QUALIFIED TRUST SERVICES PROVIDER "CENCERT"

POLICY FOR QUALIFIED TRUST SERVICES

Version: 1.4

Document Card:

Document title	Policy for qualified trust services
Document owner	ENIGMA Systemy Ochrony Informacji Sp. z o.o.
Version	1.4
Document status	**Approved**
Date of approval	2023-04-13
Number of pages	68

Approved by the Board of Directors of Enigma Systemy Ochrony Informacji Sp. z o.o.

Version history

Version no.	Prepared by	Description of changes	Valid from
1.0	Jacek Pokraśniewicz	Initial version replaces *Policy of certification for qualified certificates* in. 2.3 and *Policy of time stamping and other qualified certification services* in. 1.1.	2017-05-20
1.1	Jacek Pokraśniewicz, Piotr Popis	Implementing of the auditor's comments, ECDSA added	2017-06-14
1.2	Jacek Pokraśniewicz	New functionalities of: generating a certificate based on the public key provided, providing a remote sealing service, adjustment to the GDPR Removal of obsolete transitional provisions	2019-04-01
1.3	Jacek Pokraśniewicz	Added the ability to perform the signature service in the remote (server) rSign mode. New service for issuing certificates for advanced seal (including certificates for PSD2) and website authentication. New ability to authenticate with a notary confirmation or qualified signature. Possibility to issue certificates containing a nickname.	2020-12-03
1.31	Jacek Pokraśniewicz	Added declaration of the availability of current CRLs, details regarding certificates with a pseudonym, other minor fixes.	2021-10-10
1.4	Jacek Pokraśniewicz, Artur Krystosik, Katarzyna Ligenza	Adding a qualified electronic signature validation service. Policy review, editorial corrections. Organizing the Liability restrictions chapter and extending the possibility of revoking a certificate by CenCert.	2023-05-29

Table of contents

1. Introduction

1.1. Introduction

This document is a policy describing the implementation of qualified trust services provided by Enigma Systemy Ochrony Informacji Sp. z o. o. under the CenCert brand, consisting of:

1) issuing and revoking qualified certificates,
2) issuing qualified time stamps and
3) validation of electronic signature and electronic seal.

All provisions relating to "CenCert" should be understood as provisions relating to the company "Enigma Systemy Ochrony Informacji Sp. z o.o.", providing trust services under the "CenCert" brand.

Trust services provided on the basis of the present policy meet the requirements of Regulation 910/2014 (eIDAS).

Structure of the document has been based on standard RFC 3647 "*Internet X.509 Public Key Infrastructure Certification Policy and Certification Practices Framework*".

Provisions specific to qualified validation service for qualified electronic signatures/seals are included in Appendix A, which is an integral part of this document.

1.2. Identifier of certification policy

Policy name	POLICY FOR QUALIFIED TRUST SERVICES
Policy qualifier	None
OID number (*Object Identifier*)	1.3.6.1.4.1.10214.99.1.1.1.4
Date of entry	29.05.2023
Date of expiration	Until revoked

1.3. Description of the certification system and the participating entities

CenCert is a qualified trust service provider (QTSP) operating in accordance with the eIDAS regulation, also in accordance with the implementing acts and in accordance with the national law, namely the Act on trust services (Journal of Laws of 2016, item 1579) and implementing acts.

Public keys for verification of provided trust services:

- key to sign CRL certificates and lists,
- key to sign time stamps
- key for signing validation reports of signature and electronic seal

- are available in the form of certificates issued by the domestic root (NCCert) and on the TSL list.

CenCert does not issue certificates for subordinate trust service providers (SubCA). CenCert issues the certificate of the key to perform the OCSP service.

CenCert supports Subscribers by Registration Authorities (RA):

- Central Point of Registration (CPR) whose data can be found in Chapter 1.3.
- Field Points of Registration.

List of Field Points of Registration is modified in line with up-to-date needs of Subscribers and CenCert's possibilities. Contact details of field points of registration are available on the website.

Most field registration authorities (mobile registration authorities) offer the possibility of providing the service of issuing qualified certificate at the Subscriber's home or in a place of his or her work.

CPR is the contact point for any inquiries and applications related to CenCert's operations.

The contact point for handling any matters related to execution of this certification policy by CenCert is:

Central Registration Authority *CenCert*
ENIGMA Systemy Ochrony Informacji Sp. z o.o.
biuro@cencert.pl

Postal address, contact phones and fax number are published on the website https://www.cencert.pl.

Electronic requests to change the certificate status (invalidation, suspension, suspension repealing) and requests to change of persons authorized to initiate a sealing session in a remote mode should be sent to the address rev@cencert.pl. Correct requests sent to other CenCert addresses (e.g. biuro@cencert.pl) will be, if possible, operated, but CenCert is neither responsible for their punctual service, nor for their service in general.

The Subscriber of trust services with regard to:

- qualified certificate for electronic signature - may be any natural person having full capacity to conclude legal acts,
- qualified certificate for electronic seal-may be any legal person as defined by the national law as well as any other entity of a similar nature (an organizational unit not having legal personality, civil partnership, etc.),
- qualified time stamp, qualified certificates for website authentication, qualified validation service for electronic signatures/seals - may be any natural person, legal person as defined by the national law as well as any other entity of a similar nature (an organizational unit not having legal personality, civil partnership, etc.).

1.4. Scope of applications

CenCert, pursuing this certification policy, issues:

- qualified certificates for implementation of qualified electronic signature,
- qualified certificates for implementation of qualified or advanced electronic seal,
- qualified certificates for website authentication,
- qualified time stamps,
- reports on the validation of electronic signatures and seals,
- infrastructure certificates used internally in the CenCert,
- certificates for OCSP service provision,
- CRL lists and OCSP tokens,
- test certificates.

CenCert, as a qualified trust service provider, may provide services for the submission of:

1) a qualified electronic seal, or
2) a qualified electronic signature

- on behalf of the subscriber, on the terms set out in this policy, applicable procedures and commercial contracts.

Infrastructure certificates are clearly differentiated from qualified certificates by appropriate extensions.

Test certificates are clearly differentiated through the use of DN identifier containing "TEST" fields (or other similar fields such as "TEST1", TEST2", "TEST <characters of other alphabets>", etc.) in all places meant for text data (first and last name, common name etc.) and sample numbers (e.g. 1234…) in places meant for numerical data (PESEL , Tax Identification Number (NIP), etc.).

According to eIDAS:

1. Qualified electronic signature has full legal effect equivalent to personal signature.
2. Qualified electronic signature based on qualified certificate issued in one member state is regarded as qualified electronic signature in all of the remaining member states.
3. Qualified electronic time stamp benefits from a presumption of accuracy of the date and time that it indicates and integrity of the data which the indicated date and time are connected with.
4. Qualified electronic seal issued in in one member state is regarded as qualified electronic time stamp in all member states.

1.5. Certification policy administration principles

The entity authorized to administer the certification policy, including to approve changes is the Board of Directors of ENIGMA Systemy Ochrony Informacji Sp. z o.o.

Any amendments to the certification policy, except for those that remedy obvious editing errors or stylistic errors require a new version number to be assigned.

According to Article 24.2.a) of eIDAS, CenCert informs the supervision authority of any changes in provision of qualified trust services and the intention of cessation of its activity (see also chapter 5.8).

1.6. Glossary of used terms and acronyms

In the present document, the following phrases shall be used in the meaning mentioned below. It should be noted that the descriptions placed here are not always general definitions of a given term, but rather explain the meaning of a given term or acronym in the context used in CenCert.

Term/acronym	Description
eIDAS	Regulation of the European Parliament and the European Council (EU) No. 910/2014 of 23 July 2014 on electronic identification and trust services with regard to electronic transactions on the internal market and repealing Directive 1999/93/EC
Act	Act of 5 September 2016 on trust services and electronic identification.
QTSP	(*Qualified Trust Service Provider*) qualified provider of trust services
PKI	*Public Key Infrastructure*– public key infrastructure – is a system covering Certification Centres, Points of Registration and end users, used for distribution of public key certificates and assuring the possibility of their reliable verification
Certification Centre	CA (Certification Authority) – CenCert; organization which issues certificates, according to this policy and work procedures
Point of registration	RA (Registration Authority) – Organizational unit of CenCert or a third-party company having a contract with Enigma – performing, via authorized Registration Inspectors, activities provided for implementation of this policy and work procedures, in accordance with rights of Registration Inspectors (e.g. confirmation of identity of the persons applying for certificates, transferring electronic cards with keys, etc.)
Legal person	Legal person as defined by the national law or another unit of a similar nature (an organizational unit not having legal personality, civil partnership, etc.)
Identity document	Identity document issued in an EU Member State (including Poland) or a passport issued by a country not being an EU Member State.
Subscriber	Natural person or Legal person whom a qualified certificate has been issued to on the basis of the present certification policy (whose data are entered in the certificate as the certificate owner's data). Natural person or Legal person whom a qualified time stamp or a signature/seal validation report has been issued to.
CPR	CenCert Central Point of Registration.

Term/acronym	Description
DN	DN identifier – *Distinguished Name* – identifier of PKI entity according to syntax as defined in X.500 series standards.
NCCert	Root of the national PKI system kept by the National Bank of Poland, on the basis of the competent minister's authorization.
TSL	EU Trust service Status List – lists issued electronically by the European Commission (list of lists) and EU member countries (including Poland) containing information about entities providing trust services, their status (whether "qualified" or not) and verification data of "tokens" issued by entities providing trust services (namely verification of qualified certificates, time stamps, etc.).
CRL	*Certificate Revocation List*-List of revoked certificates, issued, electronically sealed and published by CenCert.
OCSP	*Online Certificate Status Protocol* - services informing about the certificate revocation status, as asked by the person trusting the certificate.
Private key	Data used for submission of electronic signature/stamp.
Public key	Data used for verification of electronic signature/stamp, usually distributed in the form of a certificate.
HSM	*Hardware Security Module* – a device having the functionality of generating cryptographic keys and using the private key for generating electronic signatures/electronic seals (e.g. when issuing certificates, CRL lists).
QSCD	*QSCD – Qualified Signature Creation Device* – device for submission of electronic signature or electronic seal, which a) can be found on the list referred to in Article 31.2 eIDAS, or b) is deemed as such, pursuant to Article 51.1 of eIDAS.
rSign	(Remote sign) Electronic signature provided by CenCert on behalf of the owner of the certificate.
PSD2	(Directive (EU) 2015/2366 Of The European Parliament And Of The Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC)

2. Principles of information distribution and publication

CenCert publishes the following information:

- CenCert's current public key/keys (in the form of certificates issued by NCCert).
- Current CRL list
- Archive CRL list.
- Current certification policy, marketing materials, current messages etc.

CenCert does not publish Subscribers' certificates. Archive CRL lists are published as compressed archives containing CRL lists from a given period.

The above information is available in a repository available at **www.cencert.pl**
by means of HTTP/HTTPS protocol.

3. Identification and authentication

This chapter describes the principles of identification and authentication used by CenCert at operations that require such operations – in particular when issuing certificates and changing certificate status.

3.1. Structure of names assigned to the Subscribers

Subscribers are identified in certificates using distinguished identifiers (Distinguished Names) defined in ITU Recommendations, series X.500.

CenCert confirms the identity and credibility of the information entered in the certificate, in accordance with the provisions of chapter 3.2, but does not verify the rights to use the objects of intellectual property rights, in particular copyright works, registered trademarks or registered patents, is not responsible for unauthorized use of the above items and is not a party to such disputes. In the case of loss by the Subscriber of the right to use a given name or other symbol shown in the certificate, they are obliged to notify about this fact in order to revoke the certificate due to invalidity of the data contained in the certificate.

3.1.1 Certificate for electronic signature

3.1.1.1 Certificate for electronic signature containing personal data

The Subscriber's distinguishing identifier consists of the following attributes:

Country (countryName) = PL

first name (givenName) = <name or first names of the Subscriber>

Surname (sureName) = <surname of the Subscriber>

Serial number (serialNumber) = <additional data identifying the Subscriber, for ex. PESEL (Personal ID Number), NIP (Tax Identification Number) or identity document no.>

Common name (commonName) = <Subscriber's name>

Serial number may be written in the form consistent with ETSI EN 319 412-1. In this case, the relevant certificate extension indicates compliance with this standard.

Common name may contain the Subscriber's full name or its informal identification - e.g. friendly form of name, pseudonym, nickname, surname written differently than in formal documents etc.

In the case of Subscribers having several names, it is acceptable to enter only one name to the certificate

DN identifier may contain the following optional additional attributes (fields may occur many times):

Professional position (title)

Organization (organizationName)

Name of organizational unit (organizationalUnitName)

Address (fields from set: **postalAddress, localityName, stateOrProvinceName, postalCode)**

Professional position may define the professional position, but also rights to perform a particular profession (e.g. along with the number of the license), authorization to perform certain activities.

Attribute *Organization* contains the name of the entity which the Subscriber is related to, compliant with the entry in the relevant register, records, statute or other document of this type, appropriate for the type of the entity.

Attribute *Name of organizational unit* contains the name of organisational unit being part of the organization whose name appears in attribute *Organization*.

Address fields contain address data used for better identification of the entity whose name appears in attribute Organization. This does not have to be a complete postal address of the entity.

3.1.1.2 Certificate for electronic signature containing a pseudonym

The Subscriber's distinguished identifier consists of the following attributes:

Country = <country>
Pseudonym = <nickname>
Common Name = <nickname>

The content of the "Pseudonym" field must not be misleading (in particular, give the wrong impression that the certificate belongs to a public or well-known person). The field must also not contain vulgar or offensive content.
The Common Name field has the same content as the Nickname field, possibly supplemented with an indication that the content of the field is a pseudonym (eg by a note "(pseud.)")..

DN identifier may contain the following optional additional attributes (fields may occur many times):
Organization (organizationName)
Name of organizational unit (organizationalUnitName)
Address (fields from set: **postalAddress, localityName, stateOrProvinceName, postalCode)**

Attribute *Organization* contains the name of the entity which the Subscriber is related to, compliant with the entry in the relevant register, records, statute or other document of this type, appropriate for the type of the entity.

Attribute *Name of organizational unit* contains the name of organisational unit being part of the organization whose name appears in attribute *Organization*.

Address fields contain address data used for better identification of the entity whose name appears in attribute Organization. This does not have to be a complete postal address of the entity.

3.1.2 Certificate for electronic seal

The Subscriber's distinguishing identifier consists of the following attributes:

Country (countryName) = <country>
Organization (organizationName) = <official name of the entity >

Organization identifier (organizationIdentifier) = <identifier of the entity>

Common name (commonName) = <entity name>

Field *Organization* contains the official name of the organization, consistent with the entry in a relevant register, records, statute or other document of this type appropriate for the type of the entity.

Organization identifier contains an identifier of an organization (for ex. NIP, i.e. Tax Identification Number) in the form consistent with ETSI EN 319 412-1.

Common name should contain the name most often used by the organization. It does not have to be the official name, consistent with a record in the register or statute.

DN identifier may contain the following additional attributes (fields may occur many times):

Name of organizational unit (organizationalUnitName)

Address (fields from set: **postalAddress, localityName, stateOrProvinceName, postalCode)**

Attribute *Name of organizational unit*- contains the name of organizational unit being part of the organization whose name appears in attribute *Organization*.

Address fields contain address data used for better identification of the entity whose name appears in attribute Organization. This does not have to be a complete postal address of the entity.

3.1.3 Certificate for website authentication

The Subscriber's distinguishing identifier consists of the following attributes:

CountryName = < Subscriber's country>

GivenName = <Subscribrer’s given name or names>

SureName = < Subscribrer’s family name>

albo

organizationName = <official name of the entity >

organizationIdentifier = <identifier of the entity>

commonName = < name / names of domains used by the Subscriber >

The DN identifier may also contain other attributes that identify the Subscriber (e.g. additional fields for the postal address, the name of the organizational unit, etc.)

The organization identifier is written in a form compliant with ETSI EN 319 412-1.

3.2. Subscriber's Authentication when issuing the first certificate

Verification of the identity of a **natural person** applying for a certificate - is performed by the Registration Inspector or a notary public on the basis of a valid identity document or on the basis of a valid qualified signature. If the certificate is to contain the organisation's data, an authorization is required (unless the authorization of a given person in the organization results from the statute, registration records of the organization, etc.). If the certificate is to contain specific data specifying e.g. professional qualifications, a document confirming the qualifications is required.

The person or persons acting on behalf of the **Legal Entity** applying for the certificate must be authorized to represent the Legal Entity in accordance with the provisions of the relevant register or the statute of the organization, or on the basis of a power of attorney issued by persons authorized to represent. Verification of the identity of the person receiving the certificate (if the keys are generated by CenCert) or submitting the public key to be included in the certificate is performed by the Registration Inspector on the basis of a valid identity document or an electronic signature.
If the certificate is to contain specific information regarding the Subscriber's specific rights (e.g. fulfilling the roles specified in the PSD2 Directive), the rights are checked on the basis of relevant documents or registers.

The information on DNS addresses of domains included in the website authentication certificate is checked by confirming that the domain is managed by the person submitting the application.

In the case of electronic signature certificates containing a pseudonym instead of the first and last name (see section 3.1.1.2), CenCert does not verify the rights to use a given pseudonym or its uniqueness, without prejudice to the provisions regarding the rules for including the organisation's data in the certificate. CenCert stores data that allows the identification of a specific natural person using a given certificate containing a pseudonym.
CenCert has the right to refuse to issue a certificate with a pseudonym if, in CenCert's opinion, the content of the entry in the certificate violates the conditions specified in section 3.1.1.2).

3.3. Subscriber's Authentication when issuing subsequent certificates

Another certificate for electronic signature can be made on the basis of a valid qualified signature. The new certificate contains the same Subscriber's identification data as the previous certificate. The right to use any additional certificate attributes (e.g. organization details, professional qualifications, etc.) is not re-checked. The scope of these additional data, recorded in the new certificate, may also be limited in relation to the data contained in the previous certificate, these data may also be updated or supplemented, however, when supplementing or updating, authorization or confirmation of this data is required, as when issuing the first certificate.

There is no simplified procedure for seal certificates, nor for certificates for website authentication.

3.4. Methods of Subscriber's authentication when reporting certificate invalidation, suspension and suspension repealing claims

Revocation or suspension of a certificate for electronic signature is executed:

- on the website of CenCert, on the basis of the full name and the password of the Subscriber, agreed when issuing the certificate or
- on the basis of an application signed by the Subscriber.

Suspension of a certificate for electronic signature is repealed on the basis of the application signed by the Subscriber.
Revocation of a certificate for electronic signature containing data of the organization the Subscriber is related to will be also performed at a request issued by this organization, signed by authorized persons.

Invalidation of a certificate for electronic seals is executed at a request issued by the Subscriber (a Legal Person), signed by an authorized person.

Revocation of the certificate containing data specific to PSD2 will also be implemented upon a request from an authorized financial market supervisory institution.

The certificate status change request must be supplied in the form of a paper original or electronic document signed with a qualified signature.

3.5. Management of permissions to make stamps in remote mode

In the rSeal service, CenCert creates a seal on behalf of the Subscriber, at the request of the Subscriber, during the sealing session initiated by one of the persons authorized by the Subscriber.
Each session is initiated using a valid qualified signature of an authorized person. An authorized person also has the option to terminate an active sealing session at any time.

The subscriber may manage the personal data of persons authorized to manage sessions by submitting paper or electronic applications, signed by an authorized (by the contract or official records) person. Applications should be sent in accordance with the contact details provided in chapter 1.3.

CenCert guarantees the execution of a correctly submitted application (and signed by the appropriate person / person) by the end of the next business day after receiving the application.

4. Certificate life cycle – operational requirements

4.1. Application for issuing a certificate

Notification of the need for issuance of a certificate for electronic signature may be submitted by a natural person (entity) applying for issuing a certificate or an entity financing the service, in any form accepted by a given Point of Registration. Such role is also met by a contract or order for the service of issuing certificates, containing data of the persons whom the certificates are to be issued to.

In the event when personal data for issuing the certificate are not transferred by the person whom they relate to, the transferring entity is responsible for obtaining the consent from the person the data relate to, to transferring the personal data in order to execute the trust service.

The Registration Inspector, having the data of the person applying for the certificate, prepares an application for issuing the certificate and the transfer protocol. If the issuance of the certificate does not involve the handover of a smartcard, the application for certificate issuance may also be prepared and sent in a different way, without the participation of the Registration Inspector.

The request contains information on conditions of trust service provision, including limitations of liability of CenCert – by indicating the binding version of *the Qualified trust services policy*. The request also includes required information and consent of the person applying for the certificate – in particular information and consent required by the regulations on Personal Data Protection and confirmation of assignment of databases used for verification of electronic signature, which are included in the issued certificate.
In the case a certificate for electronic seal – the application contains indication (full name, number of identity document) of a person authorised to receive the key for creating seals and/or key activation data.

In case of simultaneous purchase of the certificate to be signed and the electronic seal, on the same QSCD card:
1) In the application for issuing a certificate the person indicated as authorized to receive the QSCD card with the keys for generating seal must be the person purchasing a certificate for electronic signature (is must be the same person).
2) The Inspector generates on the same card - a pair of keys for placing the signature and a pair of keys for placing the seal.

In the case of issuing a qualified certificate to a qualified electronic signature/seal on the basis of a public key generated by the Subscriber, CenCert confirms the possession of the QSCD certificate by the device owned by the Subscriber. The application for issuing the qualified certificate is accompanied by a public key and relevant documents (including the SSCD / QSCD certificate of the device and subscriber's statements).

4.2. Processing the application

The application for a certificate may be processed on paper or in electronic form.
The application for issuing a certificate for electronic signature in paper form is signed by the person applying for the certificate in the presence of the Registration Inspector or a notary. An electronic application is signed by the person applying for the certificate (a qualified signature is required) using the qualified certificate already held by that person.

4.3. Issuing certificate

The signed application for certificate issuance is approved for execution by the Registration Inspector authorized to generate certificates. If automatic verification of the correctness of the application is possible (only applications in electronic form), the application may be approved by the CenCert computer system. After the application is approved, a certificate is generated.

After approval of the certificate application:
1) A qualified certificate is issued and sent to the Subscriber or made available to him in another way.
2) In the case of a signature or stamp "on the card" - a transport code is sent to the Subscriber to activate the card (the transport code file also includes the certificate).
3) In the case of the rSeal - the Subscriber is sent a certificate and a PIN for activating the seal creation key.

The activation of the smartcard is a one-time and irreversible process. Before activating the card, it is not possible to use the keys written on it to perform a signature or an electronic seal. By receiving an inactive electronic card, the Subscriber can be sure that the keys stored on it have not been used before.

4.4. Certificate acceptance

The Subscriber is obliged to verify and accept the certificate immediately upon receipt of the certificate and before its use (in particular before making the first signature verified using the certificate. In the case of untrue data contained in the certificate (in particular identification data of the Subscriber or data of the person or organization whose data are also included in the Subscriber's certificate), the Subscriber is obliged to immediately inform CenCert, in accordance with procedures valid when revoking certificates, in order to revoke the certificate and receive a new one, containing correct data.

Using a certificate containing false data exposes the Subscriber to penal liability.

4.5. Using key pair and certificate

4.5.1 Using certificate

Subscribers' certificates can be used solely to verify electronic signatures or electronic seals, or internet domain authentication, in accordance with this certification policy, subject to possible constraints stipulated in the certificate.

The only way to confirm the Subscriber's certificate validity in terms of possible revocation or suspension is to check certificate status on an appropriate CRL list or using the OCSP service.

The fact of not publishing a new CRL list in a given time cannot be used as the basis to imply no revocation of certificates.

4.5.2 Using private key

Private key connected with the Subscriber's certificate may be used only for goals resulting from the applications stipulated in the related certificate.

Private key for electronic signature should remain at the sole discretion of the Subscriber – the natural person whose data are placed in the certificate. It is not acceptable for the key to be used by another person.

Private key for electronic seal should remain at the sole discretion of the person or persons authorized by a given Legal Person.

In the case of a rSign or rSeal, the private sealing key is stored on CenCert's HSM and is used by CenCert exclusively to submit a signature or a seal on behalf of the Subscriber, at his/her request.

In the case of conceiving a reasonable suspicion that an unauthorized person has access to the private key, the Subscriber should immediately revoke the certificate related to the key (and if several certificates were associated with the key – all certificates should be revoked).

Specification of PIN number to smart card containing keys used for placement of qualified electronic signatures or seals may proceed only in a safe environment – that is on a computer which only persons trusted by the Subscriber have access to, protected against any type of hazardous software, in particular using relevant antivirus software and firewalls.
Terms of use the smart card for generating electronic signatures/seals:

- When signatory authentication is requested to perform digital signature, its PIN shall be submitted through a trusted channel (secure messaging) established between the signature creation application and the smart card prior to the signature computation.
- When PIN is modified it shall be modified under the sole control of its owner, i.e. the signatory and through a secure channel established with the signature creation application.
- The digital signature shall be executed under the sole control of the signatory and shall ensure that the data to be signed are issued from the signature creation application.
- The data to be signed shall be sent to the smart card through a trusted channel (secure messaging) established between the signature creation application and the smart card, after the signatory authentication.

In the event when the Subscriber's smart card contains, except for the data used for placement of qualified electronic signatures, also other data, in particular other private keys (e.g. key for e-mail encryption, key for login to the operating system etc.), the card should be organized in such a way that the card required specification of a separate PIN number in order to execute a qualified signature. PIN number for placement of electronic signatures/qualified seals should have another value than the codes starting other services available using the card.

In the case of signing or sealing using the HSM device owned by the Subscriber, the signing key activation data (eg PIN, password or activation cards) must be stored securely, with confidentiality safeguards, and entered into the HSM device in the manner provided for in documentation (in particular, certification documentation) of a given HSM device.

In the case of rSign and rSeal service, the Subscriber has the following duties:

- Ensures the confidentiality of data (received from CenCert) activating the private key for generating seals.
    - In particular: In the case of the remote signing/sealing session, key activation data is transferred to the CenCert server providing the rSign or rSeal service. Before transferring activation data, the Subscriber’s application must confirm establishing a secure transmission channel (TLS) with the CenCert server and correctly identify the CenCert server based on the SSL/TLS certificate. The

appropriate CenCert server certificate providing the stamping service is published at https://www.cencert.pl.

- Uses a reliable application that:
  - generates a cryptographic hash of data presented as data to be signed (which it intends to sign), in a form appropriate for the rSign or rSeal service;
  - attach to the signed or sealed data a seal created by the rSign or rSeal service or make this signature/seal available separately from the data.
- Ensures that the security and integrity of the elements of the system used for signing or sealing service, located on the Subscriber's side (i.e. outside the CenCert), is kept entirely under his/her control.
- Ensures that the signing/sealing application, located on the Subscriber's side (other than CenCert), ensures the confidentiality, integrity and authenticity of data sent between the end user and this application (including in particular confidentiality of all sensitive credentials and integrity and authenticity cryptographic hash from data to be signed).
- Ensures compliance with the document described in chapter 9.16 for rSign or rSeal respectively.

4.6. Certificate replacement

It is accepted to replace a valid qualified certificate without changing the Subscriber's private key – provided that the key's cryptographic safety is still sufficient for the new validity period of the certificate.

Replacement (renewal) of the certificate proceeds on the Subscriber's initiative. CenCert, if possible, will inform the Subscriber, before the expiry date of the certificate, about the need for its replacement using available contact details.

4.7. Certificate replacement combined with replacement of key pair

Certificate replacement combined with replacement of key pair is possible, meeting the requirements of chapter 3.2.

Replacement (renewal) of the certificate proceeds on the Subscriber's initiative. CenCert, if possible, will inform the Subscriber, before the expiry date of the certificate, about the need for its replacement using available contact details.

4.8. Change in the certificate content

Change in certificate content requires issuance of a new certificate containing new content. The previous certificate – provided that the data it contains have become outdated and contain untrue information about the Subscriber – is revoked.

The Subscriber is responsible for reporting the need for updates of data contained in the certificate as well as determination whether the data change implies the need for revoking the previous certificate.

CenCert is allowed to change the content of the certificate (that is, to issue a new certificate and revoke the old one) without re-authentication of the subscriber, for the same public key, in the case of corrections, obvious typographical errors or technical errors of the certificate. The Subscriber is immediately informed about the certificate correction.

4.9. Certificate revocation and suspension

The entity authorized to revoke the certificate is:

• Subscriber.

• The organization whose data is included in the certificate for electronic signature.

• For certificates containing data specific to PSD2 - the institution supervising the financial market, the data of which is entered in the certificate.

- • CenCert.

The certificate can be revoked only prior to the date of the end of its validity period. Invalidation of a certificate is irreversible – the invalidated certificate cannot become valid again.

The Subscriber and the organization whose data have been placed in the certificate for electronic signature, has the right to revoke the certificate for any reason.

The certificate Subscriber is obliged to immediately revoke the certificate when:

- he/she has lost exclusive control over the private key related to the certificate (e.g. he/she has lost the electronic card or the card has been destroyed, blocked, etc.),
- the data contained in the certificate are incorrect or outdated.

The organization whose data have been placed in the certificate for electronic signature is obliged to immediately revoke the certificate when:

- the data of the entity contained in the certificate are incorrect or outdated,
- a circumstance justifying placing data of an organization in the Subscriber's certificate (e.g. employee dismissal, change in the scope of duties, etc.) has ceased.

CenCert has the right to change the certificate status only in justified cases. In particular:

- CenCert may revoke a certificate containing a pseudonym, if it turns out that the pseudonym does not meet the conditions specified in section 3.1.1.2.,
- CenCert may suspend or revoke the Subscriber's certificate at the request of the organization that financed the issue of the certificate (applies to certificates issued on the basis of an agreement or framework agreement concluded between CenCert and a given organization),
- CenCert may suspend and then revoke the certificate in the absence of payment for the certificate issuance service by the Subscriber or the organization ordering the issuance of the certificate, after a prior unsuccessful call for payment within at least 14 days. A sufficient form of notification is an e-mail sent to the address provided for sending the invoice or to the Subscriber's e-mail address provided for issuing the certificate.

CenCert provides a possibility to apply for revocation, suspension or repealing suspension of a certificate in a 365/24/7 mode.

In the case of the certificate suspension – suspention lasts for a maximum of 7 days, then the certificate is revoked automatically.

According to Articles 28.5, 38.5 of eIDAS, the period of suspension is clearly indicated in the CenCert certificate database and the suspension status is visible, during the period of suspension, on the CRLs and OCSP tokens.

According to Article 24.3 of eIDAS-if CenCert decides to revoke the certificate, it registers such revocation of in its database concerning the certificates, and publishes information on the status of the certificate invalidation in due time, but in any case, within 24 hours, upon receipt of the application. Invalidation becomes effective immediately upon its publication.

Procedures associated with change in certificate status are located on CenCert website.

In the case of cancellation or suspension on the basis of the Subscriber's password – the operation is performed on the CenCert website, whose data can be found in Chapter 1.3.

The Subscriber is immediately informed on change in certificate status by e-mail.

4.10. Certificate status information services

CenCert informs about the certificate status using the CRL list and OCSP service.

The CRL list is issued at least once every 24 hours, with guaranteed availability of 99.95% on an annual basis.

In order to examine the status of the certificate revocation, it is required to:

- download the OCSP token for this certificate and check the certificate status saved in this token or
- download the CRL list issued after the time at which we examine the certificate validity and check the status of the certificate on CRL.

The validity of signatures under the OCSP token and the CRL list should be checked based on current TSL list.

OCSP replies and CRL lists contain correct information about revocations even after the period of certificate validity elapses.

CenCert publishes archive CRL lists at the latest after the end of validity of the key used to sign them.

4.11. End of trust service provision for the Subscriber

If not provided otherwise - the relationship between CenCert and the Subscriber or the financing entity regarding the performance by CenCert of the trust service consisting in issuing a qualified certificate ends with the expiry of the validity period specified in the certificate. In the case of time stamping - within 24 months after the time stamp is issued.

In the case of the remote sealing service (on behalf of the subscriber), the service period ends with the expiry of the certificate (revocation or expiration of the validity period).

In the case of qualified validation service for qualified electronic signatures/seals, the period of service provision is specified in the contract with the subscriber, and if the order concerns a single validation operation - within 24 months after issuing the validation report.

4.12. Entrusting and reproduction of private keys

CenCert does not entrust its private key to any entities.

In the case of the remote sealing service, the Subscriber entrusts CenCert with his private key. The entrusted key is not transferred by CenCert to anyone - it also cannot be transferred to the Subscriber.

5. Organizational, operational and physical protections

5.1. Physical protections

CenCert servers are located in air-conditioned server rooms, protected against flooding, equipped with a fire protection system, power outages, as well as an access control system and an alarm system for burglary and assault.

Physical access to CenCert server devices (including HSM devices) is possible only for authorized persons. Each access to devices is recorded.

CenCert is equipped with a backup center, located in a remote location from the primary center.

All data and devices essential for the security of CenCert and the services provided by it (in particular, electronic cards and other hardware components enabling the activation of the CenCert private key, access codes to devices, cards and systems, archiving media) are secured and available only to authorized persons .

5.2. Procedural protections

CenCert has the following functions having direct impact on provision of certification services:

Function name	Type of obligations
System administrator	Configuration of the CenCert system regarding certification policy, management of rights for the system operators. IT infrastructure management, making backups.
System operator	Constant operation of the data communications system, including making backup copies, management of rights (including certificates) of Registration Inspectors
Registration Inspector (registration officer)	Verification of Subscribers' identity, issuing orders to issue Subscribers' certificates, revoking Subscribers' certificates

Function name	Type of obligations
Audit Inspector	Analysis of records of registers of events in data communication systems used when providing the certification services
Safety Inspector (security officer)	Supervision over the implementation and application of all safe operation procedures when providing certification services, supervision over physical access to protected devices.

Substantially – every Registration Inspector is also a Revocation Inspector (revocation officer).

The function of the Safety Inspector cannot be combined with the function of the System Administrator or with the function of the System Operator. The function of the Audit Inspector cannot be combined with any of the remaining functions mentioned above.

The persons performing functions of Registration Inspectors can have various kinds of rights included in full rights of the Registration Inspector. In particular, some people performing this role may have the right only to confirm the identity of the Subscriber or only the right to revoke the certificates.

5.3. Personal protections

All persons performing at least one of the function listed in chapter 5.2 fulfil the following requirements:

- they have full capacity to be a party in legal acts,
- they have knowledge and skills necessary for work on a given position, regarding technology of provision of certification services, provided by CenCert.

All persons performing the said functions, before admission to perform their duties, are trained in the scope relevant for a certain work position, also with regard to procedures and regulations of work binding in CenCert and penal liability related to the provision of certification services.

In the case when a specific function is performed by the person cooperating with Enigma on the terms other than a contract of employment with Enigma, Enigma enters into a contract with this person or with the company where he/she is employed, specifying the rules of performing these functions for Enigma and the rules of responsibility.In the case of persons employed in

Enigma under a contract of employment, the liability of this person is stipulated by valid regulations of the Labour Code.

Regardless of a possible financial liability, people unreliably performing their obligations associated with the provision of certification services or not observing requirements imposed by regulations on trust services (in particular requirements about confidentiality, requirements with regard to issuance and revocation of certificates) are subject to penal sanctions defined in the Act.

5.4. Procedures of creating audit logs

CenCert provides recording of any significant events related to the execution of certification services provided by it.

The logs are protected against modification.

5.5. Archiving the records

CenCert archives the following paper and electronic records associated with provision of services:

- requests for issuing a certificate signed by the Subscribers,
- issued certificates and CRL lists,
- requests to invalidate a qualified certificate,
- service provision policy

- for 20 years from their generation.

5.6. Replacement of key pairs used to provide trust services

Generation and replacement of the CenCert key pair may take place on the scheduled dates or earlier.

Planned replacement of CenCert key pairs takes place

- no earlier than 8 years and no later than 6 years before the expiry of the current key pair – for RSA 4096 and ECDSA 256 keys, valid for 11 years.

5.7. Loss of private key confidentiality and action in the event of disasters

5.7.1 Loss of private key confidentiality

CenCert has relevant procedures valid in the case of loss of CenCert private key confidentiality or a reasonable suspicion that such an event has occurred.

In the case of compromising the key, these procedures stipulate in particular:

1. Reporting the incident in accordance with eIDAS, informing Subscribers about the situation and about the further action plan.
2. Producing new CenCert keys and reporting them to the competent minister in order to issue a new NCCert certificate and place on the TSL list.
3. If possible in the given situation (in particular when CenCert databases remain credible) – issuing new Subscribers' certificates for the keys held by the Subscribers, on the basis of new CenCert keys, with validity periods at least the same that the revoked certificates had.

In the case of loss of confidentiality of private keys entrusted by Subscribers (sealing service in remote mode), CenCert immediately revokes key certificates and informs the Subscribers about the situation.

5.7.2 Weakness of cryptographic algorithms

When it turns out that the cryptographic algorithms used by CA or the Subscribers, or their parameters, are insufficient for the intended use, CA shall notify all the Subscribers and shall make such information available publicly and plan revocation of the affected certificates. If possible, the certificates will be replaced with other ones, with the use of new cryptographic algorithms and/or their parameters.

5.7.3 Natural disasters

CenCert has contingency plans to ensure operation continuity, anticipating in particular unavailability and no possibility of functioning of the Basic Centre and/or Central Point of Registration and/or shutdown of the repository or OCSP services server.

5.8. End of operations

In the case of the intended end of operations with regard to qualified trust services, the Company's Board of Directors shall take every effort to ensure this activity's takeover by another qualified supplier of these services. If achieving such an agreement proves impossible, the Company's Board of Directors shall make the decision on planned end of CenCert operations.

The government body exercising supervision over provision of trust services shall be notified immediately about the intended end of operations, with at least 3-months' advance.

The following are also informed about the intended end of operations:

- Subscribers – with sufficient advance allowing them to purchase new certificates from a different qualified trust service provider and
- entities cooperating when executing trust services by CenCert (including those conducting Points of Registration) – in the time consistent with any concluded contracts.

In the period of finishing the operations, CenCert shall terminate all authorizations to act on behalf thereof (in particular with regard to the operations of Points of Registration)

After the end of the operations all issued certificates (being still within the term of validity) are revoked and, after issuing the last CRL list, CA private key is destroyed.

Documents and provisions for which archiving is required are transferred after the end of the operations to the entity indicated by the government body exercising supervision over provision of trust services.

In the case of finishing execution of only some of qualified trust services (and maintaining provision of the remaining qualified service or services) the above provisions shall respectively apply.

6. Technical protections

6.1. Generating and installing key pairs

6.1.1 Generating key pairs

The CenCert key pairs are generated by CPR personnel in accordance with the documented procedure, in presence of at least two persons performing functions related to implementation of trust services, including the Safety Inspector. A protocol shall be drawn up from the key generation ceremony.

Keys of Registration Inspectors, used for gaining access to the CenCert system, are generated independently by the inspectors or by CPR personnel, on an electronic card meeting the requirements of QSCD.

Subscribers' keys are generated by the Registration Inspector or by the Subscriber, for certificates for qualified signatures or seals - on an electronic card (or HSM) meeting the QSCD requirements.

Subscriber keys for rSign / rSeal services are generated by the CenCert system on the HSM.

When generating keys, all requirements resulting from the certification documentation of a given HSM device (or smart card) apply. CenCert checks compliance with these requirements also in the case of generating keys on the device owned by the Subscriber.

6.1.2 Delivering private key to the Subscriber

The electronic card which the Subscriber's keys are saved on is technically secured in a way enabling placement of electronic signature only after the card is activated by introducing a transport code. The transport code is delivered to the Subscriber in a different shipment than the card itself. Card activation is one-time and irreversible.

The electronic card is delivered to the Subscriber or (in the case of a seal – to the authorized person) by the Registration Inspector, after identity verification.

In the case of the rSeal service, the person authorized by the Subscriber receives from the registration inspector (in person), on a removable media (e.g. USB stick), a file containing, among others, password protecting the private key ("Passphrase"). The password is a random number with a length of 128 bits and is stored in an encrypted form. The key to decrypt the

password (also 128 bits long) is sent by the CenCert server to the e-mail address of the authorized person, after issuing the certificate for sealing.

In the case of the rSign service, the Subscriber receives the password securing the private key ("Passphrase") saved, along with other data, in the form of a QR-code on the Certificate Application. This password is a random number of 128 bits long and is stored in an encrypted form. The key to decrypt the password (also 128 bits long) is sent by the CenCert server to the Subscriber's mobile application, after the installation of this QR-code in the application and after confirmation by the CenCert server that no one has obtained this key before (the QR code is one-time). The certificate for the private key is issued only after confirming the correct installation of the data in the Subscriber's mobile application on the basis of a one-time code, so it is not possible for another person to have the access code to the Subscriber's private key.

6.1.3 Delivering public key of the Subscriber

If a certificate for the qualified seal is generated on the basis of a public key, the key is delivered to CenCert CPR by the Registration Inspector or the CenCert System Administrator, present during the pair of keys generation by the Subscriber on the QSCD device.

In the case of generating a certificate for an advanced seal or website authentication, the public key is delivered to CenCert in a form signed with a qualified signature or it is delivered together with the certificate application.

6.1.4 Delivering CenCert public key

The CenCert public key is available in the form of a certificate issued by NCCert and registration on the national TSL list.

A reference to the national TSL list is available at the CenCert website.

6.1.5 Cryptographic parameters of keys

The CenCert RSA keys have the length of 4096 bits.

The CenCert ECDSA keys have the length of 256 bits.

The Subscribers' keys have the length of 2048 bits (RSA keys) or 256 bits (ECDSA).

Infrastructure keys:

- RSA keys to protect communication between CenCert and Points of Registration have the length of 2048 bits or longer, ECDSA keys (if used) – 256 bits or longer,
- Registration Inspectors' keys have the length of 2048 bits (RSA).

All keys of the ECDSA algorithm are generated in the domains defined in NIST standards, using prime numbers.

For the submission of seals by CenCert (including the signing of certificates, signature/seals validation reports and other data structures issued by CenCert), SHA-2 hash algorithms are used.

6.1.6 Purpose of using key

CenCert private key for sealing certificates - can be used only to seal certificates and CRL lists pursuant to the present certification policy. The corresponding public key serves solely to verify certificates and CRL list.

CenCert private key for sealing time stamps - can be used only for this purpose. The corresponding public key serves solely to verify time stamps.

CenCert private key used for sealing OCSP tokens - can be used for this purpose only. The corresponding public key is used only for the verification of OCSP tokens.

CenCert private key used for sealing signatures/seals validation reports - can be used for this purpose only. The corresponding public key is used only for the verification of the reports.

Private keys of the Subscribers can be used only for placing qualified signatures or electronic stamps.

6.2. Protection of private keys

CenCert private keys are generated and processed in HSM devices having one of the certificates:

1) Common Criteria (standard ISO/IEC 15408) for level EAL4 or safer,
2) FIPS PUB 140-2 for level 3 or safer.
3) QSCD.

Subscribers' private keys for qualified signatures / seals and private keys of Registration Inspectors are generated and processed on smart cards or HSM meeting the QSCD requirements.

CenCert does not impose any requirements on the device (or software) for generating and processing the Subscribers' private keys for qualified certificates for advanced (non-qualified) seals and qualified certificates for website authentication. In such cases, the risk analysis and selection of appropriate solutions is on the part of the subscribers.

Backup copies of CenCert private keys are generated with the same security requirements as for keys in the original location of these keys.

Backup copies of Registration Inspectors' private keys are not generated.

Backups of private keys Subscribers used for rSign and rSeal service are created in a manner consistent with the HSM device certificate. Key copies are stored in protected rooms and stored for a maximum of 7 days.

The Subscribers' or the CenCert private keys are not archived.

Activation of the CenCert keys requires simultaneous presence of at least two authorized persons.

The Subscribers' and Registration Inspectors' private keys (on QSCD cards) are activated by a PIN code.

In the case of rSign and rSeal services, Subscriber's private keys are activated by means of mechanisms provided for in the HSM certification documentation.

Destroying the Subscribers' and Registration Inspectors' private keys is performed by the holder of the given card, by logical key removal from the electronic card or physical destruction of the card. In the case of the remote sealing service - the key is destroyed by removing the encrypted key from the HSM device and the key storage locations in encrypted form (including from backup copies).

CenCert private keys, used for provision of trust services, are destroyed by a committee in accordance with the documented procedure.

CenCert does not impose formal requirements for testing a manifesting electromagnetic radiation effect of devices or rooms where CenCert's, Registration Inspectors' and the Subscribers' keys are generated and processed.

6.3. Other key pair management aspects

The validity period of Subscribers' certificates is maximum 5 years.

The validity period of Registration Inspectors' certificates is maximum 2 years.

After cancellation or expiry of the last certificate associated with the private key for rSign or rSeal service, the key is destroyed (including deleted from backup copies) within 7 days.

6.4. Activating data

CenCert adopted and complies with the documented procedures of handling all the activating data. General principles on which detailed procedures are built are as follows:

1. Activation of the CenCert key requires simultaneous presence of at least two persons performing functions associated with provision of trust services.
2. Any activating data should be remembered or securely recorded by people routinely using them. The passwords are archived in a protected manner.
3. Activating data necessary – at least potentially – in both locations (Basic and Spare Centre), are saved in two copies and stored in both locations.

Subscribers' private keys for rSign / rSeal services are stored in an inactive mode, except for signing / sealing sessions. Activation of the key requires each time the Subscriber initiates a seal-creation session, including: entering the password protecting the key ("Passphrase"). In the case of rSeal, it is additionally required to approve the session with a qualified signature of one of the persons authorized by the Subscriber. The stamping session ends after the expiry of the time for which it was established or at any time - at the Subscriber's request. In the case of rSign, starting a signing session requires the use of a mobile device with an application that meets the conditions described in the document listed in chapter 9.16.

The password protecting the key for rSign / rSeal services is transferred to the Subscriber by CenCert before issuing the certificate. CenCert applies technical and procedural safeguards to ensure that the only possessor and owner of the password securing the key for placing the signature/seal is the Subscriber. Loss of access by the Subscriber to the password means the technical impossibility of placing the signature/seal (the password cannot be reproduced or read from the CenCert system).

6.5. Computer protections

CenCert carries out regular susceptibility tests and penetration tests, of the used IT system, not less frequently than every 6 months. Results of tests are not published.

All operations to be performed on computers and servers of CenCert can be made after prior authentication and control of rights. Performed operations are saved in event logs.

Part of the software used to perform the signature and seal validation service may be installed in the IT infrastructure of the user of the validation service, in the form of a secured Docker or virtual server, provided and managed by CenCert. The user of the validation service is obliged

to provide a safe environment for running this software, in particular to protect it against unauthorized access, as well as to refrain from any interference with the supplied software, including attempts to break the security measures applied by CenCert.

6.6. Protections related to IT system life cycle

CenCert has adopted documented procedure for making modifications or changes in the data communication system. In particular, this applies to tests of new software versions and/or using the existing databases for this purpose. These principles guarantee continuous operation of the data communication system, the integrity of its resources and preservation of data confidentiality.

The procedure guarantees testing new software versions in the testing environment. For implementation of any works in the test environment, it is not allowed to used private CenCert keys meant to provide trust services.

6.7. Computer network protections

Servers used by CenCert keys to provide certification services pursuant to the present policy are connected by means of logically separated, two-segment internal network, separated from the external network with firewalls.

6.8. Time stamping

Issuing time stamps, as well as time stamping of certificates, certifying statements, CRL lists, time stamping of events related to the signature and seal validation service and entries in the devices and software log is done using the indication of current time from timers built in the devices or the workstations.

Workstation timers are synchronized using NTP protocol with the UTC(pl) time shared publicly on the certificate of the Head Office of Measures.

Synchronization ensures time accuracy not smaller than 1s.

CenCert guarantees availability of the time stamping service at the level of 99,9% measured in a yearly perspective.

Timestamping services are provided in response to a timestamping request, in accordance with the provisions of Chapter 7.4

7. Profile of certificates, CRL lists and OCSP tokens

7.1. Profile of certificates and certifying statements

7.1.1 Distinguished Names

DN ID connected with provision of the service of issuance of qualified certificates for electronic signatures and seals:

Country (countryName) = ***PL***
Organization name (organizationName) = ***Enigma Systemy Ochrony Informacji Sp. z o.o.,***
Common name (*commonName*) = ***CenCert QTSP CA***
organizationIdentifier **=** ***VATPL-5261029614***

DN IDs connected with provision of the service of issuance of qualified time stamps:

Country (countryName) = ***PL***
Organization name (organizationName) = ***Enigma Systemy Ochrony Informacji Sp. z o.o.,***
Common name (*commonName*) = ***CenCert QTSP TSA***
organizationIdentifier**=** ***VATPL-5261029614***

Country (countryName) = ***PL***
Organization name (organizationName) = ***Enigma Systemy Ochrony Informacji Sp. z o.o.,***
Common name (*commonName*) = ***CenCert QTSP TSA ECC***
organizationIdentifier**=** ***VATPL-5261029614***

DN ID connected with provision of the service of issuance of qualified certificates for website authentication:

Country (countryName) = ***PL***
Organization name (organizationName) = ***Enigma Systemy Ochrony Informacji Sp. z o.o.,***
Common name (*commonName*) = ***CenCert QTSP WEB CA***

organizationIdentifier= ***VATPL-5261029614***

DN ID connected with provision of the service of qualified validation service for qualified electronic signatures/seals:

Country (countryName) = ***PL***
Organization name (organizationName) = ***Enigma Systemy Ochrony Informacji Sp. z o.o.,***
Common name (*commonName*) = ***CenCert QTSP QVal***
organizationIdentifier= ***VATPL-5261029614***

DN IDs associated with provision of trust services, for keys generated and saved in the national TSL before the effective date of this policy:

Country (countryName) = ***PL***
Organization name (organizationName) = ***ENIGMA SOI Sp. z o.o.***
Common name (*commonName*) = ***CenCert Centrum Certyfikatów Kwalifikowanych***
Serial number (serialNumber) **= *Nr wpisu:* 11**

Country (countryName) = ***PL***
Organization name (organizationName) = ***ENIGMA SOI Sp. z o.o.***
Common name (*commonName*) = ***CenCert Centrum Kwalifikowanych Znaczników Czasu***
Serial number (serialNumber) **= *Nr wpisu:* 12**

7.1.2 Profile of subscribers' certificates

CenCert issues certificates in a format of X.509 v.3 consistent with RFC 5280.

Numbers in issued certificates are pseudorandom and unique within a trust service, identified by the CenCert distinguishing identifier. Uniqueness of certificate numbers is provided by the software generating certificates along with the used databases.

CenCert applies the following identifiers of cryptographic services: sha256-with-RSA, sha384-with-RSA, sha512-with-RSA, sha1-with-RSA[1], sha256-with-ecdsa, sha384-with- ecdsa,

[1] The algorithm SHA-1 is used only for verification, in seals and signatures generated before July 2, 2018

sha512-with-ecdsa. The ECDSA algorithm is used and accepted for eliptic curves domains defined in NIST standards.

Extensions of qualified certificates of Subscribers:

Extension	**Description/value**	**critical?**
AuthorityKeyIdentifier	abbreviation from public key, CA	NO
SubjectKeyIdentifier	abbreviation from the Subscriber's public key	NO
KeyUsage	`nonRepudation` – for certificates for electronic signatures and seals `digitalSignature, keyEnciphering` – for website authentication certificates	YES
extendedKeyUsage	for website authentication certificates Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	YES
CertificatePolicies	1) `{1.3.6.1.4.1.10214.99.1.1.1.4}` or (only for certificates issued with the use of CA keys introduced to use before the effective date of this policy) `{1.2.616.1.113681.1.1.10.1.1.2}`	NO
basicConstraints	empty sequence (determination that the Subscriber is the final user and cannot issue certificates)	YES
crlDistributionPoints	contains locations of the current CRL	NO
qcStatement	`esi4-qcStatement-1` Declaration that the certificate is qualified within the area of EU id-etsi-qcs-QcCompliance {0.4.0.1862.1.1}	NO

Extension	Description/value	critical?
qcStatement	`esi4-qcStatement-4` Declaration that the private key connected with certificate is in the QSCD device id-etsi-qcs-QcSSCD {0.4.0.1862.1.4} It does not appear in certificates for advanced (non-qualified) seals and in certificates for website authentication	
qcStatement	`esi4-qcStatement-6` Declaration meaning a sort of a certificate id-etsi-qct-esign {0.4.0.1862.1.6.1}– for certificates for electronic signature id-etsi-qct-eseal {0.4.0.1862.1.6.2}– for certificates for electronic seal id-etsi-qct-web {0.4.0.1862.1.6.3} – for website authentication certificates	NO
qcStatement	`esi4-qcStatement-5` Indication (URL) for statements (PDS - *PKI Disclosure Statements*) id-etsi-qcs-QcPDS {0.4.0.1862.1.5} URL indicating PDS	NO
qcStatement	`id-etsi-qcs-semanticsId-Natural {0.4.0.194121.1.1}` indicates compliance of the serialNumber construction of DN identifier with the syntax and semantics defined in ETSI EN 319 412-1 for certificates for natural persons	NO, extension optional
qcStatement	`id-etsi-qcs-SemanticsId-Legal {0.4.0.194121.1.2}` indicates compliance of the serialNumber construction of DN identifier with the syntax and semantics defined in ETSI EN 319 412-1 for certificates for legal entities	NO

Extension	Description/value	critical?

qcStatement	Only for PSD2 certificates:
	
	`etsi-psd2-qcStatement {0.4.0.19495.2}`
	Oznaczenie instytucji nadzoru finansowego (NCAName, NCAId) oraz jedna lub więcej ról zdefiniowanych w PSD2, zgodnie z ETSI TS 119 495:
	- `PSP_AS`
	`id-psd2-role-psp-as {0.4.0.19495.1.1}`
	- `PSP_PI`
	`id-psd2-role-psp-pi {0.4.0.19495.1.2}`
	- `PSP_AI`
	`id-psd2-role-psp-ai {0.4.0.19495.1.3}`
	- `SP_IC`
	`id-psd2-role-psp-ic {0.4.0.19495.1.4}`
		NO

Authority Information Access –	*id-ad-caIssuers* indication of URL for location of the CA certificate issued by NCCert (HTTP protocol)	NO
Authority Information Access –	*id-ad-ocsp* indication of URL for OCSP server (HTTP protocol)	NO, extension optional

7.1.3 Certificates to sign OCSP tokens, certificates of infrastructure keys and test certificates

Certificates to sign OCSP tokens have extensions

- *KeyUsage->* digitalSignature - critical
- *extendedKeyUsage-> id-kp-OCSPSigning* (see RFC 5280) – non-critical
- *id-pkix-ocsp-nocheck* - non-critical.

Certificates of infrastructure keys (system access keys of Registration Inspectors, as well as for communication protection) are not qualified certificates – they do not have proper extensions of QCStatements. They have, on the other hand, extension ExtKeyUsage

{1.3.6.1.4.1.10214.2.1.1.2} or {1.3.6.1.4.1.10214.2.1.1.3} proving that these are infrastructure certificates used only under the CenCert system and cannot be used beyond this system.

Test certificates have identical structure as production certificates, provided that their DN identifier is built of fields "TEST" (or "TEST TEST", TEST2", "TEST <characters of other alphabets>", etc.) in all places meant for text data (first and last name, common name etc.) and sample numbers (1234…) in places meant for numerical data (PESEL (Personal ID Number), NIP (Tax Identification Number), etc.).

7.2. Profile of CRL lists

CenCert issues CRL lists in a format consistent with Recommendation X.509:2000 version 2. of the format.

The CRLs are sealed with the SHA-2 hash algorithm.

Extensions

Bay	**Description/value**	**critical?**
extensions		
AuthorityKeyIdentifier		NO
keyIdentifier	Hash of the public key	
cRLNumber	successive number of the CRL list issued in CenCert	NO

The CRL lists may contain other extensions, marked as non-critical.

7.3. Profile of OCSP

Demands consistent with RFC 6960 are acceptable. The demand content is sent and the reply is downloaded using the HTTP protocol.

The OCSP service address is included in the certificate extension (see section 7.1.2).

The certificate server reply is consistent with the RFC 6960 standard. For inquiries about unknown certificate number, service returns the value *unknown*. The service returns information about revocations regardless of the certificate validity date.

The OCSP token is marked with a seal placed using a key serving only for this purpose and contains a certificate of this key, issued using a CenCert key for issuance of certificates.

7.4. Profile of time stamp

RFC 3161 timestamping requests are accepted, authenticated in one of the following ways:

- using the "http basic authentication" mechanism and the "login, password" parameters entitling to obtain timestamps, or
- electronically signed for authentication, in accordance with the PKCS#7 standard, using a certificate authorized to obtain timestamps.

The http and https protocols are used to send the timestamping requests and to download timestamps, but the client should use the http protocol only if his/her system does not support https and when he/she uses the mode with signed timestamping requests (the client should never initiate a connection with the unsecured http protocol when he intends to use the login/password mode).

If the time stamping demand (according to RFC 3161) has an optional attribute *ReqPolicy*, it should contain the identifier "{2 5 29 32 0}"(any policy). Optional attribute *Extensions* may occur but is not processed by CCK system.

For signed timestamping requests - attribute *Version* of signature under the request (according to PKCS#7) should contain the value of "1". Attribute *Certificates* should contain the list of certificates, consisting only of a certificate (consistent with the X.509v3 certificates) of the key used for signing the time stamp request. Attribute *SignerInfos* should contain the list of electronic signatures, consisting of exactly one signature. Optional attributes of signature *SignedAttrs* and *UnsignedAttrs* not are processed by the CenCert system.

The time stamping server reply to a correctly formulated stamping request is consistent with standards RFC 3161 and ETSI EN 319 422 and is marked with an advanced seal placed with a CenCert private key for sealing time stamps. The seal under the time stamp includes, among others, date and time, as well as data sent by the person requesting the services (cryptographic hash from the time-stamped data).

8. Audit

CenCert is subject to audits in accordance with Article 20 of eIDAS.

9. Miscellaneous

9.1. Fees

CenCert collects fees for provision of its services according to the price list valid at a given time.

CenCert does not collect fees for invalidation, suspension or revocation of the certificate, as well as for access to public CenCert key and the published (current and archive) lists of revoked certificates.

9.2. Financial liability

Liability of the CenCert Certification Centre is defined in Article 13 of eIDAS.

The Certification Centre, as a qualified provider of trust services, is responsible for damage caused intentionally or due to negligence to a natural person or legal person in connection with default in meeting the obligations specified in eIDAS, subject to limitation of liability specified in chapter 9.8 below.

The intention or negligence CenCert is presumed, unless CenCert can demonstrate that the damage mentioned above resulted from the intended action or negligence of CenCert.

9.3. Confidentiality of information

Principles of protection of confidentiality of the information related to the provision of certification services are specified in the Act of trust services and electronic identification, as well as in the Act on protection of personal data.

CenCert treats as Confidential Information all information related to the services provided thereby, except for the following information:

- Certification policy in the currently binding versions,
- Public CenCert key,
- List of revoked certificates, OCSP tokens,
- Certificates of infrastructure keys,

- Current information, intended for publication (such as price list of services, commercial offer, current messages, contact details).

9.4. Personal data protection

CenCert processes the personal data of subscribers in accordance with

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and the Act of Personal Data Protection of 10 May 2018.

CenCert has implemented and fulfils appropriate procedures ensuring protection of personal data.

Subscribers are informed, at signing the contract, about processing of their personal data by CenCert and about their rights resulting from it.

9.5. Protection of intellectual property

Enigma Systemy Ochrony Informacji Sp. z o.o. has full right to administer proprietary copyrights pertaining to this Certification Policy.

Enigma Systemy Ochrony Informacji Sp. z o.o. allows using the policy (including printing and copying) by the Subscribers and other users of certification services, for the purposes related to the use of certificates, OCSP tokens and time stamps issued by CenCert.

9.6. Granted guarantees

Not applicable

9.7. Exemptions from guarantees granted by default

CenCert does not grant to the Subscribers any guarantees granted by default, except for guarantees which may result from the binding regulations.

Any guarantees granted by CenCert have to be granted in a written form, otherwise they are not valid.

9.8. Liability restrictions

9.8.1 General provisions

CenCert is not liable for damages resulting from failure by the Subscriber to comply with the rules set out in this policy.

CenCert, providing trust services, is not responsible for the correct operation of the software used by the Subscriber and the correctness and adequacy of technical and organizational security measures applied by the Subscriber.

Total financial liability of ENIGMA SOI Sp. z o.o. under provision by CenCert of certification services cannot exceed 1 000 000 EUR. The amount of one-time compensation under incorrect use of the certificate issued by CenCert cannot exceed 250 000 EUR.

9.8.2 Detailed provisions related to the services of issuing qualified certificates and the service of making a signature/seal on behalf of the Subscriber (rSign/rSeal)

CenCert is not liable for damages resulting from:

1) using the certificate not in line with the scope specified in the policy indicated in the certificate,
2) untrue data contained in the certificate, stated by the recipient of trust services using this certificate, unless the damage was a result of default on due diligence by the supplier of trust services,
3) storage or using, by recipients of trust services, of the private keys for submission of electronic signature, electronic seal or authentication of websites - or data protecting these keys - in a manner not ensuring their protection against unauthorised use, in particular failure to comply with the obligations arising from the provisions of Chapter 4.5.2 of this policy.

CenCert not responsible for ensuring that the issued certificate will be appropriate for the needs of the Subscriber or that it will be correctly functioning in the system in which the Subscriber wants or needs to use it.

In the case of shortening the validity period of certificates through the fault of the CenCert, the liability of CenCert is limited to reimbursement of the cost of issuing the certificates, in proportion to shortening the validity period.

CenCert is not liable for the consequences of revoking a certificate containing a pseudonym, if, after issuing the certificate, it turns out that the pseudonym does not meet the conditions specified in section 3.1.1.2, and this fact was not known to CenCert at the time of issuing the certificate.

CenCert is not liable for unavailability of the OCSP service, provided that in the unavailability period certificate status information services work correctly, on the basis of the CRL list, in accordance with the declaration of availability specified in chapter 4.10.

The Certification Centre is not liable for unavailability of the current CRL provisioning service, provided that the unavailability period does not violate the declarations of availability of the service specified in chapter 4.10.

When providing the rSign, rSeal services, CenCert is not liable for the correctness of calculating the cryptographic hash of the data to be signed/sealed, nor for the cryptographic hash sent to the CenCert system corresponds to the data that the Subscriber intends to sign/seal, and also is not liable for the security of processing, outside the CenCert system, the password securing the private key used for signing/sealing, nor for the Subscriber's management of the rights of persons authorized to initiate the sealing session, including for reporting changes in entitlements to the CenCert personnel well in advance.

CenCert is neither responsible for punctual handling of the certificate status change request (invalidation, suspension or suspension repealing), nor for handling the request in general – if it has not been delivered to CenCert to the address indicated in chapter 1.3, intended for sending certificate status change requests (traditional or e-mail address, depending on the form of the application).

CenCert is not responsible for the timely handling of an application for a change in the authorization of persons to establish a seal session in remote mode (authorization, deletion of authorization, change of data), or for the fact that the application will be served - if it has not been delivered to CenCert on indicated in Chapter 1.3 address (traditional address or email, depending on the form of the application).

CenCert is not liable for loss of the Subscriber's access to the private key used for placing electronic signatures or seals, resulting from a blockade of the electronic card due to a wrongly entered PIN and/or PUK number, exceeding the fixed limit of failed attempts, about which the Subscriber has been informed.

CenCert is not responsible for the loss of access to the private key used in rSeal service, caused by the loss of the password to activate the key.

CenCert is not responsible for the loss of access to the private key used to perform the signature in the remote mode (rSign), caused by the loss of "backup" data saved by the mobile application, or the loss of the PIN to the mobile application, or the loss of access to SMS messages sent to the defined in CenCert Phone number.

9.8.3 Specific provisions related to the timestamping service

CenCert is not responsible for the unavailability of the timestamping service, unless the period of unavailability does not violate the service availability declaration specified in section 6.8.

CenCert is not responsible for the correct calculation of the cryptographic hash from the data to be time stamped.

9.8.4 Detailed provisions related to the signatures/seals validation service

CenCert is not responsible for whether the validated signatures/seals meet the requirements of the recipient of the service, in particular it is not responsible for whether the persons who signed it were properly authorized.

Electronic signatures and seals may be placed in a way that may mislead the person validating the document - e.g. they may cover only a part of the document, they may be placed under documents containing active content, changing the way the document is presented, etc. CenCert exercises due diligence in detecting and informing the recipient of the validation service about potential security problems, but does not guarantee and is not responsible for detecting any such cases.

If the validation service is provided using CenCert software, partially installed in the infrastructure managed by the Subscriber (see description in Appendix A, chapter A.2.3), in the event of a violation of the integrity of this software, validation reports issued with its use may be considered incompatible with the input documents for the validation service (see the description of how to confirm whether the validation report corresponds to the input document, Annex A, chapter A.1.2.1). CenCert is not responsible for any damages that may result from this.

If, at the customer's request, the validation service is performed on the basis of the date of creation of the signed document entered by him - CenCert is not responsible for the correctness

of this date and the resulting correctness of the validation report. Appropriate information is included in the validation report.

CenCert is not responsible for any consequences that may occur due to the use of incorrect, i.e. non-compliant with the regulations or applicable standards, information such as CRLs, OCSPs, time stamps - published by other qualified providers of qualified services - used in the implementation of the validation service.

9.9. Assignment of compensation claims

CenCert has concluded a valid civil liability insurance contract for damage caused to the recipients of certification services, in accordance with the Act on trust services.

9.10. Transitional regulations and period of validity of certification policy

This certification policy applies to trust services products (certificates, timestamps, validation reports, etc.) issued during its validity period.

The policy can be applied from the moment of approval (before the effective date) to the implementation of trust services for testing and audit purposes.

The qualified validation service of qualified electronic signatures and seals is performed after indicating it on the TSL list.

9.11. Determination of the manner and addresses for delivery of letters

Any letters associated with the current activity of CenCert should be delivered at the Central Registration Point.

Any letters can also be delivered to the address of the registered office of Enigma Systemy Ochrony Informacji Sp. z o.o.

9.12. Changes in the certification policy

The certification policy management principles are described in chapter 1.5.

9.13. Settlement of disputes

All disputable matters concerning provisions of trust services of CenCert, including complaints, should be addressed to Enigma Systemy Ochrony Informacji Sp. z o.o. at biuro@enigma.com.pl.

9.14. Applicable law

Operation of the certification subsystem is governed by the law of the Republic of Poland and the European Union.

9.15. Legal basis

Rules of action of CenCert are consistent with the binding law and, in particular, with the regulations contained in the following legal acts:

- Regulation of the European Parliament and of the Council (EU) No. 910/2014 of 23 July 2014 and Commission Implementing Decisions (EU) issued on its basis.
- The Act of 5 September 2016 on trust services and electronic identification.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and the Act of Personal Data Protection of 10 May 2018.
- The Penal Code Act.
- The Copyright Act.

9.16. Miscellaneous

CenCert provides potential customers with rSeal service, before the service begins, description of remote sealing service interface.

CenCert provides potential developers of a mobile application for the rSign service, after signing an appropriate contract, a description of the security and functional requirements for the mobile application.

Appendix A - Policy Provisions Specific to the Qualified Validation Service of Qualified Electronic Signatures and Seals

A.1 Introduction

A.1.1 Overview

This document describes the provisions of the Policy For Qualified Trust Services specific to the qualified validation service of qualified electronic signatures and seals ("Service"). The provisions of the main policy document also apply to the Service.

The structure of the annex is based on the standard ETSI TS 119 172-1 V1.1.1.

The method of performing the validation service is compliant with the standard ETSI TS 119 441.

A.1.2 Business or Application Domain

A.1.2.1 Scope and boundaries of signature policy

The service is used to validate qualified electronic signatures and seals in all applications of a qualified electronic signature and seal. The service can also be used to validate selected types of advanced electronic signatures and seals. The product of the Service is a validation report containing the results of validation of signatures and seals contained in the document or attached to the document.

In the case of confirming the validity of a signature or seal, the validation report clearly defines the type of validated signature/seal, in particular whether it is a qualified signature or a qualified seal.

In order to confirm whether a given validation report corresponds to a given document (whether it constitutes evidence confirming the validity status of signatures or seals of a specific document), it is necessary to:

1) confirm the compliance of the cryptographic hash from the document file(s) with the hash(s) placed in the validation report AND
2) confirm the compliance of the hash(s) from individual parts of the document, covered by individual signature(s)/seal(s), with the hash(s) included in the validation report (XML form of the validation report).

CenCert provides a free application on its website, available to all interested parties, which allows to confirm the compliance of a given document with a given validation report.

In some cases, explicitly stated in the validation report, validation is based on evidence of the existence of a signed document on the part of the user of the Service (see section A.3.2.3). In this case, the report confirms the validity of the signature/seal only in conjunction with the appropriate proof of existence of the document held by the user.

The subject of operation of the Service is a document of any digital content, containing electronic signatures or seals, or signatures and seals attached to the document as signatures/external seals and saved in other files.

The validation result of a given signature or seal is specified as:

1) TOTAL-PASSED – which means that the validity of the signature/seal has been confirmed,
2) INDETERMINATE – which means that the signature/seal is mathematically correct, but - with the input data currently available for the validation service - there is no way to confirm the validity of the signature/seal, or
3) INVALID – which means that it is not possible to confirm the validity of the signature/seal (e.g. a mathematically incorrect signature, the certificate was revoked before the signature was made, etc.).

According to Art. 32(1), Art. 40 eIDAS, the validation process of a qualified electronic signature or seal confirms the validity of the qualified electronic signature or qualified electronic seal, provided that:

a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I or a qualified certificate for electronic seal complying with Annex III,
b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;
c) the signature validation data corresponds to the data provided to the relying party;
d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party;
e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;
f) the electronic signature was created by a qualified electronic signature creation device;
g) the integrity of the signed data has not been compromised;
h) the requirements provided for in Article 26 for signatures and Article 36 for seals were met at the time of signing.

According to Art. 32.2, Art. 40 eIDAS, the system used for validating the qualified electronic signature shall provide to the relying party the correct result of the validation process and shall

allow the relying party to detect any security relevant issues. In particular, the Service performs the activities described in section A.1.2.3 (providing data on the context of the signature/seal operation), A.3.2.3 (possible uncertainty of evidence related to the lifetime of the signed document), A.3.1.3 (relationship between signatures and signed data), A.3.4.2 (cryptographic algorithms).

A.1.2.2 Domain of applications

The scope of use of the Service is not limited.

Validated documents can be used both in B2B, B2C, Gov2B, Gov2C relationships, as well as contractual, financial, medical, consumer relationships, within one organization or relationships between organizations, domestic and international.

A.1.2.3 Transactional context

The service is used to validate documents in various contexts.

If the validated signature contains an indication of its context in accordance with the qualifiers defined in the ETSI 101 733 standard (e.g. the role of the signer Proof of origin, Proof of creation, etc.) [2], this fact is clearly visible in the validation report.

A.1.3 Document and policy(ies) names, identification and conformance rules

A.1.3.1 Signature policy document and signature policy(ies) names

See chapter 1.2.

A.1.3.2 Signature policy document and signature policy(ies) identifier(s)

See chapter 1.2.

A.1.3.3 Conformance rules

See chapter 1.

A.1.3.4 Distribution points

See chapter 1.3

[2] Signature context flags are defined in the ETSI TS 101 733 standard for CAdES signatures, but are referenced in the relevant standards and are also valid for other signature formats (e.g. in the ETSI TS 101 903 standard for XAdES signatures)

A.1.4 Signature policy document administration

See chapter 1.5

A.1.5 Definitions and Acronyms

DA - Driving Application – part of the CenCert software used to perform the Service, generally installed in the IT infrastructure of the Service client (in order to avoid submitting to CenCert documents with validated signatures/seals, due to the confidentiality of the documents), responsible for calculating representations (cryptographic hashes) of data covered by signatures/seals.

SVA – Signature Validation Application – Signature Validation Application - a part of the CenCert software used to perform the Service, operating on CenCert servers, responsible, among others, for examining the validity of relevant qualified certificates at specific moments of time, issuing decisions as to the result of validation of signatures/seals and documents, issuing a validation report.

POE – Proof od Existance – Evidence that the signature/seal already existed at the time (it was made at this time or earlier).

A.2 Signature application practices statements

This clause includes the set of policy and security practices requirements that applications DA and SVA meets when validating signatures/seals.

A.2.1 Legal driven policy requirements

See chapter 9.15.

A.2.2 Information security (management system) requirements

Enigma Systemy Ochrony Informacji Sp. z o. o. (owner of the CenCert trademark) has implemented and maintains an information security management system, certified for compliance with the requirements of the ISO 27001 standard. This system also includes the provision of trust services under the "CenCert" brand, including signature and electronic seal validation services. As part of this management system, the Integrated Management System Policy was defined, which is certified in accordance with ISO 9001 and ISO 27001 standards and is available on the website.

Information on securing the CenCert computer network interface is specified in section 6.7 of the policy. The connection between the DA and the SVA is carried out over a secured transmission channel (TLS), with server authentication based on a TLS certificate. The DA

component is also authenticated using the "http basic authentication" mechanism with a sufficiently long password.

The provisions regarding the security of the IT system are included in section 6.5 of the policy.

The provisions on ensuring application integrity in the context of updates are also specified in section 6.5 of the policy. In addition, CenCert maintains a list of applications used to provide the Service, along with specifying the version numbers.

DA component applications are distributed by CenCert to customers using technology that ensures that DA is not available to customers for modification, e.g. in the form of an operating system image for a virtual machine.

Data backups on the CenCert side (applies to SVA) are regularly made on encrypted media, which are stored in a different location than the servers. Data is also replicated between the Primary Center and the Backup Center.

CenCert supervises the results of audits in accordance with the requirements of ISO 9001 and ISO 27001, any possible non-compliances and other audit remarks are recorded along with the course of their handling (including decisions made, status of proceedings, possibly analysis of causes, etc.).

A.2.3 Signature Creation and Signature Validation processes requirements

The service is performed automatically by the following programming components:

- SVA, which includes the rVer Server service and auxiliary services,
- DA, rVer Gateway, which includes the rVer Client service and user interface components.

SVA is located on CenCert servers and communicates with DA and repositories of revocation information published by trust service providers. SVA performs part of the validation process consisting in checking the correctness and status of certificates used to affix a given signature/seal and issues a final report. SVA maintains a central database for the validation service.

For the client of the validation service, SVA is only available via DA. The communication protocol between SVA and DA is compliant with ETSI TS 119 442.

DA, as a rule, is intended for installation in the IT infrastructure of the client of the Service (ensuring that the data contained in validated documents does not leave the client's infrastructure). DA provides a web interface for the Service user, which allows for ordering validation processes and reading the status of the operation and its result (validation reports). DA also provides management of local users of the Service and provides a rest interface that allows for integration with the service client's systems.

It is also possible to configure the service with a DA instance installed in the CenCert infrastructure. In this case, documents for validation and reports are transferred in a different way (e.g. via a website or encrypted e-mails, etc.).

SVA provides the user with a validation report, via DA, in an asynchronous manner - when it collects all the necessary data. If, at the time of submission of the document for validation, all information regarding the potential revocation of the certificate at the time of signature or seal is not yet available, SVA automatically re-attempts the validation periodically, without charging the user with additional activities or costs. The validation report is prepared when the SVA collects the required information from third-party trust service providers or, failing that, after the maximum time allowed for the service, which is no less than 24 hours.

CenCert guarantees the availability of the Service at the level of 99.9% measured on an annual basis. The above indicator does not include interruptions in the operation of the Service resulting from reasons beyond CenCert (in particular, due to reasons related to the client's IT infrastructure in which DA is installed).

The service supports the following signature/stamp formats:

• XAdES (XML Advanced Electronic Signatures compliant with the ETSI TS 103 171 v.2.1.1),

• PAdES (PDF Advanced Electronic Signatures compliant with the ETSI TS 103 172 v.2.2.2),

• CadES (CMS Advanced Electronic Signatures compliant with the ETSI TS 103 173 v.2.2.1),

• ASiC (ASiC Electronic Signatures compliant with the ETSI TS 103 174 v.2.2.1).

All signature/stamp levels are supported: B-Level (Basic), T-Level (Timestamped), LT-Level (Long Term) and LTA-Level (Long Term with Archive time-stamps).

Signatures/seals can be integral with the signed content or detached (in a separate file). Validated documents may contain multiple signatures/stamps, including countersignatures.

In order to confirm the validity of a signature or seal, the Service must have information on the revocation of certificates from the relevant date, therefore there are certain limitations as to the possibility of confirming the validity (TOTAL-PASSED) of historical signatures/seals. The following can be confirmed:

- signatures/seals made using certificates for which the validity period has not yet expired at the time of signature/seal validation,
- signatures/seals made using certificates whose validity period has already expired at the time of signature/seal validation, provided that:
    - they are properly maintained LTA-Level signatures/seals or

- these are signatures/seals made with the use of certificates - issued by Polish qualified trust service providers (included in the Polish TSL list) - whose validity period expired no earlier than December 28, 2020 or
- to a limited extent, depending on the availability of historical information on revocations - these are signatures/stamps made using certificates issued by qualified trust service providers included in the TSL list of one of the EU countries, the validity period of which expired no earlier than December 28, 2020 r.

The integrity and origin of the validation report are guaranteed by the advanced electronic seal of the Service, made using a key belonging to CenCert and a certificate used to perform the Service, included in the national TSL list.

The validation report is issued in XML and PDF formats. The report in the form of XML complies with the standard ETSI TS 119 102-2 v 1.3.1.

Both forms of the validation report are marked with the same identifier and constitute a set. Both forms of the report are consistent with each other, in particular they contain the same validation statuses of signatures/seals. The PDF form of the report is optimized for readability in natural language. The XML form is mainly machine-readable and contains more details about the validation process.

The report contains an unambiguous indication of the input data of the Service, including data identifying files consisting of a document and a signature/signatures (including representations of data in the form of cryptographic hashes) and data on the information on revocations used.

A.2.4 Development & coding policy requirements

As far as possible, CenCert participates in available interoperability tests of software used to validate signatures/seals, organized by ETSI and/or other European Union or national organizations. The test results are analyzed in detail and may be the basis for changes in the implementation of the service.

A.2.5 General requirements

No additional requirements specified.

A.3 Business scoping parameters

A.3.1 BSPs mainly related to the concerned application/business process

A.3.1.1 BSP (a): Workflow (sequencing and timing) of signatures

Not applicable.

A.3.1.2 BSP (b): Data to be signed

The service does not impose any restrictions on the format or size of the signed data. However, the file size limitation may result from technical reasons, including the IT infrastructure provided by the user for DA installation.

A.3.1.3 BSP (c): The relationship between signed data and signature(s)

The validation report contains information if a given signature does not cover the entire document, where the signature may include the content of the document directly (referring to a hash from the document) or indirectly (referring to an earlier signature or timestamp that refers to a hash from the document) .

Supported signature formats and levels are specified in chapter A.2.3.

A.3.1.4 BSP (d): Targeted community

Not applicable.

A.3.1.5 BSP (e): Allocation of responsibility for signature validation and augmentation

As part of the Service, signature/seal validation is performed. Along with the validation service, depending on the arrangements with the client, the possibility of extending the signature to more advanced forms (timestamping, etc.) may be available, but these options are not part of the validation service and may be initiated for a given document by the client.

A.3.2 BSPs mainly influenced by the legal/regulatory provisions associated to the concerned application/business process

A.3.2.1 BSP (f): Legal type of the signatures

The service is intended for the validation of qualified electronic signatures and seals. It also enables validation of selected types of advanced electronic signatures/seals, clearly informing about the type of signature/seal, in particular whether it is a qualified signature/seal.

The service confirms the validity of the signature/seal, but it does not cover whether a specific type of signature/seal is legally appropriate for a given scope of activities or a given document, and whether the number of signatures/seals is appropriate or whether the persons are properly restrained, etc.

A.3.2.2 BSP (g): Commitment assumed by the signer

See chapter A.1.2.3.

A.3.2.3 BSP (h): Level of assurance on timing evidences

The following time sources can be used as evidence of the existence of a given signature/seal at a specific point in time (POE):

1) Qualified timestamps,

2) Own time of the CenCert server providing the Service, synchronized with UTC(pl) time in accordance with the provisions of section 6.8 of the policy.

3) The time entered by the client of the validation service.

In the case described in point 3) above, the fact of collecting the time when the signed document existed from the client of the Service is clearly recorded on the validation report, along with the information that the validation report is proof of the signature/seal validity only in conjunction with proof of the document's existence at a certain time, which the proof lies with the service client.

A.3.2.4 BSP (i): Formalities of signing

Not applicable.

A.3.2.5 BSP (j): Longevity and resilience to change

Validation reports are sealed with the CenCert key used to perform the Service, to which the certificate recorded on the TSL list is related, with a validity period ending not earlier than 8 years from the date of issuing the validation report.

Validation reports are kept by CenCert for 10 years from the date of issue

A.3.2.6 BSP (k): Archival

Not applicable.

A.3.3 BSPs mainly related to the actors involved in creating/augmenting/validating signatures

A.3.3.1 BSP (l): Identity (and roles/attributes) of the signers

The validation report is sealed with the CenCert key used to perform the Service. Certificate identification data are specified in chapter 7.1.1.

The entity that made the signature or seal subject to validation is identified on the validation report by presenting the full content of the DN identifier, including in particular:

1) for an electronic signature based on a qualified certificate:
    a. name, surname
    b. nickname (if the certificate contains a nickname)
    c. content of the DN "serial number" field
2) for an electronic seal based on a qualified certificate:
    a. the name of the organization,
    b. name of the organizational unit (if provided)
    c. content of the DN "serial number" field.

A.3.3.2 BSP (m): Level of assurance required for the authentication of the signer

The validation report is sealed automatically by the IT system used to perform the Service. The software of this system is approved as part of an audit carried out in accordance with art. 20(1) eIDAS.

A.3.3.3 BSP (n): Signature creation devices

The key for signing the validation report is placed on hsm in accordance with the provisions of chapter 6.2 of the policy. Key activation is carried out in accordance with the provisions of chapter 6.4.

A.3.4 Other BSPs

A.3.4.1 BSP (o): Other information to be associated with the signature

No provisions included.

A.3.4.2 BSP (p): Cryptographic suites

The validation report is sealed using the signature/seal algorithms and their parameters specified in section 6.1.5.

In terms of validated signatures/seals, the following cryptographic algorithms are accepted:

1) The following signature/seal cryptographic algorithms are accepted: RSA (PKCS#1 v.1.5, RSA-PSS), ECDSA, DSA.
2) The following hash functions used to issue a qualified certificate and CRL lists, OCSP tokens, timestamps are accepted:
    a. SHA-224, SHA-256, SHA-384, SHA-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512,
    b. SHA-1 but only for seals/signatures issued before July 1, 2018.
3) The following hash functions applied to the validated signature/seal are accepted:
    a. SHA-224, SHA-256, SHA-384, SHA-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512,
    b. SHA-1, but only for signatures/seals issued before July 1, 2018 (see chapter A.3.2.3 for determining the time of signing/seal)

A.3.4.3 BSP (q): Technological environment

No provisions included.

A.4 Requirements / statements on technical mechanisms and standards implementation

No provisions included.

A.5 Other business and legal matters

No provisions included.

A.6 Compliance audit and other assessments

The provisions of chapters 8 and 6.5 apply.