QUALIFIED TRUST SERVICES PROVIDER "CENCERT"

PKI Disclosure Statement

Version: 2.0

Document Card:

Document title	PKI DISCLOSURE STATEMENT
Document owner	ENIGMA Systemy Ochrony Informacji Sp. z o.o.
Version	2.0
Document status	**Approved**
Date of approval	2024-09-02
Number of pages	12

approved by:

Version	approved by
2.0	The Director of CenCert Department of Enigma Systemy Ochrony Informacji Sp. z o.o.

Table of contents

1 TSP contact info 4

2 Certificate types, validation procedures and usage 4

2.1 Certificate types 4

2.2 Validation procedures 4

3 Certificate usage 5

4 Reliance limits 5

5 Obligations of subscribers 5

6 Certificate status checking obligations of relying parties 7

7 Limited warranty and disclaimer / Limitation of liability 7

7.1 General provisions 7

7.2 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) 8

8 Applicable agreements, CP 9

9 Privacy policy 9

10 Refund policy 9

11 Applicable law, complaints and dispute resolution 9

12 TSP and repository licenses, trust marks, and audit 9

13 Abbreviations andTerms 9

1 TSP contact info

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

Centralny Punkt Rejestracji *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, see also https://www.cencert.pl/jak-uniewaznic-certyfikat/

2 Certificate types, validation procedures and usage

2.1 Certificate types

CenCert issues:

- qualified certificates for implementation of qualified electronic signature,
- qualified certificates for implementation of qualified or advanced electronic seal,
- qualified certificates for website authentication,

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 certificates for website authentication - 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.).

All certificates have profile compliant with X.509 v3 standard.

Private keys for qualified electronic signatures/seals are generated and stored on the eIDAS QSCD devices.

2.2 Validation procedures

Verification of identity of the person applying for a certificate for electronic signature is performed by the Registration Inspector on the basis of a valid Identity document (personal visit, “face-to-face”). If the certificate is to contain data of the organization, authorization is required (unless authorization of a given person in the organization results from the articles of association, registry records of the organization etc.) If the certificate is to contain specific data determining e.g. professional licenses, a document confirming the licenses is required.

Person or persons acting on behalf of a Legal Person applying for the certificate for electronic seal must be authorized to represent the given Legal Person in accordance with the provisions of a relevant register or the articles of association of the organization, or on the basis of a power of attorney, issued by persons authorized to represent.

In the case of:

a) companies operating under the commercial law, associations, foundations and other organizations whose registration data are included in the National Court Register,
b) businesses and civil law partnerships whose registration data can be found in the Central Registration and Information on Business (CEIDG),

- the rights to represent are verified by the Registration Inspector on the basis of the publicly available databases of from the National Court Register or CEIDG.

In other cases, documents proving qualifications to represent the given Legal Person should be delivered in the form of an authenticated copy.

Identity check of a person receiving electronic seal (i.e. a key for creating seals and / or key activation data) is performed by the Registration Inspector on the basis of valid Identity documents (personal visit, "face-to-face").

Authentication may be also made basing on previous qualified certificate (on a valid qualified signature of the person applying for the certificate). In such case a new certificate will contain the same data identifying the Subscriber (a natural person) as the data in the previous certificate.

3 Certificate usage

Subscribers' certificates can be used solely to verify electronic signatures, electronic seals or authenticate web pages, 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 Reliance limits

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.

5 Obligations of subscribers

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 (server signing/sealing 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 of the actual CP, for rSign or rSeal respectively.

6 Certificate status checking obligations of relying parties

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.

7 Limited warranty and disclaimer / Limitation of liability

7.1 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.

7.2 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 actual CP (see chapter 5 above).

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 of the actual CP, 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 of actual CP. Cencert 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 of actual CP.

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 of actual CP, 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 of actual CP 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.

8 Applicable agreements, CP

See for applicable documents: https://www.cencert.pl.

9 Privacy policy

See for applicable documents: https://www.cencert.pl.

10 Refund policy

If a subscriber or a relying party is not satisfied with the services, they may request certificate revocation and fee refund only if CenCert did not fulfiled its obligations and duties specified in the subscriber agreement and the CP.

A legitimate claim may be submitted by e-mail to biuro@cencert.pl.

11 Applicable law, complaints and dispute resolution

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

12 TSP and repository licenses, trust marks, and audit

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

13 Abbreviations andTerms

Abbreviation /Term	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
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 has been issued to.
CPR	CenCert Central Point of Registration.
DN	DN identifier – *Distinguished Name* – identifier of PKI entity according to syntax as defined in X.500 series standards.
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.
Remote seal **rSeal**	Electronic sealing service provided by Cencert on behalf of the signer, where signer’s key is located on qSCD hsm in Cencert and is managed remotely by the signer.

Remote Sign **rSign**	Electronic signature service provided by CenCert on behalf of the signer, where signer’s key is located on qSCD hsm in Cencert and is managed remotely by the signer.