production process life cycle

The principles of life cycle technical control have been defined in operational procedures used by CUZ Sigillum.

Subject applications and CUZ applications are developed in a controlled environment utilising relevant quality management procedures, which guarantee software integrity and control of its version.

According to the system security requirements, an ICT security department representative takes part in every stage of project works, whose task is to assess security of the implemented solution. Prior to commissioning and periodically, the system is subject to independent and reliable penetration tests.

6.5. Application of time stamps

Time stamps compliant with the ETSI EN 319 422 standard are made within the operations of CUZ Sigillum.

7. Profile of a certificate and CRL lists

Qualified certificate profiles are compliant with the formats described in the ITU-T X.509 standard. Additionally, the issued certificates are compliant with certificate profiles defined in the following standards:

- For natural persons' certificates - ETSI EN 319 412-2
- For legal persons' certificates - ETSI EN 319 412-3
- QCStatements for qualified certificates - ETSI EN 319 412-5

7.1. Certificate structure

Under the Policy, CUZ Sigillum issues qualified certificates containing the following electronic data structures:

1. Certificate contents (**tbsCertificate**)
2. Information about the algorithm used for signing the certificate (**signatureAlgorithm**)
3. Validation of the certificate, made by the authority issuing the certificate (**signatureValue**)

Please find below a description of each of the structures

7.1.1. Certificate contents

According to the X.509 standard the certificate contents comprise standard and extended fields.

The table presents the range and value of **standard fields** of CUZ Sigillum certificates.

No	Field	Description	Contents
1.	Version	Format version compliant with X.509	V3
2.	SerialNumber	Certificate serial number, unique within the authority issuing the certificate	--
3.	Signature	Information about the algorithm used for signing the certificate	--
4.	Issuer	Identifier (DN name) of the certificate issuer	For the CUZ Sigillum authority - qualified CA1 CN = CUZ Sigillum - qualified CA1 O = Polska Wytwórnia Papierów Wartościowych S.A. OrganizationIdentifier = VATPL-5250009010 C = PL

5.	Validity	Certificate expiry date, defined as the data and time of the beginning of certificate validity (notBefore) and the date and time of certificate expiry (notAfter)	--
6.	Subject	Identifier (DN name) of the certificate issuer	--
7.	SubjectPublicKeyInfo	Definition of the algorithm used by the certificate owner and their public key	--

Please find below the range and values of certificate extended fields:

1) Standard extensions
    a. AuthorityKeyIdentifier

    This extension identifies the public key certificate of the authority issuing the certificate - the extension is not critical

    b. KeyUsage: nonRepudiation

    Defines the allowed certificate usage - the extension is critical.

    c. CertificatePolicies

    For the CUZ Sigillum authority - qualified CA1:

    1. In case of a qualified electronic signature certificate: 1.2.616.1.113725.0.0.3
    2. In case of a qualified electronic seal certificate: 1.2.616.1.113725.0.0.4

    The extension contains information about the certification policy (identifier, electronic address) adopted by the certification authority - the extension is not critical.

    d. SubjectAltName

        i. rfc822Name - e-mail address of the Subject – if present

    Alternative name of the entity - the extension is not critical.

    e. BasicConstraints

Defining, whether the certificate owner is the end user, or an entity issuing certificates - the extension is critical.

f. SubjectDirectoryAttributes

This extension contains additional attributes associated with the Subject and supplementing information included in the Subject and SubjectAlternativeName files - the extension is not critical.

It may contain the following attributes:

- DateOfBirth - contains the date of birth of the certificate owner,
- PlaceOfBirth - defines the place of birth of the certificate owner,

g. Authority Information Access

i. OCSP – OCSP service address

ii. caIssuers – authority certificates publishing address

The extension contains indication of the localisation and method of access to information or services made available by the certificate issuer, in which the extension is included - the extension is not critical.

h. cRLDistributionPoints

The extension contains indication of the manner of making CRL lists available - the extension is not critical.

2) Non-standard extension - qcStatements

The extension contains a declaration of the certificate issuer - the extension is not critical. Declaration consists following attributes (in brackets indicated whether the attribute is required:

a. qcStatement-QcCompliance (Critical)

A statement of the issuer that the certificate is a qualified certificate meeting the requirements in compliance with the requirements of annex I or III or IV to the Ordinance, issued by a qualified entity providing certification services - the extension is present only in qualified certificates.

b. qcStatement-QcLimitValue (Not critical)

Limit of the transaction, which may be confirmed in one operation with the certificate - the extension may be present only in qualified certificates.

c. qcStatement-QcRetentionPeriod (Not critical)

   Storage time ofthe documentation concerning the certificate owner's identity verification.

d. qcStatement-QcSSCD (Not critical)

   A statement of the issuer that the private key associated with the public key of the certificate is stored in a Secure Signature Creation Device (SSCD).

e. qcStatement-SubjectSignatureType (Not critical)

   Definition of the role, which the Subject holds, if the 'Subject' field defines data of the Subscriber.

f. qcStatement- QcType (Not critical)

   i. for qualified certificates for electronic signature: id-etsi-qct-esign
   ii. for qualified certificates for electronic seal: id-etsi-qct-eseal

   Definition of the issued qualified certificate type.

g. qcStatement – QcPDS (Critical)

   Pointing of URL address, document PKI Disclosure Statements (PDS)

h. esi4-qcStatement-4 (Not critical)

   Indicates that the private key associated with the certificate was generated on QSCD device

   id-etsi-qcs-QcSSCD {0.4.0.1862.1.4}

i. esi4-qcStatement-6 (Not critical)

   Declaration designating that the electronic signature / seal certificate are compliant to eIDAS Regulation

   i. id-etsi-qct-esign {0.4.0.1862.1.6.1} - for certificates for electronic signature

   ii. id-etsi-qct-eseal {0.4.0.1862.1.6.2} - for electronic seal certificates

The above mentioned extension fields of the certificate have been qualified as critical or non-critical.

In case of **critical fields** the system using the certificate is required to interpret it correctly. If the system using the certificate does not handle fields indicated to be critical, the certificate may not be handled correctly.

Non-critical fields may be ignored if the system using the certificate is not able to interpret them correctly.

7.1.2. Algorithm used for signing the certificate

The value of the **signatureAlgorithm** parameter identifies the cryptographic algorithm used for the purpose of certifying the certificate by its issuer. For the CUZ Sigillum - qualified CA 1 the algorithm sha256WithRSAEncryption is used. { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }

7.1.3. Certificate validation

The value of the **signatureValue** parameter is created by preparing an abbreviation of the certificate contents (tbsCertificate) followed by signing the thus prepared abbreviation with the certificate issuer's private key.

7.2. CRL list structure

The structure of the lists of revoked and suspended certificates (CRL) issued hereunder is defined herein. The contents and format of the list is compliant with the provisions of the ITU-T X.509 standard.

The CRL list of certificates is a set of fields, whose meaning has been presented below:

1. Information about revoked certificates (**tbsCertList**)
2. Information about the algorithm used for signing the list (**signatureAlgorithm**)
3. Electronic validation, made by the authority issuing the list (**signatureValue**)

Revoked certificates are published on the CRL list also after the expiry date, whereas suspended certificates are removed from the CRL list the moment they are unsuspended.

Please find below a description of each of the structures

7.2.1. Revoked certificates

According to the X.509 standard the list contents comprise standard and extended fields.

The table presents the range and value of **standard fields** of CRL lists issued by CUZ Sigillum.

No	Field	Description	Contents
1.	Version	Format version compliant with X.509	„1" (X.509 v2)
2.	Signature	Information about the algorithm used for signing the CRL list	--
3.	Issuer	Identifier of the certification authority issuing the CRL list	For the CUZ Sigillum authority - qualified CA1 CN = CUZ Sigillum - qualified CA1 O = Polska Wytwórnia Papierów Wartościowych S.A. OrganizationIdentifier = VATPL-5250009010 C = PL
4.	ThisUpdate	Data/time of issuing the CRL list	--
5.	NextUpdate	Data/time of issuing the next CRL list (the next list may not be issued later)	--
6.	RevokedCertificates	List of revoked certificates, an individual certificate is described with the following attributes: serial number of the revoked certificate (userCertificate), certificate revocation date (revocationDate), extension of information for the revoked certificate (crlEntryExtensions)	--
7.	CrlExtensions	Extended information about the CRL list	--

Please find below the range and values of CRL list extended fields:

a. AuthorityKeyIdentifier

   This extension identifies the public key certificate of the authority issuing the CRL list - the extension is not critical

b. CRLNumber

   Contains the CRL list number Numbers are assigned consecutively, according to the order of issuing CRL lists by the certification authority.

7.2.2. Algorithm used for signing the list

The meaning of the **signatureAlgorithm** parameter is the same as in case of a certificate.

For the CUZ Sigillum - qualified CA 1 the algorithm sha256WithRSAEncryption is used.

{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }

7.2.3. Certificate validation

The meaning of the **signatureValue** parameter is the same as in case of a certificate.

7.3. OCSP response structure

The certification authority makes available an on-line certificate status verification service (OCSP). The contents and format of the OCSP answer is compliant with the provisions of the RFC 6960 standard.

The server of the authority issuing the notification about the certificate status uses a dedicated pair of keys, allocated solely for this service.

The OCSP answer is a set of fields, whose meaning has been presented below:

1. Information about the certificate status (**tbsResponseData**)
2. Information about the algorithm used for signing the answer (**signatureAlgorithm**)
3. Electronic validation, made by the authority issuing the answer (**signatureValue**)
4. Certificate as an option

7.3.1. Description of structures

No	Field	Description	Contents
1.	Version	Format version compliant with RFC6990	v1
2.	Responder	Identifier of the service provider's certification authority	--
3.	ProducedAt	Date / time of generating the answer	--
4.	Responses	List of current certificate statuses, an individual certificate is described with the following attributes: serial number of the revoked certificate (certID), certificate status (certStatus), date / time for which the status has been verified (thisUpdate), date / time of the next	--

		status update (nextUpdate), certificate information extension (singleExtensions)	
5.	responseExtensions	Extended information about the OCSP answer	--

7.3.2. Algorithm used for response signing

The meaning of the **signatureAlgorithm** parameter is the same as in case of a certificate.

For the CUZ Sigillum - qualified CA 1 the algorithm sha256WithRSAEncryption is used.

{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }

7.4. TSA message structure

CUZ Sigillum provides qualified electronic time stamps as the qualified trust service.

In order to obtain the time stamp Subject should send the time stamp request in accordance with RFC 3161 and ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.

The request is electronically signed by the Subject and include its certificate, used to verify the signature.

The request does not contain the document. Only hash value is sent, which is calculated by a Subject's application.

Timestamps preservation require the same procedure and data formats, such as for the original timestamp.

After receiving the timestamp, CUZ Sigillum verifies electronic signature and authorizes Subject.
After positive validation timestamp is issued to the Subject.

The timestamp contains the date and time (UTC) of timestamp issuance which needn't be identical with the moment of the receiving request by TSA.

If the timestamp token can't be issued, TSA send the reason for denial of service instead.

Qualified TSA uses a dedicated pair of keys, designed only for this service.

Timestamp request profile and timestamp server response profile are presented in sections below.

7.4.1.Non-authenticated timestamp request profile

No	Field	Description	Contents
1.	Version	Format version compliant with RFC 3161	„1”
2.	messageImprint	Hash value of the time-stamped message.	--
3.	hashAlgorithm	OID identifier of hash function alghoritm	SHA-256 {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha256(1)}
4.	hashedMessage		A bytes string representing the abbreviation of the message.
5.	reqPolicy	Mandatory field. Means a request to issue a timestamp according to the specified policy.	1.2.616.1.113560.10.2.2.0
6.	Nonce	Number once – value generated by Subject.	--
7.	certReq	Optional field. If there is and it is equal to "1" indicates that the server should respond to attach the certificate used to verify the timestamp.	“1” lub „0”
8.	Extensions	Extensions by RFC 3161. The field can’t occur. If it occurred, the request is rejected by the server.	--

The possibility of the use of unauthenticated timestamp requests, in accordance with the profile above may be admitted for selected Subjects identified by other means (in particular for the internal system entities CUZ Sigillum).

For other Subjects valid is *Profile authenticated timestamp request.*

7.4.2.Authenticated timestamp request profile

No	Field	Description	Contents
1.	Version	Format version compliant with RFC 3161	„1”
2.	digestAlgorithms	Hash algorithm identifier (OID)	SHA256 {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha256(1)}
3.	contentInfo	Field contains proper timestamp request.	--

4.	contentType	OID Identifier	id-signedData { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 2 }
5.	content	Encoded in ASN.1 (DER) unauthenticated request timestamp - in line with the profile specified in section 7.4.1	--
6.	certificates	Certificate list.	The list should include the certificate (X509v3) key, which was signed request marks the time (and only the certificate)
7.	crls	List of CRLs.	The list can be empty - it is not processed by the server timestamp (CRL are taken from another source).
8.	signerInfos	List of signatures.	The list must contain exactly one signature
9.	version	version	„1”
10.	singerIdentifier	Information about the person signing the certificate request	
11.	issuerAndSerialNumber		
12.	issuer	Distinguished Name (DN) of certificate issuer	
13.	serialNumber	Certificate serial number	
14.	digestAlgorithm	OID identifier of hash function algorithm.	SHA-256 {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha256(1)}
15.	signedAttrs	Pole opcjonalne. Jego zawartość nie jest przetwarzana przez serwer znacznika czasu.	--
16.	signatureAlgorithm	Algorytm podpisu	sha256WithRSAEncryption { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
17.	signature	Wartość podpisu.	
18.	unsignedAttrs	Optional field. The content is not processed by TSA.	

7.4.3. TSA response profile.

No	Field	Description	Contents
1.	Status	Status information to process your request issue timestamp.	
2.	Status	Status process your request. If the field is equal to 0, this means that the tag has been properly issued. Any other value of listed in the "Content" means: not issued (according to RFC 3161).	One of following values: 0, 2, 3, 4.

3.	statusString	Text description of the reasons for rejecting the request to issue a timestamp.	
4.	failInfo	The reason for the rejection of a request to issue a timestamp	One of following number codes (according RFC 3161): 0, 2, 5, 14, 15, 16, 17, 25.
5.	timeStampToken		
6.	contentType	OID identifier	id-signedData { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 2 }
7.	content		
8.	version	version	„1”
9.	digestAlgorithms	Identifier of hash function algorithm.	SHA-256 {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha256(1)}
10.	contentInfo		
11.	contentType	OID identifier	id-ct-TSTInfo { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) ct(1) 4}
12.	content	Coded timestamp token value.	
13.	version	version	„1”
14.	policy	Timestamp policy identifier (OID)	1.2.616.1.113560.10.2.2.0
15.	messageImprint	Message hash value	
16.	hashAlgorithm	OID identifier of hash function algorithm.	SHA-256 {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha256(1)}
17.	hashedMessage	Byte string representing the hash of the message	
18.	serialNumber	Timestamp serial number	
19.	genTime	UTC Time of issueing timestamp.	
20.	accuracy	GenTime accuracy.	
21.	seconds		„1”
22.	nonce	Nonce value from timestamp request	
23.	certificates	Certificate list.	If the value of certreq field is equal to "1", the field contains the certificate CUZ Sigillum used to verify the timestamp.
24.	Crls	Empty CRL list.	
25.	signerInfos	List of signatures.	Contains certificates of CUZ Sigillum.
26.	version	Version number	„1”

27.	singerIdentifier	Information about the service signing the certificate response	
28.	issuerAndSerialNumber		
29.	issuer	Distinguished Name (DN) of certificate issuer	
30.	serialNumber	Serial number	
31.	digestAlgorithm	IOID identifier of hash function algorithm	SHA-256 {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha256(1)}
32.	signedAttrs	Set of signed attributes	1) Certificate hash value CUZ Sigillum 2) Timestamp hash value
33.	signatureAlgorithm	Signature algorithm	sha256WithRSAEncryption { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
34.	signature	Signature value of signed attributes signedAttrs (contains timestamp).	
`35.	unsignedAttrs	Empty set of attributes	

8. Compliance audit

PWPW SA conducts its activity in compliance with the requirements of international management standards. It has established inter alia the Integrated Management System Policy and the Detailed Information Security Policy. The implementation of international standards is not just a guarantee of the highest quality of products, but also assuring the highest possible security level of the security produce and services provided. This is confirmed by numerous certificates, in particular:

- Certificate of the Business Continuity Management System for the compliance with ISO 9001
- Certificate of the Information Security Management System for the compliance with ISO IEC 27001 for the activity conducted by CUZ Sigillum.

The audit of compliance with the ISO IEC 27001 standard concerns the area of issuing qualified certificates. It was performed by external units, independent of PWPW SA.

Moreover, CUZ Sigillum undergo a compliance audit pursuant to art. 9 of the Act. The purpose of the audit is to confirm the compliance of the CUZ Sigillum activity with the requirements of the law and standards, concerning the provisioning of trust services. The audit is performed in compliance with the ETSI EN 319 403 standard guidelines by an accredited, external compliance assessment unit.

8.1. Frequency and circumstances of assessment

The audit of compliance with the eIDAS requirements is performed at least every 24 months, whereas the certification audit for the compliance with the ISO IEC 27001 standard - every three years.

Moreover, the Minister of Digital Affairsmay perform an audit of the compliance with the eIDAS requirements (pursuant to art. 20 point 2) of the Act.
In turn, supervisory audits take place every year and after three years of the certification audit - a recertification audit takes place for the purpose of the ISO IEC 27001 standard.

8.2. Auditors identity / qualification

All external audits are performed by companies independent from PWPW SA.
In case of a compliance audit it has to be a company which is listed in the European Union register, containing the list of entities which may perform such audits.

Internal audits are performed by a PWPW SA own unit in charge of audits.

8.3. Relation of the auditor to the assessed entity

Internal auditors are permanent employees of PWPW SA, employed in a unit other than CUZ Sigillum. There is no official dependence between the internal auditors and the CUZ Sigillum management.

External auditors are employed by companies independent from PWPW SA, and in case of compliance audits they are employees of companies listed in the registers published by the European Union Parliament. The said auditors may not have any relations (family, professional and the like) with PWPW SA.

8.4. Issued covered by the audit

The certification audit is performed according to the rule that all of the CUZ Sigillum activity must be verified for the compliance with the ISO IEC 27001 standard within three years (the certification or recertification audit and two annual supervisory audits).

The compliance audit, performed pursuant to art. 20 of eIDAS has the purpose of confirming, that a qualified provider of trust services and the qualified trust services they provide meet the requirements stipulated in the eIDAS ordinance and the Act. The compliance audit scope is presented by the company performing the audit.

In particular, the compliance audit should include:

- Physical security measures;
- Organisation security measures, including those associated with personnel management;
- Security measures associated with the protection of ICT resources;
- Security measures associated with the protection of records.

The issues covered by the audit performed pursuant to art. 21 of eIDAS by the supervisory body are defined by the said organ.

8.5. Actions taken in case of detecting irregularities

In case the performed audit detects cases of CUZ Sigillum failing to meet the requirements of the eIDAS ordinance or the ISO IEC 27001 standard, CUZ Sigillum is taking all possible actions to eliminate them. The unit responsible for IT systems security at PWPW SA Is responsible for eliminating the requirements which are not met. The said unit is also responsible for the preparation of a written answer with information concerning the removal of the requirements not met to the supervisory body and / or the auditing unit.

8.6. Communication of the audit results

Due to the type of its activity, CUZ Sigillum does not publish audit results or any documentation associated with the audit.

9. General provisions

This chapter presents the responsibility and obligations of PWPW SA, the Subjects, Registration Points and Certificate Users (the Relying Parties)

9.1. Fees

Fees are charged for all services provided by the CUZ Sigillum. The amounts and types of fees are published at the website at:

Cennik PWPW

9.2. Liability of PWPW SA

PWPW SA is liable towards the certification services Recipients for all damage caused by the non-performance or undue performance of its obligations, unless the non-performance or undue performance is a result of circumstances, for which PWPW SA Bears no responsibility and which it could not have prevented despite exercising appropriate care.

9.2.1. Financial liability

PWPW SA is covered by insurance compliant with the requirements of the Ordinance of the Minister of Finance of 16.12.2003 on the Compulsory Civil Liability of a Qualified Certification Services Entity.

PWPW SA Financial liability for the provisioning of qualified services regarding a single event is the equivalent of EUR 250 000, however not more than EUR 1 000 000 concerning all events of that kind. The financial liability is in place in a 12-month calendar period the same as the calendar year.

9.3. Protection of information

All data, whose unauthorised disclosure might prejudice the interest of Sigillum Centrum Usług Zaufania PWPW SA or a Subject of trust services are treated as confidential and Subject to protection. Confidential information described herein is not the same as confidential information within the meaning of the Act on the Protection of Confidential Information. The word ‘confidential’ should be understood as ‘discretion, making available only to few persons’.

9.3.1. Scope of confidential information

All information, whose unauthorised disclosure might prejudice the interest of Sigillum Centrum Usług Zaufania PWPW SA or Subjects of trust services and in particular it is:

1) data used for making qualified electronic signatures of electronic seals

2) data for making electronic affirmations

3) all private infrastructure keys

4) personal data of the trust services Subjects

5) personal data of the Subscriber representatives

6) agreements signed with the Registration Points (if relevant)

7) system security overview and operational risk assessment

8) operational continuity plan

9) basic configuration description

10) operational and security procedures

The detailed scope of information constituting company secrets is defined in

Internal documents of PWPW SA.

9.3.2. Information remaining outside the scope of confidential information

The following information are not treated as confidential:

1) reason to revoke a certificate

2) information contained in the Subject's certificates and CRL lists

3) information published in the repository

4) information concerning breaches of the provisions on trust services by a provider of trust services

5) policies

6) rules and regulations

7) other documents, listed herein as documents placed in the repository

9.3.3. Responsibility for the protection of confidential information

The following persons are obliged to keep information confidential:

1) persons remaining in a labour, contractor or other legal relation of a similar type with the provider of trust services;

2) persons remaining in a labour, contractor or other legal relation of a similar type with the entities providing services to the provider of trust services;

The confidentiality obligation is valid for 10 years since the day the legal relation terminates.

The validity period of the obligation to keep secret the data for making an electronic signature or electronic stamp is not limited in time.

Subject private keys associated with certificates should be treated as protected by the Subject. All legal effects resulting from improper or unauthorised use of the said keys after they are transferred to the Subject are borne by the Subject.

9.4. Personal Data Protection

Personal data is processed by Sigillum Centrum Usług Zaufania PWPW SA in accordance with Art. 13 para. 1 and 2 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (RODO) on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (Regulation 2016/679)

To this end, at PWPW SA, the Personal Data Security Policy was developed and implemented, and the Information Security Administrator was appointed, whose task is to supervise the implementation of the provisions of this policy.

9.4.1. Privacy protection plan

The principles of gathering, protection and use of personal data are compliant with the mandatory provisions of the Act on the Protection of Personal Data and internal PWPW SA documents.

Personal data protection is performed through: physical security measures, Organisational procedures and ICT security measures. Personal data security is understood as assuring its confidentiality, integrity and accountability.

The scope of personal data gathered and processed by CUZ Sigillum is consistent with the purpose, for whose realisation the data is necessary.

9.4.2. Information considered to be private

Private data is considered personal information. Within the meaning of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (RODO), all personal or identifiable information is considered personal data.

A person possible to be identified is a person, whose identity may be directly or indirectly determined, in particular by quoting the identity number or one or a couple specific factors determining the person's physical, physiological, mental, economic, cultural or social characteristics.

9.4.3. Information not considered to be private

Within the meaning of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (RODO), information is not considered to enable identification of a person if it would require excessive costs, time or actions.

9.4.4. Responsibility for the protection of private information

The following persons are obliged to keep personal data private:

1) persons remaining in a labour, contractor or other legal relation of a similar type with the provider of trust services;

2) persons remaining in a labour, contractor or other legal relation of a similar type with the entities providing services to the provider of trust services;

The confidentiality obligation is valid for 10 years since the day the legal relation terminates.

9.4.5. Consent to use private information

The Consent of the Recipient of trust services / representative of the Subscriber for processing their personal data in association with the provisioning of trust services is included in the agreement on the provision of the service and is mandatory. The Recipient of trust services must give additional consent for the processing of personal data for marketing purposes and for communicating commercial information.

9.4.6. Disclosure of information to administrative authorities

An exception from the confidentiality obligation is possible solely under art. 15 item 4 of the Act.

9.5. Intellectual property right

All trademarks, labels, patents, graphical signs, patents, licenses and other marks used by the CUZ Sigillum and PWPW SA are the intellectual property of their owners.

All keys issued by the CUZ Sigillum and PWPW SA associated with the public key certificate are the property of the entity in case of an individual subject and the property of the entity represented by the subject in the case of a subject of a qualified certificate.

9.6. Exclusion from the warranty

PWPW SA bear no liability towards the certification services recipients for:

a) Damage resulting from the use of a public key certificate outside the scope defined herein, including in particular if the damage results from exceeding the Highest Limit Transaction Value, if the value has been defined in the public key certificate.
b) Damage resulting from false data of the Subscriber included in the public key certificate

In case PWPW SA operates through Registration Points, liables for the activity of the Registration Points as for its own activity.

9.7. Limitation of liability

PWPW SA bears no liability for any damage, which resulted or might have resulted for the certification services recipients for reasons other than the non-performance or undue performance of obligations by PWPW SA or by authorised entities acting on its behalf. In particular, PWPW SA bears no liability for:

a) The effects of incorrect use of the Subject's private key,
b) The effects of the use of the Subject's private key by an unauthorised person,
c) The results of the loss of security of the cryptographic algorithms used by PWPW SA, subject to the use of the said algorithms not being compliant with executive ordinance for the Act,
d) The results of incorrect, incompliant herewith, verification of public key certificates issued by PWPW SA, including the results of using by the Relying Party of a simplified verification procedure of public key certificates described herein.

9.8. Term and Termination

Validity and manner of introducing changes

This Certification Policy is valid for an indefinite period. PWPW SA reserves the right to introduce changes at any time. Changes may result in particular from:

- changes of the mandatory provisions of law, both Polish and European,
- changes resulting from the manner of provisioning by PWPW of services discussed herein.

Changes will be announced by PWPW SA at the website available at: www.sigillum.pl

Changes enter into force after 30 days after being published, subject to mandatory provisions of law providing another time.

9.9. Notification

This subcomponent discusses the way in which one participant can or must communicate with another participant on a one-to-one basis in order for such communications to be legally effective.

9.10. Changing Policy provisions

Each modification hereof must be accepted by the Certification Policies Acceptance Council of PWPW SA. The amended Policy is labelled with a new, unique version number and OID.

A change hereof may be made in a planned or accelerated manner.

In case of a planned change of the Policy, PWPW SA will inform the Minister of Digital Affairsof changing the Policy 7 days in advance of the entering into force of the change.

The procedure of accelerated amendment of the Policy takes place when RPZC PWPW SA determines that the use of the previous version hereof is not secure for the certification services recipients. In such a case, RPZC PWPW SA may introduce the amended Policy immediately. RPZC PWPW SA will inform the Minister of Digital Affairs of amending the Policy immediately, no later than 7 days after the amendment is accepted.

The new version of the Policy concerns certificates issued after it enters into force.

In cases justified by necessary, changing requirements for the security of information protected with the use of already issued certificates, RPZC PWPW SA may decide that the new version here of or some of its provisions will enter into force for all certificates and time stamps, also those issued under previous versions of the Policies.

If the changes do not result from results attributable to PWPW SA, but are caused e.g. by requirements of the law of changing security conditions, including the security of cryptographic algorithms, the Subjects will not be entitled to damages for the possible limitations of the use of certificates.

If the changes to the Policy result solely from reasons attributable to PWPW SA and are associated with limitations of the possibility to use certificates, the Subjects have the right to refuse consent to further use of certificates under the new Policy version and a reimbursement of remuneration - upon the principles defined in the Rules and Regulations.

If changes of TS Policy effect on content of the "Terms and Conditions" this document will be updated.

9.11. Resolution of disputes

In case a dispute arises between CUZ Sigillum and a Subject, the parties will attempt to resolve the dispute by amicable understanding. Should there be no understanding, the dispute will be settled by the common court of jurisdiction for the seat of PWPW SA.

9.12. Applicable Law

The Agreement, its execution and all legal relations thereunder are subject to the law mandatory in the Republic of Poland.

9.13. Compliance with provisions of the law

The provisions hereof and of the agreements on the provision of certification services are subject to the provisions of law of the Republic of Poland.

The certification services provided by PWPW SA hereunder are compliant with the requirements of the Act regarding qualified entities providing certification services. For the purpose of interpreting the terms included herein, they should be construed pursuant to the Act on Trust Services and Electronic Identification of September, 5th 2016 (Journal of Laws of

the Republic of Poland 2016, item 1579) and the Ordinance of the Minister of Digitisation of October, 5th 2016 on the National Trust Infrastructure (Journal of Laws of the Republic of Poland of 2016, item 1632)

10. A record of changes in the document

Description of the amendment	Version	Date
Document creation	1.0	01.06.2017
Document publication	1.0	27.06.2017
Document review	1.1	15.06.2018