NBP Narodowy Bank Polski

# National Certification Centre — Certification Policy

**OID: 1.3.6.1.4.1.31995.3.3.3**
**Version 3.3**

NBP Security Department
Warsaw, 2018

## Table of contents

## Disclaimer for the Relying party

Before relying on an eSignature or an eSeal which is verified by a Trust Service Provider Certificate issued in accordance to this National Certification Centre Certification Policy, please read the rules contained in this document.

In particular, make sure that you have read and understood any and all disclaimers of Narodowy Bank Polski, as well as the requirements for the Subscriber and the Relying party.

# 1. Introduction

## 1.1 Overview

The National Certification Centre – the main certification office in the national trust infrastructure created by NBP to implement the tasks entrusted to NBP by the minister in charge of digital affairs pursuant to Article 11(1) of the Act of 5 September 2016 on Trust Services and Electronic Identification (Journal of Laws 2016, item 1579 as amended) hereinafter referred to as the "Act on Trust Services". The National Certification Centre is not a Qualified Trust Services Provider.

The functioning of the National Certification Centre is regulated by the law applicable in the Republic of Poland, including in particular the Act on Trust Services and appropriate implementing regulations.

The provisions of this National Certification Centre Certification Policy, hereinafter referred to as the "Policy", are applicable for NBP, Subscribers and the Relying party. The Policy is applicable in the process of the creation and management of Trust Service Providers issued by the National Certification Centre. The Policy specifies in particular: types and scope of usage of Trust Service Provider Certificates, rules concerning issuance thereof, participants of the process of issuing Trust Service Provider Certificates, their responsibility and duties as well as the rules for the revocation of issued Trust Service Provider Certificates. This Policy also fulfils the role of the National Certification Centre Certification Code of Conduct.

This Policy is based on the recommendations of ETSI EN 319 401 Electronic Signatures and Infrastructures; General Policy Requirements for Trust Service Providers and ETSI EN 319 411-1 Electronic Signatures and Infrastructures; Policy and security requirement for Trust Service Providers issuing certificates; Part 1: General requirements. The core policy for this document is the NCP+ policy, in other words the Normalized Certificates Policy requiring a secure cryptographic device.

## 1.2 Document Name and Identification

| | |
|---|---|
| **Document name** | National Certification Centre — Certification Policy |
| **Document version** | 3.3 |
| **Document status** | Working |
| **Effective date** | 02.07.2018 |
| **OID:** | 1.3.6.1.4.1.31995.3.3.3 |

| | |
|---|---|
| **Core policy** (in accordance with ETSI EN 319 411-1) | NCP+ |
| **Location** | http://www.nccert.pl/files/PC_NCCert_EN.pdf |

## 1.3 Definitions

For the purposes of this Certification Policy the following terms shall denote as follows:

1) **Certificate** – a certificate for eSignature, a certificate for eSeal, or a certificate of website authentication.

2) **Certificate for eSignature –** electronic attestation which assigns eSignature validation data to a natural person and confirms at least the name and last name or a pseudonym of that person.

3) **Certificate for eSeal** – electronic attestation which assigns eSeal validation data to a legal person and confirms at least the name of that person.

4) **Trust Service Provider Certificate** – a certificate used in the verification of advanced eSignatures or advanced eSeals referred to in Annex II letter g, Annex III letter g, Annex IV letter h to Regulation (EU) No 910/2014 of the European Parliament and of the Council of the European Union of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/ECor a certificate used in verification of Trust Services provided by qualified Trust Service Providers.

5) **Certificate of the National Certification Centre** – a certificate for verification of eSeals which National Certification Centre appends to the Trust Service Provider Certificates.

6) **Certificate for website authentication** – electronic attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued.

7) **eSeal creation data** – unique data which is used by the creator of the eSeal to create an eSeal

8) **eSignature creation data** – unique data which is used by the signatory to create an eSignature.

9) **Validation data** – data that is used to validate an eSignature or an eSeal.

10) **Trust Service Provider** – a natural or a legal person who provides one or more Trust Services, either as a qualified or as a non-qualified Trust Service Provider.

11) **eIDAS** – Regulation (EU) No 910/2014 of the European Parliament and of the Council of the European Union of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

12) **Electronic Time-Stamp** – data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time.

13) **Conformity Assessment Body** – a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a Qualified Trust Service Provider and the Qualified Trust Services it provides.

14) **Qualified certificate for eSeal** – a certificate for an eSeal that is issued by a Qualified Trust Service Provider and meets the requirements laid down in Annex III to eIDAS.

15) **Qualified Certificate for eSignature** – a certificate for eSignatures that is issued by a Qualified Trust Service Provider and meets the requirements laid down in Annex I to eIDAS.

16) **Qualified Certificate for Website Authentication** – a certificate for website authentication that is issued by a Qualified Trust Service Provider and meets the requirements laid down in Annex IV to eIDAS.

17) **Qualified Trust Service Provider** – a Trust Service Provider who provides one or more Qualified Trust Services and is granted the qualified status by the supervisory body.

18) **Qualified Electronic Time Stamp** – an electronic time stamp which meets the following requirements:

    a. it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;

    b. it is based on an accurate time source linked to Coordinated Universal Time;

    c. it is signed using an advanced eSignature or sealed with an advanced eSeal of the Qualified Trust Service Provider, or by some equivalent method.

19) **Qualified eSeal** – an advanced eSeal which is created by a qualified eSeal creation device and which is based on a qualified certificate for eSeals.

20) **Qualified eSignature** – an advanced eSignature that is created by a qualified eSignature creation device and which is based on a qualified certificate for eSignatures.

21) **Qualified eSeal Creation Device** – an eSeal creation device that meets the appropriate requirements laid down in Annex II to eIDAS;

22) **Qualified eSignature Creation Device** – an eSignature creation device that meets the appropriate requirements laid down in Annex II to eIDAS;

23) **Qualified Electronic Registered Delivery Service** – an electronic registered delivery service which meets the following requirements:

    a. it is provided by one or more qualified trust service provider(s);

    b. it ensures with a high level of confidence the identification of the sender;

    c. it ensures the identification of the addressee before the delivery of the data;

    d. the sending and receiving of data is secured by an advanced eSignature or an advanced eSeal of a Qualified Trust Service Provider in such a manner as to preclude the possibility of the data being changed undetectably;

    e. any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data;

    f. the date and time of sending, receiving and any change of data are indicated by a Qualified Electronic Time Stamp.

24) **Qualified Trust Service** – a Trust Service that meets the applicable requirements laid down in eIDAS.

25) **CRL** – a list of revoked Trust Services Provider Certificates.

26) **National Certification Centre** – the main certification office in the national trust infrastructure created by NBP to implement the tasks entrusted to NBP by the minister in charge of digital affairs pursuant to Article 11(1) of the Act on Trust Services and Electronic Identification.

27) **Supervisory Body** – minister in charge of digital affairs.

28) **eSeal** – data in electronic form which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.

29) **Creator of a Seal** – a legal person who creates an eSeal;

30) **eSignature** – data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.

31) **Signatory** – a natural person who creates an eSignature.

32) **Service Provision Policy** – a named set of rules, in particular such as certification policy, which applies to a specified group of entities or applications with security requirements common for this group.

33) **Product** – hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of Trust Services.

34) **Legislation on Trust Services** – eIDAS together with implementing acts and the Act on Trust Services together with implementing acts.

35) **Register** – a register of Trust Service Providers referred to in Article 3 of the Act on Trust Services.

36) **Repository** – the website www.nccert.pl, where in particular trust service providers' certificates, lists of revoked Trust Service Provider Certificates, Polish Trusted List and "National Certification Centre Certification Policy" are published.

37) **Regulation** – Regulation of the Minister of Digital Affairs of 5 October 2016 on the Domestic Trusted List.

38) **Relying party** – a natural or legal person that relies upon an electronic identification or a Trust Service.

39) **Subscriber** – a Qualified Trust Services Provider who received a Trust Service Provider Certificate;.

40) **Electronic Seal creation device** – configured software or hardware used to create an eSeal.

41) **Electronic signature creation device** – configured software or hardware used to create an eSignature.

42) **Electronic registered delivery service** – a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations.

43) **Trust Service** – an electronic service normally provided for remuneration which consists of:

    a. the creation, verification, and validation of eSignatures, eSeals or electronic time stamps, electronic registered delivery services and certificates related to those services; or

    b. the creation, verification and validation of certificates for website authentication; or

    c. the preservation of eSignatures, seals or certificates related to those services

44) **Validation** – the process of verifying and confirming that an eSignature or a eSeal is valid.

45) **Advanced eSeal** – an eSeal which meets the following requirements:

   a. it is uniquely linked to the creator of the seal;

   b. it is capable of identifying the creator of the seal;

   c. it is created using eSeal creation data that the creator of the seal can, with a high level of confidence under its control, use for eSeal creation;

   d. it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.

46) **Advanced eSignature** – an eSignature which meets the following requirements:

   a. it is uniquely linked to the signatory;

   b. it is capable of identifying the signatory;

   c. it is created using eSignature creation data that the signatory can, with a high level of confidence use under his sole control;

   d. it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

47) **Trusted List** – a list of Trust Sservice Providers referred to in Article 22 (1) of eIDAS.

48) **Certification Request** – a file in PKCS#10 format containing, among others information, a distinct name of the Subscriber and validation data.

## 1.4 Parties to the Certification Policy

### 1.4.1 Narodowy Bank Polski

Pursuant to Article 11 (1) of the Act on Trust Services, on request by the President of NBP, on 27 October 2016 the Minister of Digital Affairs entrusted NBP with the execution of the following tasks:

1. the creation and issuance of trust service provider certificates to qualified trust service providers;
2. the publication of certificates referred to in item 1;
3. the publication of a list of issued certificates, referred to in item 1 herein;
4. the creation of data for sealing certificates referred to in item 1 and certificates of the National Centre for Certification of Trust Services;
5. the maintenance of the Register;

6. the maintenance of the Polish Trusted List.

### 1.4.2 National Certification Centre

The National Certification Centre is the main certification office in the national trust infrastructure created by NBP to implement the tasks listed in item 1.4.1.

### 1.4.3 Registration Office

The Security Department operates a registration point for the National Certification Centre and is responsible for receiving and executing decisions of the minister in charge of digital affairs, including decisions to revoke trust service provider certificates, as well as exchanging documents and information between the Subscriber, the minister in charge of digital affairs, and the National Certification Centre.

### 1.4.4 Subscriber

A Subscriber is a Qualified Trust Service Provider who received a Trust Service Provider Certificate.

### 1.4.5 Relying Parties

Relying Party – a natural or legal person that relies upon a Trust Service.

## 1.5 Scope of certificate usage

Trust Service Provider Certificates issued to a Subscriber by the National Certification Centre are used in the verification of advanced eSignatures or advanced eSeals referred to in Annex I letter g, Annex III letter g, Annex IV letter h of eIDAS or in the verification of Trust Services provided by the Subscriber.

The usage scope for the Trust Service Provider Ccertificate issued by the National Certification Centre is not limited by the Centre, and results from the Legislation on Trust Services.

In accordance with Article 16 of the Act on Trust Services, the advanced eSignature or the advanced eSeal verified with the use of the Trust Service Provider Certificate are used for signing or sealing electronically:

1. qualified certificates referred to in Annex I letter g, Annex III letter g and Annex IV letter h of eIDAS;
2. information on the status of qualified certificates, including the list of suspended or revoked certificates;
3. other certificates related to the provision of Qualified Trust Services.

See also Chapter 6.1.7

## 1.6 Policy Management

### 1.6.1 Organisation responsible for document management

The author of and the entity responsible for managing the Policy is:

**Narodowy Bank Polski**
**ul. Świętokrzyska 11/21**
**00-919 Warszawa**

### 1.6.2 Contact data

To obtain information concerning services and the activity of the National Certification Centre, please contact:

**Narodowy Bank Polski**
**Departament Bezpieczenstwa**
**ul. Świętokrzyska 11/21**
**00-919 Warszawa**
**Poland**
tel.: (+48 22) 185 15 13 fax: (+48 22) 185 23 36
https://www.nccert.pl email: nccert@nccert.pl

### 1.6.3 Document Approval Procedure

The general rules for the provision of Trust Services by NBP are laid down in Resolution No. 53/2016 of the Management Board of NBP. The Policy has been created based on Annex 1 to the above-mentioned resolution and is subject to approval by the Director of the Security Department of NBP.

Any version of the Policy is valid until the approval and publication of a new version. A new version is prepared by the NBP employees and is submitted to the minister in charge of digital affairs and Qualified Trust Service Providers, with the status of "to be agreed". After the document has been agreed, the new version of the Policy is approved by the Director of the Security Department of NBP.

Corrections of editing errors and changes to contact data are the only changes which may be introduced without prior consultation with the minister in charge of digital affairs and Qualified Trust Service Providers.

Any provision of the Policy may be changed, provided a 20-day period for comments and amendments is given. In the event of a reasonable need, this period may be shortened to 5 days.

Any proposed changes which may materially influence the parties of the Policy shall be published in the Repository. Any entities whose interests will be affected by the proposed changes may submit their comments concerning the changes to the Director of the Security Department of NBP..

Should the proposed change be modified as a result of the submitted comment, the notification of the modified wording of the change should be promulgated at least 20 days before the change comes into force.

In justified cases, and in particular when the change or its enactment date result from the provisions of law, the above-mentioned periods for submission of comments or notification of modification of the change as a result of a comment may be shortened further.

The valid version of the Policy and the previous versions are available in the Repository.

Where a change in provisions of the Policy necessitates changes in the Resolution of the Management Board of NBP – prior to preparing a new version of the Policy it is necessary to introduce changes to the Resolution of the Management Board of NBP. A change of the resolution is enacted in line with the rules applicable in NBP.

# 2. Publication and Repository Responsibilities

## 2.1 Repository

The Repository of the National Certification Centre is available at the following website www.nccert.pl . NBP declares that the Repository will be accessible 24 hours a day, 7 days a week. NBP makes every effort to minimize the likelihood of unavailability of the Repository, and the maximum time of episodic periods of unavailability shall not exceed 1 hour in the case of an action related to the revocation of the Trust Services Provider Certificate and 4 hours in the case of other aspects of the functioning of the Repository. The unavailability of the Repository shall not have an impact on the declared time of implementation of a decision on the revocation of certificates of Trust Service Providers referred to in point 4.9.5.

## 2.2 Information Published in the Repository

The following are published in the Repository:

- National Certification Centre Certificate (issued in 2009) – https://www.nccert.pl/files/nccert.crt ;
- National Certification Centre Certificate (issued in 2016) – https://www.nccert.pl/files/nccert2016.crt ;
- Valid list of issued Trust Service Provider Certificates – http://www.nccert.pl/zaswiadczeniaE.htm ;
- Valid list of revoked Trust Service Providers Certificates (corresponding to the certificate issued in 2009) - http://www.nccert.pl/arl/nccert-n.crl ;
- Valid list of revoked Trust Service Providers Certificates (corresponding to the certificate issued in 2016) - http://www.nccert.pl/arl/nccert2016.crl ;
- Valid Polish Trusted List – https://www.nccert.pl/tsl/PL_TSL.xml ;
- Up-to-date Register - http://www.nccert.pl/uslugiE.htm ;
- Valid version of the Policy – https://www.nccert.pl/policies/PC_NCCert_EN.pdf ;
- Archived versions of the Policy - http://www.nccert.pl/archiwumE.htm#archiwumPolityki ;
- Additional information, e.g. notices and information concerning proposed changes to the Policy– https://www.nccert.pl/komunikaty.htm .

## 2.3 Time and Frequency of Publication

- National Certification Centre Certificates – immediately upon their creation;
- Trust Service Provider Certificates – immediately upon their creation and issuance;

- Valid list of issued Trust Service Provider Certificates – immediately upon their creation and issuance of a Qualified Trust Service Provider Certificate;
- Valid list of Revoked Trust Service Providers Certificates – at least once a day (excluding Saturdays, Sundays and bank holidays), and each time upon revocation of a Trust Service Provider Certificate, no later than within 1 hour from the revocation of the certificate of a Trust Service Provider from the minister in charge of digital affairs;
- Valid Polish trusted list — at least once every 3 months and immediately upon issuance or revocation of a Qualified Trust Service Provider Certificate by the National Certification Centre, or upon each update of the Register of Trust Service Providers, if such a change requires an update to the Polish Trusted List;
- Valid Register – modified every time upon receiving a request from the minister in charge of digital affairs to make (or remove) an entry to (from) the Register;
- The Policy – a valid version, following each change to this document, immediately upon the approval of changes thereto, along with the information on the implementation date of these changes;
- Additional information, e.g. notices and information concerning proposed changes to the Policy, if required.

## 2.4 Access Controls on Repositories

Information published in the Repository is publicly available for viewing. This information is published solely by duly authorized employees of NBP.

# 3. Identification and Authentication

The general rules of receipt by the National Certification Centre of a decision of the minister in charge of digital affairs are presented below.

The Policy distinguishes between:

- receipt of a decision on entering a Trust Services Provider or services provided by it to the Register; the decision on making the entry is the basis for the issue of the certificate and making the entry into the Trusted List;
- receipt of a decision on striking a Qualified Trust Service Provider or a service provided by it off the Register, which may cause the revocation of the Trust Service Provider Certificate;
- Receipt of a decision to revoke a Trust Service Provider Certificate.

The rules do not stipulate receipt of decisions related to suspension of Trust Service Provider Certificates.

The issuance of a Trust Services Certificate to the Qualified Trust Service Provider is made based on a decision of the minister in charge of digital affairs, referred to in Article 4 (6) of the Act on Trust Services. The decision issued to the Qualified Trust Services Provider is forwarded for the information of the National Certification Centre. Data necessary for issuing a Trust Service Provider Certificate (certification request) is submitted to National Certification Centre by the Trust Service Provider. National Certification Centre issues a Trust Service Provider Certificate immediately, not later than within 3 business days from the date of receipt of a decision and accurate data required for the issue of a Trust Service Provider Certificate.

## 3.1 Naming

Trust Service Provider Certificates are issued by the National Certification Centre in accordance with standard X.509 v3. This means, in particular, that the National Certification Centre accepts only such Subscriber names that are in line with standard X.509 (with reference to the recommendations of series X.500).

Data provided in a Trust Service Provider Certificate are submitted to the National Certification Centre in the form of a certification request.

Data contained in the certification request must clearly identify the Subscriber and must be identical with the data given by the Subscriber in the request to make an entry in the Register. First of all, the field "Organisation" should contain the name of the Subscriber that is the same as the name of the company entered in public registers (e.g. KRS, CEIDG).

### 3.1.1 Types of Names

The name contained in the National Certification Centre Certificate issued in 2009 consists of the following three fields:

| Name of Field | Content |
|---|---|
| **Country** | PL |
| **Organization** | Minister wlasciwy do spraw gospodarki |
| **Common name** | Narodowe Centrum Certyfikacji (NCCert) |

The name contained in the National Certification Centre Certificate issued in 2016 consists of the following four fields:

| Name of Field | Content |
|---|---|
| **Country** | PL |
| **Organization** | Narodowy Bank Polski |
| **Common name** | Narodowe Centrum Certyfikacji |
| **Organisation Identifier:** | VATPL-5250008198 |

The name contained in the Trust Service Provider Certificate, verified using the National Certification Centre Certificate issued in 2009, consists of the following four fields:

| Name of Field | Content |
|---|---|
| **Country** | PL |
| **Organization** | *Subscriber name* |
| **Common name** | *Name given by the Subscriber and related to a given trust service* |
| **Serial number.** | *Number of Register entry* |

The name contained in the Trust Service Provider Certificate, verified using the National Certification Centre Certificate issued in 2016, consists of the following four fields:

| Name of Field | Content |
|---|---|
| **Country** | PL |
| **Organization** | *Subscriber name* |
| **Common name** | *Name given by the Subscriber and related to a given trust service* |
| **Organisation Identifier:** | VATPL – *NIP (tax identity) number of the Subscriber* |

The UTF-8 system is used for the coding of characters in all the mentioned fields in certificates issued by the National Certification Centre.

### 3.1.2 Need for Names to be Meaningful

The names contained in the Trust Service Provider Certificate must enable clear identification of the Subscriber and the National Certification Centre.

### 3.1.3 Rules for Interperting Various Name Forms

Identifiers distinguishing Subscribers are interpreted in accordance with standard ISO/IEC 9595 (X.500) Distinguished Name (DN)

### 3.1.4 Uniqueness of Names

The identifier distinguishing the Subscriber must ensure unambiguous indication of the Subscriber.

### 3.1.5 Recognition, Authentication and Role of Trademarks

Not applicable.

## 3.2 Initial Identity Validation

### 3.2.1 Method to Prove Possession of eSeal Creation Data

Ownership of eSeal creation data, associated with validation data provided in the request for certification, is checked by verifying the eSeal on this request for certification, created with the use of validation data included in the request. The National Certification Centre will additionally compare validation data included in the certification request with data which has already been assigned to another Subscriber in the issued Trust Service Provider Certificates. Should this data be repeated, the National Certification Centre will inform the minister in charge of digital affairs about this fact.

### 3.2.2 Authentication of Organization Identity

Not applicable.

### 3.2.3 Authentication of Individual Identity

Authentication of identity concerns only individuals sending a certification application. It is carried out on the basis of a qualified electronic signature, which is supplied with the certification application and the authentication issued for that person.

### 3.2.4 Non-verified Subscriber Information

All Subscriber data contained in a Trust Service Provider Certificate are subject to verification in the National Certification Centre.

### 3.2.5 Validation of Public Bodies and Organisations

Not applicable.

### 3.2.6 Criteria for Interoperation

Not applicable.

## 3.3 Identification and Authentication for Re-key Requests

The same as in the case of the issue of the first Trust Service Provider Certificate – see Chapter 3.2.

# 4. Certificate Life-Cycle Operational Requirements

## 4.1 Certificate Application

The National Certification Centre does not accept applications directly from the Subscriber. All applications by Subscribers must be submitted to the minister in charge of digital affairs. The National Certification Centre creates and issues Trust Service Provider Certificates upon receiving an appropriate administrative decision of the minister in charge of digital affairs.

### 4.1.1 Who can Submit a Certificate Application

A request to issue a Trust Service Provider Certificate in the form of an administrative decision of the minister in charge of digital affairs can be submitted only by the minister in charge of digital affairs.

### 4.1.2 Enrolment Process and Applicants' Responsibilities

The minister in charge of digital affairs forwards the decision on the entry into the Register, which is the basis for the issue of the certificate or the decision to remove from the Register, which is the basis for the revocation of the certificate to the following address Departament Bezpieczeństwa Narodowy Bank Polski, ul. Świętokrzyska 11/21, 00-919 Warszawa. In the case of an application in electronic form, the minister in charge of digital affairs shall forward the application bearing a qualified eSignature to the following email addresses: sekretariat.DB@nbp.pl and nccert@nccert.pl

The NBP employee who acts as the System Operator in the National Certification Centre shall verify the following:

1. the qualified eSignature affixed to the request,
2. the authorisations of the person who signed the decision using a qualified eSignature,
3. the correctness and completeness of the request.

Having verified the above, the NBP employee confirms receipt of the request via email to the address indicated by the minister in charge of digital affairs.

To create a Trust Service Provider Certificate, the Subscriber prepares a request for certification which shall be compliant with the profile specified in Attachment B to this Policy and forwards it to the National Certification Centre, together with information on whether the issued certificate is to bear the eSeal verified with the certificate of the National Certification Centre issued in 2009 or with the one issued on 2016. The request can be submitted in the form of a file stored on CD to the following address: Departament Bezpieczeństwa Narodowy Bank Polski, ul. Świętokrzyska 11/21, 00-919 Warszawa, or via

email to the following email addresses sekretariat.DB@nbp.pl and nccert@nccert.pl. If the certification request is sent via email, it must bear the qualified eSignature of the authorised employee of the Subscriber.

## 4.2 Certificate Application Processing

### 4.2.1 Performing Identification and Authentication Functions

Identification and authentication functions are performed by the National Certification Centre in compliance with the conditions specified in Chapter 3.2.

### 4.2.2 Approval or Rejection of Certificate Applications

The application forwarded by the minister in charge of digital affairs is accepted by the National Certification Centre only where all the stages of the verification process described in item 4.1.2 have ended with a positive result. In the event that at least one of the stages ends with a negative result, the application is rejected. The information on the rejection of an application is sent via email to the address indicated by the minister in charge of digital affairs.

### 4.2.3 Time to Process Certificate Applications

NBP issues a Trust Service Provider Certificate immediately, not later than within 3 business days from the date of receipt of a complete application from the minister in charge of digital affairs and a complete certification request.

The National Certification Centre implements the revocation of the Trust Service Provider Certificate and publishes information on the revocation within 24 hours of taking the decision to revoke the certificate by the minister in charge of digital affairs.

## 4.3 Certificate Issuance

### 4.3.1 Actions during Certificate Issuance

The procedure of issuing a Trust Service Provider Certificate is as follows:

1. The System Operator checks if the Subscriber for whom the certificate is to be issued is registered in the National Certification Centre database and makes the registration, if necessary.
2. The System Operator imports the certification request submitted by the Subscriber and approves its execution.
3. Following the creation of the Trust Service Provider Certificate, he or she forwards the certificate to the Subscriber for verification.
4. Following the receipt of confirmation that the Trust Service Provider Certificate is correct from the Subscriber (the Subscriber is required to send the information on the

correctness of the issued certificate or on spotted errors by 12.00 noon on the following business day at the latest), the System Operator publishes the certificate in the Repository, updates the Trusted list and informs the minister in charge of digital affairs and Qualified Trust Service Providers of the issuance of the certificate.

#### 4.3.2 Notification to Subscriber of Issuance of Certificate

The information on the issuance of a new Trust Service Provider Certificate is forwarded to the Subscriber via email, and once the Subscriber confirms the correctness of the certificate, the certificate is published in the Repository and entered on the Trusted List.

### 4.4 Certificate Acceptance

#### 4.4.1 Certificate Acceptance Confirmation

The Subscriber is obliged to check the correctness of the issued Trust Service Provider Certificate. The Subscriber is obliged to send the information on the correctness of the issued certificate or spotted errors by 12.00 noon on the following business day at the latest. Failure to send this information is treated as acceptance of the issued certificate.

In the event that errors have been spotted in the issued Trust Service Provider Certificate, the National Certification Centre notifies the minister in charge of digital affairs thereof, revokes the incorrect certificate and issues a new one. In such a case the provisions of Chapter 4.9 concerning certificate revocation do not apply.

#### 4.4.2 Publication of the Certificate by National Certification Centre

When the Subscriber confirms the correctness of the certificate, it is published in the Repository and entered on the Trusted List. This is the basic form of informing other entities about the issue of the Trusted Service Provider Certificate. Additionally, information on the issuance of a new Trust Service Provider Certificate is sent via email to the minister in charge of digital affairs and to Qualified Trust Service Providers

#### 4.4.3 Notification of Certificate Issuance to other entities

Publication of a certificate in the Repository and entering the certificate on the Trusted List are the prime method of informing other entities about the issuance of the certificate.

### 4.5 Cryptographic Key and Certificate Usage

#### 4.5.1 Key Pair and Certificate Usage by Subscribers

See Chapter 1.5 and 6.1.7.

#### 4.5.2 Relying Party Certificate Usage

A Relying Party must use certificates:

- in compliance with the content of the Trust Service Provider Certificate (keyUsage and extendedKeyUsage fields),
- only after verification of their status (see Chapter 4.9) and credibility of the eSeal attached by the National Certification Centre.

## 4.6 Certificate renewal

Not applicable.

## 4.7 Certificate re-key

The same as in the case of the issuance of the first Trust Service Provider Certificate – see Chapters 4.1 - 4.4.

## 4.8 Certificate Modification

The same as in the case of the issuance of the first Trust sSrvice Provider Certificate – see Chapters 4.1 - 4.4.

## 4.9 Certificate Revocation

With the exception of the case described in item 4.4.1, the National Certification Centre revokes a Trust Service Provider Certificate only on the basis of an administrative decision of the minister in charge of digital affairs. Requests for Trust Service Provider Certificate revocation should be submitted directly to the minister in charge of digital affairs.

### 4.9.1 Circumstances for Revocation

The decision to revoke a Trust Service Provider Certificate can only be taken by the minister in charge of digital affairs.

### 4.9.2 Who can Request a Revocation

The revocation of a Trust Service Provider Certificate may only be requested by the minister in charge of digital affairs.

### 4.9.3 Procedure for Revocation Request

Following the receipt of a decision to revoke a Trust Service Provider Certificate from the minister in charge of digital affairs, the person acting as the System Operator revokes the certificate and publishes a new certificate revocation list in the Repository. Thereafter the Register and the Trusted List are modified.

After the publication of a certificate revocation list, the National Certification Centre forwards to the minister in charge of digital affairs and to Subscribers the confirmation that the certificate has been revoked.

Operations related to Trust Service Provider Certificate revocation, the creation and publication of an up-to-date certificate revocation list are recorded in an event log.

### 4.9.4 Revocation Request Grace Period

The National Certification Centre processes the decision on the revocation of the Trusted Service Provider Certificate and immediately publishes information on the revocation, i.e. within 1 hour of the revocation of the certificate, however not later than 24 hours after receiving the decision on the revocation from the minister in charge of digital affairs.

The certificate revocation list makes it possible to determine the time of Trust Service Provider Certificate revocation with an accuracy of one second. This time is recorded automatically by the software used for certificate revocation. The National Certification Centre ensures the receipt of the decision on the revocation of the Trusted Service Provider Certificate 24 hours a day.

### 4.9.5 Time within which CA must Process the Revocation Request

The National Certification Centre processes the decision on the revocation of the Trusted Service Provider Certificate and immediately publishes information on the revocation, i.e. within 1 hour of the revocation of the certificate, however not later than 24 hours after receiving the decision on the revocation from the minister in charge of digital affairs.

### 4.9.6 Revocation Checking Requirements for Relying Parties

Before it accepts an eSeal verified using a Trust Service Provider Certificate issued by the National Certification Centre, the Relaying Party should check if the Trust Service Provider Certificate is not listed on the certificate revocation list published at the www.nccert.pl website.

It should be noted, however, that the publication of a certificate revocation list, similarly to the lists of suspended and revoked certificates published by the Subscriber, occurs later than the actual revocation of the Trust Service Provider Certificate.

### 4.9.7 CRL Issuance Frequency

Up-to-date certificate revocation lists are published in the following situations:

- immediately, i.e. not later than 1 hour after the revocation of the Trusted Service Provider Certificate;
- at least once a day (excluding Saturdays, Sundays and all bank holidays).

### 4.9.8 Maximum Latency for CRLs

The National Certification Centre publishes the valid certificate revocation list without delay immediately upon its creation.

#### 4.9.9 Online Revocation/Status Checking Availability

The National Certification Centre does not provide an online certificate status verification service.

#### 4.9.10 Online Revocation Checking Requirements

Not applicable.

#### 4.9.11 Other Forms of Revocation Advertisements Available

Information on Trust Service Provider Certificate revocation is entered into the Register and the Trusted List.

#### 4.9.12 Special Requirements Related to Key Compromise

In the event of a security compromise or alleged compromise of data for eSeal creation, the Subscriber shall immediately notify the minister in charge of digital affairs of this fact.

In the event of a security compromise or alleged compromise of data for eSeal creation by the National Certification Centre, NBP is obliged to immediately notify the minister in charge of digital affairs of this fact.

### 4.10 Certificate Status Services

#### 4.10.1 Operational Characteristics

Information on the status of certificates issued by the National Certification Centre can be obtained based on the certificate revocation lists published on the www.nccert.pl website. Information on the revocation of a certificate is included on every list published after the revocation has been carried out.

The National Certification Centre provides its services using solutions that ensure synchonisation with the international time standard (UTC) with an accuracy of 1 second. Synchronisation is carried out every 15 minutes.

#### 4.10.2 Service Availability

Certificate status verification services are available 24 hours a day, 7 days a week. NBP makes every effort to minimize the likelihood of unavailability of the Repository, and the maximum time of episodic periods of unavailability shall not exceed 1 hour in the case of an action related to revocation of the Trust Services Provider Certificate and 4 hours in the case of other aspects of the functioning of the Repository.

#### 4.10.3 Optional Features

Not applicable.

## 4.11 End of Subscription

Termination by the Subscriber of usage of Trust Services provided by the National Certification Centre is tantamount to the Subscriber ceasing their activity as a Qualified Trust Service Provider.

## 4.12 Key Escrow and Recovery

Not applicable.

# 5. Facility, Management and Operational Controls

This chapter includes the most important information concerning the physical, organisational and operational safeguards applied in NBP in connection with the performance of tasks entrusted to it by the minister in charge of digital affairs.

## 5.1 Physical Controls

### 5.1.1 Site Location and Construction

The National Certification Centre is located in two separate data centres based in two distant facilities of NBP, which are safeguarded by the physical security systems in accordance with the regulations applicable in NBP. The back-up centre, which enables full restoration of the system's functionality as provided by the main centre as well as back-up and archive copies storage, is accessible only to authorised persons in the following regime: 24 hours a day, 7 days a week.

### 5.1.2 Physical Access

Access to facilities which house the National Certification Centre is controlled. Access to system components is granted exclusively to authorised persons. Persons other than NBP employees are allowed to perform work in the system in connection with the performance of tasks specified in contracts signed by NBP. The contracts contain provisions which secure an appropriate level of security of the service and maintenance work that is performed solely under supervision of the persons who have been assigned roles in the National Certification Centre.

### 5.1.3 Power and Air Conditioning

To prevent interruptions of operations caused by power outages, the National Certification Centre owns an emergency power system. The adequate air temperature and humidity required in the facilities of the main and back-up centres are secured by air-conditioning systems.

### 5.1.4 Water Exposure

The critical elements of the National Certification Centre are located in facilities with low exposure to flooding risk, also as a result of a damage of the water and central heating system in the building. In the case of flooding risk, the employees shall act in accordance with the procedures in force in NBP and the procedures for ensuring continuity of operations of the National Certification Centre are activated.

### 5.1.5 Fire Prevention and Protection

The facilities housing the National Certification Centre are protected by an automatic fire extinguishing system. In the case of fire risk, the employees shall act in accordance with the procedures in force in NBP and the procedures for ensuring continuity of operations of the National Certification Centre.

### 5.1.6 Media Storage

All devices enabling the recording and transmitting of information are subject to special control measures in computer centres, including restricted movement between security zones,.

Access to data carriers is restricted, and the carriers are stored in facilities under surveillance. Data entered to the system from outside electronic data carriers are, prior to data entry, scanned for computer viruses and other malicious software.

### 5.1.7 Waste Disposal

Redundant paper documents, electronic documents and other data carriers used within the system operated by the National Certification Centre are destroyed safely, in accordance with procedures in force at NBP.

### 5.1.8 Off-site Backup

Secure back-up copies are stored in separate locations with access control. The back-up centre, which enables full restoration of the system's functionality as provided by the main centre, is accessible only to authorised persons in the following regime: 24 hours a day, 7 days a week. The back-up centre is protected by the same security measures as the main centre.

## 5.2 Procedural Controls

### 5.2.1 Trusted Roles

The following roles are defined within the National Certification Centre:

1. **System Security Inspector**, responsible for supervision of the implementation and application of any and all security procedures for the operation of IT systems used by the National Certification Centre;
2. **System Administrator,** responsible for installation, configuration and management of the IT system and for data recovery from a back-up copy;
3. **System Operator,** responsible for day-to-day operation of the system, including making back-up copies; at the same time, fulfils the role of Registration Inspector and Revocation Inspector.

4. **Audit Inspector**, responsible for analysing event logs in the National Certification Centre.

### 5.2.2 List of persons required to perform a task

In compliance with the procedures in force in the National Certification Centre, certain tasks require the attendance of more than one NBP employee with a function in the National Certification Centre.

| No. | Task name | List of required persons |
|---|---|---|
| **1.** | Starting the system | System Operator, System Administrator, System Security Inspector |
| **2.** | Import of data for creation of eSeals | two System Operators, System Security Inspector |
| **3.** | Issuing a Trust Service Provider Certificate | two System Operators |
| **4.** | Revocation of a Trust Service Provider Certificate | two System Operators |
| **5.** | Recovery of a back-up copy of the system | System Operator, System Administrator, System Security Inspector |
| **6.** | System shutdown | System Operator, System Security Inspector |
| **7.** | Making a back-up copy | System Operator, System Security Inspector |
| **8.** | Generation of data for creation of eSeal | two System Operators, System Security Inspector |

### 5.2.3 Identification and Authentication for Each Role

Identification and authentication of employees performing roles is handled through physical and procedural safeguard systems, including in particular:

1. limitation and control of access to the facilities housing the National Certification; Centre;
2. allocation of individual accounts in the system and a specified scope of authority appropriate for the given scope of responsibilities;
3. use of electronic cards to activate elements of the system.

### 5.2.4 Roles Requiring Separation of Duties

All roles in the National Certification Centre require separatrion of duties.

## 5.3 Personnel Controls

### 5.3.1 Qualifications, Experience and Clearance Requirements

NBP guarantees that all NBP employees performing tasks within the National Certification Centre:

1. have full capacity to enter into legal transactions;
2. have the knowledge and skills required to create certificates and to render other services related to the eSignature and eSeal, hardware and software used for electronic data processing, and automatic data processing in telecommunications networks and systems;
3. have access to documentation in a reasonable scope, as required by their roles and responsibilities, including any procedures, policies and regulations.

### 5.3.2 Background Check Procedures

Operational employees of the National Certification Centre are selected based on their professional qualifications and in accordance with the rules of employment in force at NBP.

### 5.3.3 Training Requirements

Persons with roles in the National Certification Centre are trained, especially in the scope of:

1. technology of creating certificates and rendering other services related to the eSignature and eSeal;
2. operation of hardware and software used for electronic data processing and automatic data processing in telecommunications networks and systems;
3. adherence to security procedures applicable for ICT systems;
4. adherence to emergency procedures;
5. adherence to procedures used in the conduct of professional duties.

### 5.3.4 Reraining Frequency and Requirements

Training shall relate to the scope of knowledge required at a given post. Persons with roles in the National Certification Centre shall attend staff development courses, as required by the training policy of NBP. Any changes in the operations of the National Certification Centre shall result in further NBP employee training.

### 5.3.5 Job Rotation Frequency and Sequence

Not applicable.

### 5.3.6 Sanctions for Unauthorised Actions

Any and all actions performed in the course of duties related to the activities of the National Certification Centre are documented and supervised. This shall, in particular, enable detection of any unauthorized activities by any persons with roles in the National Certification Centre.

Violation of safety rules, regulations and policies in force shall be punishable by disciplinary action or criminal liability specified in separate regulations.

### 5.3.7 Contracting Personnel Requirements

Not applicable.

### 5.3.8 Documentation Supplied to Personnel

Persons with roles in the National Certification Centre shall receive a description of responsibilities applicable to their post, together with required procedures, in accordance with the rules in force at NBP.

## 5.4 Audit Logging Procedures

To ensure an appropriate level of security of its operations, the National Certification Centre has developed and implemented security control procedures for these operations, including in particular:

1. system status monitoring;
2. creating event logs for the purposes of security audits of business operations;
3. periodical review and analysis of the event logs;
4. inspections of implemented mechanisms and security measures;
5. procedures in the event of a security breach.

Persons with roles in the National Certification Centre shall perform periodic reviews of event logs. Reviewing event logs is aimed at detecting attempted breaches of the system operations security, in particular

1. unauthorized attempts to gain access to the systems in use;
2. unauthorized attempts to gain access to the used and processed information;
3. unauthorized attempts to gain access to the premises of the National Certification Centre;
4. attempts to disrupt the operations of the systems in use;
5. attempts to prevent performance of tasks of the National Certification Centre.

### 5.4.1 Types of Events Recorded

Event logs are created during the day-to-day operations of the National Certification Centre. Event logs contain information on operations performed in the course of fulfilling the tasks of the National Certification Centre, including in particular:

1. requests to provide a service normally handled by the system or services which are not handled by the system, as well as information on the execution or failure to execute such a service or services (and, in the case of non-execution, the reason for this);

2. significant events related to the changes in the system environment, including in the sub-system for the management of infrastructure keys management, Trust Service Provider Certificate and data for eSeal creation by the National Certification Centre, such as the creation of user accounts and to the type of authorisations assigned;
3. installation of new software or updates to the existing software;
4. starting and stopping event loggers;
5. changes in the configuration of event loggers, including in particular each modification of the system time;
6. date and time of the creation of back-up copies:
7. date and time for event log archiving;
8. shutdown, start-up and restart of the system;
9. actions undertaken upon detection of malfunctioning event loggers;
10. negative results of random number generator quality tests;
11. any Trust Service Provider Certificate revocation request and any changes related to such requests, including in particular any messages sent and received between the minister in charge of digital affairs and NBP.

Each entry into the event Register shall contain at least the following information:

1. date and time of the event, with an accuracy of one second;
2. type of the event;
3. identifier or other information identifying the person responsible for the event;
4. specification of whether the event was related to a successful or an unsuccessful operation.

The National Certification Centre allows for viewing event logs, checking for information at least in the aforementioned scope, and enables authorized persons to review their content, along with human-readable and interpretable records. Making changes in the records concerning recorded events is forbidden. The system contains mechanisms which ensure the integrity of event registers and prevent their modification upon their transfer to the archives.

Event registers concerning the installation of new software or software updates, archiving or creating back-up copies do not have to be created in an electronic format.

Network devices used in the on-line part register and store for approx. 4 months information regarding the following:

1. source and target address;
2. network communication IP protocol;
3. number of source and target port;

4. time of initiation and termination of session;
5. data volume in the framework of sent/received packets.

The above information is also sent to a specialised system for security information and event management (SIEM), in which it is stored for a 1-year period.

### 5.4.2 Frequency of Event Log Processing

Event logs are reviewed at least once a day (excluding Saturdays, Sundays and all bank holidays). Rules of inspection and analysis of event logs are specified by the procedures of the National Certification Centre.

### 5.4.3 Retention Period for Audit Log

Event logs shall be stored for at least three years (20 years in the case of event registers connected with the use of eSeal Creation Data for the National Certification Centre) in a manner which allows the stored information to be electronically searchable. Upon the expiration of the storage period, event logs shall be securely destroyed or moved to the archive pursuant to applicable legal regulations, norms and standards.

### 5.4.4. Protection of Audit Log

Event logs are stored in an appropriately secure environment. The integrity of files in event registers is ensured.

The event registers should be backed up. Back-up copies of the registers must be performed using techniques that ensure data integrity. Data backup operations must be performed in the presence of at least two people referred to in Chapter 5.2.1 of this Policy. Data backup operations shall be directly supervised by the System Security Inspector.

### 5.4.5 Audit Log Backup Procedures

Copies of event logs are created along with the secure back-up copies of the system. Two identical copies of the event logs are stored in two separate locations. Back-up copies of the registers must be performed using techniques that ensure data integrity. Data backup operations must be performed in the presence of at least two people referred to in Chapter 5.2.1 of this Policy. Data backup operations shall be directly supervised by the System Security Inspector.

### 5.4.6 Audit Data Collection System (Internal vs. External)

Electronic event logs are created automatically by the software and operational systems. In addition, event logs concerning the operation of the system are created and include events that are not otherwise registered by the IT system, but are entered by authorised persons with roles in the National Certification Centre.

The table below lists sample information concerning data collection for the purposes of security inspections.

| No. | Event type | Manner of collection | Ensured by |
|---|---|---|---|
| **1.** | Successful and unsuccessful attempts to change parameters of the operating system. | Automatic | Operational system |
| **2.** | Opening and closing of systems and applications. | automatic/manual | Operational system |
| **3.** | Successful and unsuccessful login/logout attempts. | Automatic | Operational system |
| **4.** | Successful and unsuccessful attempts to create, modify or delete system accounts. | Automatic | Operational system |
| **5.** | Successful and unsuccessful attempts to create, modify or delete authorised system users. | automatic/manual | Operational system and personnel |
| **6.** | Successful and unsuccessful attempts to create and revoke Trust Service Provider Certificates. | Automatic | Software |
| **7.** | Successful and unsuccessful operations related to the publication of Trust Service Provider Certificates and information about revoked Trust Service Provider Certificates. | automatic/manual | Software and personnel |
| **8.** | Successful and unsuccessful operations related to the publication of other information. | automatic/manual | Software and personnel |
| **9.** | Creating and archiving secure back-up copies. | automatic/manual | Operational system and personnel |
| **10.** | Changes in the system configuration | Manual | Personnel |
| **11.** | Software updates and computer hardware modifications | Manual | Personnel |
| **12.** | System maintenance tasks | Manual | Personnel |
| **13.** | Personnel changes | Manual | Personnel |

### 5.4.7 Notification of Event Causing Subject

Persons with roles in the National Certification Centre shall notify the System Security Inspector of any events which may influence the security of the system or any events indicating that the security of the system has been compromised. In the event of an incident referred to in Article 19 of eIDAS, the information about the occurrence of the incident is submitted to the minister in charge of digital affairs.

### 5.4.8 Vulnerability Assessment

The system shall be periodically assessed in order to identify risks, assess the probability of their occurrence and assess the system's vulnerability to the aforementioned. On the basis of the risk analysis results, the National Certification Centre shall implement solutions aimed at eliminating or reducing the vulnerability of the system to these identified risks.

## 5.5 Records Archival

### 5.5.1 Types of Records Archived

The National Certification Centre archives and stores the following information:

1. certificates of the National Certification Centre
2. Trust Service Provider Certificates
3. certificate revocation lists,
4. Trusted Lists,
5. Register,
6. accepted certification requests;
7. secure backup copies of system elements;
8. secure backup copies of databases;
9. copies of NBP correspondence pertaining to the operations of the National Certification Centre;
10. event logs;
11. other information published by the National Certification Centre;

### 5.5.2 Retention Period for Archive

Event logs shall be stored in a manner enabling their electronic search, for a minimum period of 3 years. Following the lapse of the period, they can be securely destroyed or archived. Event registers connected with the use of eSeal Creation Data for the National Certification Centre are stored for 20 years from the day of the termination of the validity of the National Certification Centre certificate connected with these data.

NBP shall store all documents and electronic data referred to in Chapter 5.5.1, with the exception of event logs, for a period of 20 years from the moment of creation of a document or data. In the case of certificates of the National Certification Centre and Trust Service Provider Certificates, the period of 20 years is counted from the moment the certificate expires,

### 5.5.3 Protection of Archive

All documents and electronic data directly related to the execution of tasks of the National Certification Centre are stored in a manner that ensures the security of the stored documents and data. In particular:

1. archival resources are safeguarded by physical protective measures;
2. access to the archive is limited only to authorised persons with roles in the National Certification Centre;
3. the premises of the archive are monitored.

### 5.5.4.Archive Backup Procedures

The National Certification Centre has implemented procedures for the collection and management of archived resources, and in particular:

1. resource classification;
2. automatic electronic data collection;
3. processing of hard copies into electronic formats;
4. ensuring the security of archival resources.

The rules of collection and management of archived resources are specified by the procedures of the National Certification Centre.

### 5.5.5 Requirements for Time-Stamping of Records

Archive copies are time-marked by the operating system during the execution of a given copy. The National Certification Centre uses solutions that ensure synchronicity with Coordinated Universal Time (UTC) with an accuracy of one second.

In addition, the date of the execution of the archive copy is placed on the electronic medium containing the copy.

### 5.5.6 Archive Collection System (Internal vs. External)

Archive copies shall be made manually by System Operators and saved on external data carriers.

### 5.5.7 Procedures to Obtain and Verify Archive Information

Information may only be disclosed to authorized entities. Information can be added to and removed from the archives only by duly authorized persons with roles in the National Certification Centre. The possibility to read data from the archived secure back-up copies is tested at regular intervals. In the event of detecting any problems with reading the data, these data will be restored from the data currently residing in the system or any copies of archived

resources. A detailed description of the above actions is contained in the procedures of the National Certification Centre.

## 5.6 Key Changeover

The validity periods of certificates of the National Certification Centre and Trust Service Provider Certificates are not longer than:

- 23 years for a certificate of the National Certification Centre;
- 11 years for a Trust Service Provider Certificate.

The eSeal creation data and validation data are valid as long as the certificate of the National Certification Centre or the Trust Service Provider Certificate to which these data relate are valid. The start of the validity period of a certificate of the National Certification Centre and a Trust Service Provider Certificate cannot be earlier than the moment of creation of the certificate.

Amending the eSeal creation data by the National Certification Centre requires the creation of a new certificate of the National Certification Centre. In order to ensure continuity of operations of the National Certification Centre, the process of amending the eSeal creation data begins no later than after half the period of validity of the National Certification Centre certificate connected with these data. Owing to the complexity of the operation of exchanging a certificate of the National Certification Centre, the manner of the certificate exchange is agreed each time with the minister in charge of digital affairs and with the Subscribers. Depending on the decision, one of the following scenarios is applied:

1. The exchange of eSeal creation data takes place in the same Certification Authority, i.e. it does not trigger the exchange of the distinguishing identifier contained in the certificate of the National Certification Centre.
2. The exchange of eSeal creation data is combined with the launch within the National Certification Centre of a new Certification Authority with a new distinguishing identifier. In such a case, by the time the previous certificate of the National Certification Centre expires, two Certification Authorities operate simultaneously, with the proviso that all new Trust Service Provider Certificates are issued under the new Certification Authority. The Certification Authority related to the previous certificate of the National Certification Centre is used solely for the publication of certificate revocation lists and in the event of revocation of the Trust Service Provider Certificate it has issued.

The principles of exchange of eSeal creation data or eSignature creation data by a Subscriber are determined by the Subscriber.

## 5.7 Compromise and Disaster Recovery

The National Certification Centre has developed and tested an emergency plan, which:

1. includes information concerning settings and configuration of the hardware and software;
2. specifies measures and detailed procedures for recovery and estimated time for their performance;
3. indicates persons responsible for the activation of procedures aimed at limiting the impact of the event or the natural disaster and restoring the required level of security and an appropriate level of provided services;
4. identifies the persons responsible for the development and maintenance of procedures, including those responsible for regular tests described in the procedures;
5. specifies priorities for individual activities.

NBP owns a backup facility which secures the execution of tasks of the National Certification Centre should the operation of the main centre become impeded. The procedures specify the circumstances and rules for starting the system in the backup centre.

At least once a month tests are carried out, consisting in the recreation of data in the back-up centre. After completion of the tests, a report is prepared.

### 5.7.1 Incident and Compromise Handling Procedures

In accordance with internal regulations on incident handling in force in NBP and applicable provisions from the contracts entered into by NBP with external providers of support and maintenance of the software and hardware used in the National Certification Centre.

In the event of an incident referred to in Article 19.2 of eIDAS, the information on the incident is forwarded by the supplier to the following address nccert@nccert.pl. All information on incidents are forwarded by NBP to the minister in charge of digital affairs.

### 5.7.2 Computing Resources, Software, and/or Data are Corrupted

The procedures of the National Certification Centre include actions in the event of failure of hardware, software and any damage of processed and stored data. They include a description of the basic configuration of the system, installation and configuration procedures, and the procedures for the restoration of elements of the system from backup copies. The procedures specify the circumstances for starting the system in the backup facility.

### 5.7.3 eSeal Creation Data are Compromised or Allegedly Compromised

The procedures of the National Certification Centre include activities in the event that eSeal creation data used by the National Certification Centre are compromised. The procedures specify the methods for notifiying the minister in charge of digital affairs and the Subscribers.

### 5.7.4 Business Continuity Capabilities after a Disaster

The procedures of the National Certification Centre include measures required for the restoration of appropriate security and service levels in the event of a natural disaster, terrorist attack, sabotage or other dangers which might interrupt the operations of the National Certification Centre.

## 5.8 Termination of Operations of the National Certification Centre

1. In the event that NBP:

1) intends to cease its activity as an authorized entity,
2) shall no longer be able to act as an authorized entity, or
3) is informed by the minister in charge of digital affairs of the intent to revoke the authorization referred to in Art. 11 (1) of the Act on Trust Services.

- NBP undertakes to ensure that it will continue to act as an authorized entity until the minister in charge of digital affairs selects a new entity which will take over these obligations.

2. NBP shall ensure it will continue to act as an authorised entity for no longer than:

1) 6 months from the day a notification is given to the minister in charge of digital affairs concerning the circumstances referred to in items 1 and 2 hereinabove, or
2) 4 months from the day NBP is informed of the circumstance referred to in item 3 hereinabove.

3. Should the minister in charge of digital affairs revoke his authorization referred to in Art. 11 (1) of the Act on Trust Services, NBP shall immediately cease operating as an authorized entity.

4. In the event it ceases to act as an authorised entity, NBP shall ensure that it will enable another entity, including the minister in charge of digital affairs, to take over the role and continue to act as an authorised entity – at the request of the minister in charge of digital affairs – and shall provide all information and data which will enable the performance of this role by the new entity. The National Certification Centre has procedures describing the detailed end activities.

# 6 Technical Security Controls

## 6.1 Data for the Creation and Validation of the eSeal Generation and Installation

### 6.1.1 Generation of Data for the Creation and Validation of eSeals

Data for the creation and validation of the eSeal of the National Certification Centre shall be generated directly within the cryptographic module which serves as the eSeal creation device, and shall be saved (in the form of a shared secret) on electronic cards. Data generation shall take place in the main facility, in the premises of the National Certification Centre in the presence of at least two System Operators and the System Security Inspector. Following data generation, electronic cards allocated to the backup facility are transported to that facility.

The rules of generating and storing data for eSeal generation by the Subscriber are defined by the Subscriber taking into account the standards and regulations for Trust Service Providers.

### 6.1.2 Delivery of eSignature or eSeal Creation Data to Subscriber

Not applicable. The eSignature creation data or eSeal creation data of a Subscriber are generated by the Subscriber.

### 6.1.3 Validation Data Delivery to the National Certification Centre

The Subscriber delivers the validation data to the National Certification Centre with the intermediation of the minister in charge of digital affairs, in the form of a certification request.

### 6.1.4 National Certification Centre eSeal Validation Data Delivery to Subscriber

The eSeal validation data of the National Certification Centre are released to the Subscriber in the form of a certificate of the National Certification Centre. A certificate of the National Certification Centre is also published in the Repository.

### 6.1.5 eSignature Creation and Validation Data Sizes

Data for the creation and validation of the eSeal of the National Certification Centre shall use at least a 4096 bit RSA (in the case of the certificate issued in 2016) or a 2048 bit RSA (in the case of the certificate issued in 2009).

Data for the creation and validation of the eSeal of the Subscriber shall use: at least:

- a 4096 bit RSA or a 256 bit ECDSA (in the case of the certificates issued since 9 December 2016)
- or a 2048 bit RSA (in the case of the certificates issued until 9 December 2009).

### 6.1.6 Generation Parameters and Quality Checking of eSeal Creation and Validation Data

Unless legal provisions state otherwise, the generated data for eSeal creation and validation must meet the minimum requirements specified in ETSI TS 119 312 "Electronic Signatures and Infrastructures; Cryptographic Suites".

An appropriate quality of data for creation and validation of the eSeal is secured by the eSeal creation device used in the National Certification Centre. Following data generation, the National Certification Centre verifies the size and algorithm of the generated data.

### 6.1.7 Acceptable Usage of eSignature or eSeal Creation Data

The scope of use of data for the creation and validation of the eSeal by the National Certification Centre is defined by two attributes of the certificate of the National Certification Centre: keyUsage and basicConstraints. These data may only be used for:

1. sealing electronically Trust Service Provider Certificates,
2. sealing electronically the certificate revocation lists.

The scope of use of eSignature creation data and eSeal creation data by the Subscriber is defined by three attributes of the Trust Service Provider Certificate: keyUsage, extKeyUsage and basicConstraints. The above data may only be used for signing or sealing electronically:

1. qualified certificates referred to in Annex I letter g of eIDAS, Annex III letter g of eIDAS and Annex IV letter h of eIDAS;
2. information on the status of qualified certificates, including the list of suspended or revoked certificates;
3. other certificates related to the provision of Qualified Trust Services.

The use of eSignature creation data or eSeal creation data by the Subscriber must conform to the certification policy specified in the Register.

## 6.2 eSeal Creation Data Protection and Cryptographic Module Engineering Controls

Data for the creation and validation of the eSeal of the National Certification Centre shall be generated directly within the cryptographic module which serves as the eSeal creation device, and shall be saved (in the form of a shared secret) on electronic cards. Data generation shall take place in the main facility, in the premises of the National Certification Centre in the presence of at least two System Operators and the System Security Inspector. Cryptogtaphic modules never leave the premises of the National Certification Centre and are located only in the facilities secured with an alarm system. Electronic cards which carry a shared secret are secured with PIN codes and are stored in a manner that prevents unauthorised access to them.

### 6.2.1 Cryptographic Module Standards and Controls

The cryptographic modules used in the National Certification Centre are compliant with standard FIPS 140-2 Level 3.

### 6.2.2 eSeal Creation Data Multi-Person Control

In the case of their export outside the eSeal creation device, the eSeal creation data are transferred in shared secret form. Nine electronic cards shall be created containing the shared secret, and recovery of the eSeal creation data shall require two cards.

### 6.2.3 eSeal Creation Data Escrow

eSeal creation data shall neither be stored nor escrowed, with the exception of a situation referred to in Chapter 6.2.2.

### 6.2.4 eSeal Creation Data Backup

eSeal creation data shall be stored only in the eSeal creation devices located in the main and backup facilities and on electronic cards referred to in item 6.2.2. No additional eSeal Creation Data Backup copies shall be created.

### 6.2.5 eSeal Creation Data Archival

eSeal creation data shall not be archived. Following the expiry of the certificate of the National Certification Centre related to that data, the data are destroyed in accordance with procedure in force at NBP.

### 6.2.6 eSeal Creation Data Transfer into or from a Cryptographic Module

When needed, the eSeal creation data shall be entered into the cryptographic module with the use of the electronic cards referred to in item 6.2.2. The data shall be entered in the presence of at least two System Operators and the System Security Inspector.

The eSeal creation data shall be retrieved from the cryptographic module only in two cases:

1. immediately following their generation in order to save the data on electronic cards and transfer them into the backup facility;
2. when there is a need to create a new set of electronic cards referred to in item 6.2.2., i.e. when the electronic cards forming the set created at the time of generation of the eSeal creation data are damaged. Following generation of a new set of electronic cards, the previous set shall be destroyed.

### 6.2.7 eSeal Creation Data Storage on Cryptographic Module

The eSeal creation data shall be stored on the cryptographic module only in open form. These shall not be accessible to unauthorised persons, though.

### 6.2.8 Method of Activating eSeal Creation Data

The eSeal Creation Data can only be activated once they are entered into the cryptographic module. Data activation shall require entering the access code to the module.

### 6.2.9 Method of Deactivating eSeal Creation Data

The eSeal Creation Data can be deactivated by their removal from the cryptographic module or stopping the application using the data.

### 6.2.10 Method of Destroying eSeal Creation Data

The eSeal creation data stored in the cryptographic module shall be destroyed by their removal from the module via the module management software.

The destruction of the eSeal creation data stored on electronic cards (as shared secret) shall consist in the physical destruction of the electronic cards.

### 6.2.11 Cryptographic Module Rating

See chapter 6.2.1

## 6.3 Other Aspects of eSeal Creation Data Management

### 6.3.1 eSeal Validation Data Archival

The validation data of the eSeal of the National Certification Centre and the Subscriber shall be archived and stored for at least 20 years following their expiry.

### 6.3.2 Usage Periods of eSeal Creation and Validation Data

The validity period of the eSeal creation data and validation data shall be equal to the validity period of the certificate to which these data relate, specified in chapter 5.6.

## 6.4 Activation Data

Activation data are used to activate the eSeal creation data by the National Certification Centre and to activate eSignature creation data by System Operators.

The activation data for eSeal creation data include elements of the shared secret saved on electronic cards which, after being imported, enable the recovery of the e-Seal creation data, as well as the PIN codes protecting these electronic cards.

The activation data for the System Operator's eSignature creation data take the form of a PIN code protecting the Operator's electronic card.

### 6.4.1 Activation Data Generation and Installation

The activation data in the form of shared secret components saved on electronic cards are generated in the manner described in item 6.1.1.

The activation data in the form of PIN codes are established by System Operators.

### 6.4.2 Activation Data Protection

The activation data for eSeal creation data shall be under special protection. Electronic cards which contain shared secret components shall be stored in the National Certification Centre in a manner which ensures an appropriate level of security, under the supervision of the System Security Inspector. PIN codes for these cards shall only be known to their holders. Additionally, procedures of disclosure of PIN codes for cards to other authorized persons in emergency situations are prepared.

### 6.4.3 Other Aspects of Activation Data

Not applicable.

## 6.5 Computer Security Controls

### 6.5.1 Specific Computer Security Technical Requirements

The components of the National Certification Centre are controlled in the following way:

1. physical separation of system components from other IT systems,
2. control of access both relating to access to facilities and particular system components (e.g. individual accounts in the operating system and applications),
3. auditing controls,
4. separation of roles in the operating system and applications,
5. identification and authentication of roles,
6. cryptographic protection of communication between particular system components,
7. eSeal creation data recovery mechanism,
8. creation of back-up and archived copies,
9. maintainance of a back-up centre ready to take over the activity at any time,
10. monitoring and warning in the event of unauthorized access to the ICT system.

### 6.5.2 Computer Security Rating

The National Certification Centre uses an IT system ensuring the level of security required by the regulations on trust services and internal regulations of NBP.

## 6.6 Life Cycle of Technical Controls

In accordance with the general law provisions and internal regulations of NBP concerning, among others, the security policy at NBP and IT system security management at NBP.

### 6.6.1 System Development Controls

The development of applications is handled in an separate testing environment, using appropriate quality control measures. Application development work is performed in a separate testing environment.

### 6.6.2 Security Management Controls

In accordance with the general law provisions and internal regulations of NBP concerning, among others, the security policy at NBP and IT system security management at NBP.

### 6.6.3 Life-Cycle Security Ratings

This Policy lays down no requirements in this respect.

## 6.7 Network Security Controls

Components of the National Certification Centre are not linked to an external network. Communication between these components and the outside world is made with the use of data carriers.

## 6.8 Time-Stamping

Not applicable.

# 7. Certificate, CRL and Profiles

See Annex C and D.

# 8. Compliance Audit and Other Assessments

## 8.1 Frequency or Circumstances of Assessment

The National Certification Centre is audited for compliance with the provisions of the Act on Trust Services. The compliance audit is conducted as needed or if significant changes are introduced in the National Certification Centre.

In addition, the operations of the National Certification Centre within NBP may be subject to internal audits and internal inspections, pursuant to the regulations in effect in NBP.

## 8.2 Identity/Qualifications of Compliance Auditor

Compliance auditors should have sufficient knowledge and qualifications to be able to reliably assess the audited issue.

## 8.3 Compliance Auditor's Relationship to Assessed Entity

Compliance audits may not be conducted by employees directly participating in the operations of the National Certification Centre.

## 8.4 Topics Covered by Compliance Audit

The date and scope of a compliance audit shall be determined by the Director of the Security Department.

## 8.5 Actions Taken as a Result of Deficiency

Audit results are submitted to the President of NBP. Should the inspectors detect any irregularities, the Director of the Security Department shall immediately act upon the recommendations made following the inspection.

## 8.6 Communication of Results

Selected fragments of the internal inspection report may, with the permission of the minister in charge of digital affairs, be published in the Repository.

# 9. Other Business and Legal Matters

## 9.1 Fees

NBP shall do the following free of charge:

1. create, issue and publish Trust Service Provider Certificates;
2. grant access to data contained in the Repository;
3. enable the import of Trust Service Provider Certificates;
4. publish information on the revocation of a Trust Service Provider Certificate;
5. provide access to the lists of revoked Trust Service Provider Certificates contained in the Repository;
6. grant access to the Trusted List contained in the Repository.

The "Certification Policy of the National Certification Centre" document is available free of charge on the website of the National Certification Centre in electronic version only.

## 9.2 Financial Responsibility

Not applicable.

## 9.3 Confidentiality of Business Information

NBP observes the provisions of the Act on Trust Services with reference to information collected in connection with the operations of the National Certification Centre.

### 9.3.1 Scope of Confidential Information

Any information related to the operations of the National Certification Centre, the unauthorized disclosure of which may cause damage to NBP, the National Certification Centre, the Subscriber or the Relying Party, is subject to confidentiality, including in particular the eSeal creation data used by the National Certification Centre.

Confidentiality does not apply to information on the infringement of the regulations on Trust Services by the Subscriber and to information on security infringement and loss of integrity referred to in Article 19 paragraph 2 of eIDAS.

The obligation to maintain the confidentiality referred to in Art. 15 paragraph 1 of the Act on Trust Services shall last for 10 years from the cessation of the legal relationship described in Art. 15 paragraph 3 of the Act. The obligation to maintain the confidentiality of the eSeal creation data by the National Certification Centre applies indefinitely.

### 9.3.2. Information not within the Scope of Confidential Information

Public information includes, in particular:

1) certificates of the National Certification Centre;
2) issued Trust Service Provider Certificates;
3) lists of issued Trust Service Provider Certificates;
4) certificate revocation lists;
5) the Trusted List;
6) the Register,
7) the Policy;
8) information concerning proposed changes to the Certification Policy;
9) announcements concerning current activity.

#### 9.3.3 Responsibility to Protect Confidential Information

All the employees of NBP who perform tasks associated with the provision of trust services are obliged to maintain the confidentiality of the information described in Chapter 9.3.1. The obligation to maintain confidentiality of information by employees of external companies performing tasks for NBP is governed in the agreements that NBP concluded with these companies.

NBP shall disclose data concerning the operations of the National Certification Centre and covered by confidentiality exclusively to the following entities:

1) courts and prosecutors – only in relation to on-going proceedings;
2) the minister in charge of digital affairs – in relation to his supervision of the operations of Trust Service Providers;
3) other authorized bodies – in relation to the proceedings conducted by them.

Pursuant to Article 15 paragraph 4 of the Act on Trust Services, the eSeal creation data used by the National Certification Centre may not be disclosed.

### 9.4 Personal Data Protection

Not applicable.

### 9.5 Security of intellectual property

NBP has the full right to the copyright related to this Policy. NBP allows the use of the Policy (including printing and copying) by Subscribers and Relying Parties.

### 9.6 Representations and Warranties

#### 9.6.1 NBP Obligations

NBP is obligated to, in particular:

1) create certificates of the National Certification Centre;
2) create and issue Trust Service Provider Certificates based on a decision by the minister in charge of digital affairs;
3) publish certificates of the National Certification Centre;
4) publish issued Trust Service Provider Certificates;
5) publish lists of issued Trust Service Provider Certificates;
6) maintain the Register;
7) publish the Trusted List;
8) ensure that the Trusted List is up-to-date;
9) publish data used in verification of the Trusted List;
10) publish an up-to-date certificate revocation list in a timely manner;
11) ensure an appropriate level of security for the activity in question;
12) use eSeal creation data in accordance with the Act on Trust Services;
13) use solutions which ensure synchronicity with Coordinated Universal Time (referred to henceforth as UTC), with an accuracy of one second, while acting as an authorized entity, and especially while creating event registers and Authority Revocation Lists.

### 9.6.2 Obligations of the Registration Point

The National Certification Centre Registration Point in the Head Office of NBP is responsible for receiving and executing orders of the minister in charge of digital affairs as well as for exchanging documents and information between the Subscriber, the minister in charge of digital affairs and NBP.

### 9.6.3 Obligations of the Subscriber

The Subscriber is obligated to, in particular:

1) fulfil the provisions of the Act on Trust Services and other laws applicable within the territory of the Republic of Poland;
2) adhere to the rules laid down by the Certification Policy;
3) comply with the security requirements specified by the Act on Trust Services and norms and applicable standards, including the requirements to properly and securely generate data related to the Trust Service Provider Certificate and used for eSeal and eSignature creation, and to protect this data against loss, theft, disclosure, modification, as well as unauthorized access and use;
4) immediately notify the minister in charge of digital affairs of any security breaches or any suspicion that the security of data related to the Trust Service Provider Certificate and used for eSeal or eSignature creation may have been compromised;
5) check and confirm the validity of information contained in the issued Trust Service Provider Certificate;

6) read correspondence received from NBP;
7) notify the minister in charge of digital affairs immediately, but not later than within 14 days from the change of the factual or legal status, of any changes in the information entered into the register referred to in Article 7 of the Act on Trust Services.

### 9.6.4 Obligations of the Relying Party

The Relying Party should perform diligent verification of each eSignature and eSeal that it intends to rely on, including in particular any data contained in this Certification Policy.

## 9.7 Disclaimers of Warranties

The issuance of a Trust Service Provider Certificate shall not make NBP an agent, trustee or representative of the entity to whom the Trust Service Provider Certificate is issued.

## 9.8 Limitations of Liability

NBP is not liable towards the Relying Party for any damages resultant from the failure by the Relying Party to fulfil its duties, nor the failures to fulfil the duties on the part of the Subscriber or other Relying Party, including:

1) neglecting the obligation to verify eSignatures or eSeals;
2) trusting an incompletely or negatively verified eSignature or eSeal;
3) trusting documents signed or sealed electronically which contain false information;
4) signing or sealing electronically false data by the Subscriber;
5) failure to fulfil the obligation to protect eSignature or eSeal creation data.

NBP is not liable for the processes related to trust service provision by the Subscriber.

## 9.9 Compensation

Not applicable.

## 9.10 Transitional provisions and the period of validity of the Policy

See chapter 1.6.3.

## 9.11 Specification of the mode and addresses to written correspondence

All written correspondence related to the activities of the National Certification Centre should be sent to the address indicated in chapter 1.6.2. Correspondence related to the activities of Subscribers should be delivered to the minister in charge of digital affairs.

## 9.12 Changes in the Policy

See chapter 1.6.3.

## 9.13 Settlement of disputes

All claims and complaints regarding the activities of the National Certification Centre should be sent to the address indicated in chapter 1.6.2. Claims and complaints regarding Subscribers should be sent to the minister in charge of digital affairs.

## 9.14 Interpretation and enforcement of laws

The activity of the National Certification Centre is in compliance with the law in force in the Republic of Poland, including in particular the Act on Trust Services together with the implementing acts.

Should any provision of the Certification Policy be deemed invalid or unenforceable, the validity and enforceability of the remaining provisions shall not in any way be affected thereby. Each provision of the Certification Policy concerning limitation of liability is binding and shall be interpreted as separate from other provisions.

## 9.15 Legal basis

See chapter 9.14

## 9.16 Other provisions

See chapter 10.

# 10. Publication of the Trusted List

Pursuant to Article 11 paragraph 1 of the Act on Trust Services and Electronic Identification, NBP maintains the Trusted List referred to in *Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22 (5) of Regulation (EU) No 910/2014 of the European Parliament and and of the Council on electronic identification and trust services for electronic transactions in the internal market.*

The Trusted List contains information on Qualified Trust Service Providers liable to supervision by the Republic of Poland, together with information on the qualified trust services provided by them, in accordance with the relevant provisions of *Regulation (EU) No. 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.*

The cross-border use of eSignatures was facilitated through Commission Decision 2009/767/EC of 16 October 2009 which imposed the obligation on Member States to establish, maintain and publish Trusted Lists with information on certification service providers issuing qualified certificates to the public who are supervised/accredited by Member States, in accordance with Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. The Trusted List published by the National Certification Centre is a continuation of the Trusted List established by Commission Decision 2009/767/EC. Trusted Lists are a fundamental element of the process of building trust among electronic market operators since they enable users to determine the qualified status and status log of Trust Service Providers and their services.

Certificates used to verify the eSeal affixed to the Polish Trusted List are published at www.nccert.pl and on the European central list – the "List of the lists" maintained by the European Commission. The unique identifier of these certificates has the following format:

| Name of Field | Value |
|---|---|
| **Country** | PL |
| **Organization** | Narodowy Bank Polski |
| **Common name** | Polish TSL Operator |

## 10.1 Frequency of publication of the Trusted List

A valid trusted list shall be published at least once every three months and immediately upon:

- issuance or revocation of a Trust Service Provider Certificate

- each update of the Register, if such an update requires a change of information contained in the Trusted List.

Operations related to the creation and publication of a valid Trusted List shall be recorded in the event log.

The valid Trusted List shall be published at the following address: https://www.nccert.pl/tsl/PL_TSL.xml

In addition, the page https://www.nccert.pl contains the following:

1. certificates used in the verification of the eSeal attached to the Trusted List;
2. file containing abbreviation (sha256) from the valid Trusted List;
3. link to the European "list of the lists", which is a collection of links to lists published by each Member State, and contains certificates used for the verification of eSignatures and eSeals affixed to these lists;
4. Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22 (5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

# Attachment A – Certificates of the National Certification Centre

| | |
|---|---|
| Date of issue | 26 October 2009 |
| Date of expiry | 27 October 2020 |
| Key Identifier: of the entity | 59 34 0c fb 7d e7 45 01 6f c9 70 96 c2 4e 06 f8 0f 81 43 f6 |
| Certificate in base64 format | -----BEGIN CERTIFICATE-----<br>MIIDzTCCArWgAwIBAgIUYqcNBMMkuNQnVsw/gWvy6zLvBxkwDQYJKoZIhvcNAQEF<br>BQAwbjELMAkGA1UEBhMCUEwxLjAsBgNVBAoMJU1pbmlzdGVyIHdsYXNjaXd5IGRv<br>IHNwcmF3IGdvc3BvZGFya2kxLzAtBgNVBAMMJk5hcm9kb3dlIENlbnRydW0gQ2Vy<br>dHlmaWthY2ppIChOQ0NlcnQpMB4XDTA5MTAyNjA2NTcwMVoXDTIwMTAyNjIzNTk1<br>OVowbjELMAkGA1UEBhMCUEwxLjAsBgNVBAoMJU1pbmlzdGVyIHdsYXNjaXd5IGRv<br>IHNwcmF3IGdvc3BvZGFya2kxLzAtBgNVBAMMJk5hcm9kb3dlIENlbnRydW0gQ2Vy<br>dHlmaWthY2ppIChOQ0NlcnQpMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC<br>AQEA47WXqJ/BLdHdOOh7Stj8NMUVYlmwmpfr8KUOoJA4AEYp+KZaK58wgaknV7a/<br>v1y+4OXSGCRtvDP7YiLbqlC3TmkKaUFxeizygmo07PtUEIyAXhA72yfe/RI8ZyW9<br>+jv8tY6aNPK7FTpBP6T2WngLdNMN9iwd7AhCZoZCYL3auA/xqKJUmJC8F/9+tkzk<br>B8PEV6LIzuyE8cF+225VTHJtMkqNhwJSn35BKlAm+d4j/ra58Bh/KYicqLibDKV0<br>TKPG/3MIFNXLmW9ia/7GkGkGXmjHwlNrWwwpgaPHLTeUMOghD9ve/dyD1afEdjyi<br>Q1BNGcfUCZ8qXKF0ROZaDoy7PQIDAQABo2MwYTAOBgNVHQ8BAf8EBAMCAQYwDwYD<br>VR0TAQH/BAUwAwEB/zAfBgNVHSMEGDAWgBRZNAz7fedFAW/JcJbCTgb4D4FD9jAd<br>BgNVHQ4EFgQUWTQM+33nRQFvyXCWwk4G+A+BQ/YwDQYJKoZIhvcNAQEFBQADggEB<br>ALt95q4lwfjnsFsENeoq8xhYOz/y7veagxLM6f7t0nTPn4GVihXdVZUWQ3IpvRHu<br>h0x1X3etV2IcuEWQw4oNsdWk2ydZwxbMdxebnrVIk7tteyTRjSg3FCjtCyPfHRga<br>y505/bxiWVph64uClZA/1D5cC+IzN3h2xxU2faX1A4Bq2m52s9XzNqZe6SwJBqn2<br>YE9oDER0MFXhpgZOOSK5owveLBb4MdFKqno96CD9V8u/fD16v7lSwJE+fSub+ih+<br>DlUEMBM3kJ0SA7pClHl3fOlGCw7rzVjX67QlYbr1vMFuWYx0fv65YD9UrNX5THkT<br>2kq8e5JRDuHq4X17XtGHlU4=<br>-----END CERTIFICATE----- |

| | |
|---|---|
| Date of issue | 9 December 2016 |
| Expiry date | 10 December 2039 |
| Key Identifier: of the entity | 29 b3 c8 c4 df a3 87 f8 66 05 12 58 fd 46 2a b8 98 0d 79 87 |
| Certificate in base64 format | -----BEGIN CERTIFICATE-----<br>MIIFzzCCA7egAwIBAgIUQPj3irDjZBBWkcjZ4Cz4wcZACkYwDQYJKoZIhvcNAQEN<br>BQAwbzELMAkGA1UEBhMCUExwHTAbBgNVBAoMFE5hcm9kb3d5IEJhbmsgUG9sc2tp<br>MSYwJAYDVQQDDB1OYXJvZG93ZSBDZW50cnVtIENlcnR5ZmlrYWNqaTEZMBcGA1UE<br>YQwQVkFUUEwtNTI1MDAwODE5ODAeFw0xNjEyMDkwODUyNDFaFw0zOTEyMDkyMzU5<br>NTlaMG8xCzAJBgNVBAYTAlBMMR0wGwYDVQQKDBROYXJvZG93eSBCYW5rIFBvbHNr<br>aTEmMCQGA1UEAwwdTmFyb2Rvd2UgQ2VudHJ1bSBDZXJ0eWZpa2FjamkxGTAXBgNV<br>BGEMEFZBVFBMLTUyNTAwMDgxOTgwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIK<br>AoICAQDuyaDrULBW0PLYMfDwG1cZ6qWlTCzhb+vffSNd6AvF/4uTwCpNNcbHH3WH<br>st1FD1ZygGBFyWjb6QpGwW58JSd+6+UuvsVTzYSilhrd4afmNGyKg945e4z1vY91<br>bzivNPQ+LcXPMFx+GLcncrYzyQLsK5fqNOuVQDXPhrFG3o4gDxhUWsHjpBKWvFwI<br>n1VzNcP17/MML5pYAnOGnlNQpjqexbzSEsDF3b1mTi50kkfHD/NN4zSaJMJGvsFj<br>aIFhakEuLA6GeI7OO+do3oh5U8osUYOznbB1BtC3NGAE9NU1JeSHQH3speUX8iH7<br>0UjNdhyf96HY/ZDMRJF4bfWLdBCxCAmWJEYADbciUxus6TUjrjEzKSceMEmjg2Or<br>DMUISSmsH44Usx6S367WmGVpsuMh39X0GQRLz+ntwqJi1yvRttcdrhrNo7jOEG2R<br>Elm113+GDo1mmtMB6TrKU42kEQsR1yH7FAO0/zsvnnVjUtFEHH45SQWS43fuZXO1<br>ioS0SFNO/7wKZS+cYOzzGlMvv+eW6jVYouXupM/Fa5+vkhYnw6v/LTWIYylw9XbZ<br>Xpgf+aSa8ZWiaTKfHhEHFmhVPjqUF4bkACVUknu+5UZKUTE1+69PgpEe0uhyzJ/z<br>QIwZ6+MHpzDx2cfi6qU2sKGS8M99upjMm7GQ4LqHlG/lYrterwIDAQABo2MwYTAO<br>BgNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/BAUwAwEB/zAfBgNVHSMEGDAWgBQps8jE<br>36OH+GYFElj9Riq4mA15hzAdBgNVHQ4EFgQUKbPIxN+jh/hmBRJY/UYquJgNeYcw<br>DQYJKoZIhvcNAQENBQADggIBAK+GzchsHQruy9sCZ2QDtF6kveZT5JVfpfJ7Aspw<br>VR3+VrH50aiGlSid4va1EBHWxD1uw7t3FMYvlvU/KAk+TA5+0GSrJFalO5nYNma9<br>dYcgiD8tBQdB3tOU27wTrSD0VXsolXnRYNerNyeo5TWzqcy5InfZAT95XtmTE9me<br>l1cu4yYwdT1/+m0ws9YZLdvaDK9tIJzkOn4CFTCvMUcGMOg1ncE1X07LH26ibsiV<br>zgbVBoK6Qe+O4w533pTta9rOoudOqL44F/+YPSSfBNvRD49OpQNYsf2umgS2WTsk |

```
wcSEM/gJoelE0Avp4c1rz0/6VQsX+JNOnHadKZQl1GUrUxEAiAy4A5hpz6qyTNtu
DSc3tdbjaddLr7jESAaU3Zbi/s+vDeYqgO5jsR6RX1iyBpUTdciTnZOGSyRE5ek2
g6IERpmnhP4bKL2ylJK+OchYFL/HFPFiAuRXBhiv5o8AOQGvWVY8bCvzliI869IS
w4kdpmxnyx9GKxcuTTmvr3TMIbEpCuG+vCsmjvl+JtP/bGWSNjSpzxO4NEABnAjM
BI4m+SGQy2wxJ3dEONZvjk1ph0bYE/cQRlgoxAlk8JuGt0XTw03Ar2EklhN8IeBk
8e6KDeKxSNX60z3XTChCgTPj+ErwdNzX8tcRo5FrQ68VwTF27+pYYAEfAs2hqHZ2
KHW0
-----END CERTIFICATE-----
```

# Attachment B – Certification request profile

| Field (field type) | Notes |
|---|---|
| **CertificationRequest (*CertificationRequest*)** | Certification request PKCS#10 |
| **certificationRequestInfo (*CertificationRequestInfo*)** | Actual text of the certification request. |
| **version (*Version*)** | Version of the certification request, field value: 0 (version v1 ) |
| **subject (*Name*)** | Unique identifier distinguishing the Trust Service Provider, compliant with the requirements set out in item 3.1.1 |
| **subjectPKInfo (*SubjectPublicKeyInfo*)** | Value of validation data along with the identifier of the algorithm with which these data are associated. |
| **algorithm (*AlgorithmIdentifier*)** | Identifier of the algorithm with which the validation data are associated. |
| **Algorithm(1) (*OBJECT IDENTIFIER*)** | Object Identifier assigned to the algorithm with which the validation data are associated. |
| **Parameters** | Attribute is compliant with the field **Algorithm(1)** and specified by the Qualified Trust Service Provider. |
| **subjectPublicKey *(BIT STRING)*** | Validation data. |
| **attributes (*Attributes*)** | Certification request attributes to be inserted in the Trust Service Provider Certificate. |
| **subjectKeyIdentifier (*SubjectKeyIdentifier*)** | Optional field – Validation data identifier. |
| **keyUsage (*KeyUsage*)** | Intended application of eSeal or eSignature creation data. |
| **extKeyUsage (*ExtendedKeyUsage*)** | Extended intended application of eSeal or eSignature creation data. In the case of the Qualified Certification Service **there is no such field**. |

| | |
|---|---|
| **signatureAlgorithm (*AlgorithmIdentifier*)** | Identifier of the algorithm with which the eSeal or eSignature creation data of the Qualified Certification Service Provider are associated. |
| **Algorithm(2) (*OBJECT IDENTIFIER*)** | Object identifier of the algorithm with which the eSeal or eSignature data of the Qualified Certification Service Provider are associated. |
| **Parameters** | Attribute is compliant with the field **Algorithm(2)** and specified by the Qualified Certification Service Provider. |
| **signatureValue *(BIT STRING)*** | Value of the eSeal or eSignature affixed by the Qualified Certification Service Provider. |

# Attachment C – Profile of a Trust Service Provider Certificate

| Field (field type) | Notes |
|---|---|
| **tbsCertificate (*TBSCertificate*)** | Actual text of the certificate. |
| **version** (*Version*) | Version of the certificate, field value: 2 (version v3) |
| **serialNumber** (*CertificateSerialNumber*) | Unique serial number. |
| **signature** (*AlgorithmIdentifier*) | Algorithm identifier of the eSeal affixed by the National Certification Centre. |
| **algorithm** (*OBJECT IDENTIFIER*) | Object Identifier:<br>{ iso( 1 ) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }[1]<br>{ iso( 1 ) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 13 }[2] |
| **parameters** | **null** |
| **issuer** (*Name*) | Distinguishing identifier of the National Certification Centre, described in item 3.1.1. |
| **validity** (*Validity*) | Designation of the validity period of the certificate. |
| **notBefore** (*Time*) | Beginning of the certificate validity period. |
| **notAfter** (*Time*) | End of the certificate validity period. |
| **subject** (*Name*) | Distinguishing identifier of the Subscriber, described in item 3.1.1. |
| **subjectPublicKeyInfo** (*SubjectPublicKeyInfo*) | Value of validation data along with the identifier of the algorithm with which these data are associated. |

[1] For certificates verified with the National Certification Centre Certificate issued in 2009 and issued until 1 July 2018.
[2] For certificates verified with the National Certification Centre Certificate issued in 2016.

| | |
|---|---|
| **algorithm** (*AlgorithmIdentifier*) | Identifier of the algorithm with which the validation data are associated. |
| **algorithm** (*OBJECT IDENTIFIER*) | Object Identifier assigned to the algorithm with which the validation data are associated. |
| **parameters** | Attribute is compliant with the field **algorithm** and specified by the Qualified Certification Service Provider. It is transferred to the National Certification Centre in the certification request. |
| **subjectPublicKey** (*BIT STRING*) | Validation data. |
| **extensions** (*Extensions*) | Certificate extensions. |
| **authorityKeyIdentifier** (*AuthorityKeyIdentifier*) | **Non-critical extension** – Identifier of validation data of the eSeal affixed by the National Certification Centre. |
| **keyIdentifier** (*KeyIdentifier*) | Value of abbreviation (algorithm SHA-1) of validation data of the eSeal affixed by the National Certification Centre. |
| **authorityCertIssuer** (*GeneralNames*) | Unique distinguishing name consistent with the **issuer** field. |
| **authorityCertSerialNumber** (*AuthorityCertSerialNumber*) | Serial number of the National Certification Centre certificate. |
| **subjectKeyIdentifier** (*KeyIdentifier)* | **Non-critical extension** – Identifier – value of abbreviation (algorithm SHA-1) of validation data of the eSeal or eSignature affixed by the Subscriber |
| **KeyUsage** (*KeyUsage*) | **Critical extension** – application of the Subscriber's eSeal or eSignature creation data. |
| **certificatePolicies** (*CertificatePolicies*) | **Critical extension** – National Certification Centre Certification Policy. |

| | |
|---|---|
| **policyIdentifier** (OBJECT IDENTIFIER) | Policy identifier (anyPolicy) – field value **{ 2 5 29 32 0 }** |
| **policyQualifiers** (PolicyQualifierInfo) | Information on the National Certification Centre Certification Policy |
| **qualifier** (PolicyQualifierInfo) | Certification Policy data type identifier (id-qt-cps) – field value **{ 1 3 6 1 5 5 7 2 1 }** |
| **cPSuri** (IA5String) | URI to the Certification Policy – field value: "www.nccert.pl" |
| **basicConstrains** (*BasicConstrains*) | **Critical extension** – Specification as to whether a given certificate is a certificate of a Trust Service Provider issuing certificates |
| **cA** (*BOOLEAN*) | The value of this field is:<br>1. **True** – in the case of a certificate of a Trust Service Provider issuing qualified certificates.<br>2. **False** – in other cases. |
| **extKeyUsage** (a list of fields of the type*OBJECT IDENTIFIER*) | Critical extension:<br>1. In the case of certificates of a Trust Service Provider providing certification trust services there is no such field,<br>**2.** in other cases, the field contains an object identifier indicating the type of trust services defined by the Subscriber and provided to the National Certification Centre in the certification request. |
| **SignatureAlgorithm** (*AlgorithmIdentifier*) | Algorithm identifier of the eSeal affixed by the National Certification Centre. |
| **Algorithm** (*OBJECT IDENTIFIER*) | Object Identifier: |

| | |
|---|---|
| | { iso( 1 ) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }[3]<br>{ iso( 1 ) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 13 }[4] |
| **parameters** | **null** |
| **signatureValue *(BIT STRING)*** | Value of the eSeal affixed by the National Certification Centre. |

[3] For certificates verified with the National Certification Centre Certificate issued in 2009 and issued until 1 July 2018.
[4] For certificates verified with the National Certification Centre Certificate issued in 2016.

# Attachment D – CRL profile

| Field (field type) | Notes |
|---|---|
| **tbsCertList (*TBSCertList*)** | CRL |
| **version** (*Version*) | Version of the CRL — field value: 1 (version v2) |
| **signature** (*AlgorithmIdentifier*) | Algorithm identifier of the eSeal affixed by the National Certification Centre. |
| **algorithm** (*OBJECT IDENTIFIER*) | Object Identifier:<br>{ iso( 1 ) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 13 } |
| **parameters** | **null** |
| **issuer** (*Name*) | Distinguishing identifier of the National Certification Centre, described in item 3.1.1. |
| **thisUpdate** (*Time*) | List issuance date. |
| **nextUpdate** (*Time*) | Estimated date for the publication of the next list. |
| **revokedCertificates** (*Name*) | Certificate revocation list. |
| **userCertificate** (*CertificateSerialNumber*) | Serial number of the revoked certificate. |
| **revocationDate** (*Time*) | Date and time of revocation. |
| **crlEntryExtensions** (*Extensions*) | Extensions to revocation information concerning each separate certificate. |
| **cRLReason** (*CRLReason*) | Reason for certificate revocation (see item D.1) |
| **crlExtensions** (*Extensions*) | Extensions to Certificate Revocation List. |
| **authorityKeyIdentifier** (*AuthorityKeyIdentifier*) | Identifier of validation data of the eSeal affixed by the National Certification Centre. |

| | |
|---|---|
| **keyIdentifier** (*KeyIdentifier*) | Value of abbreviation (algorithm SHA-1) of validation data of the eSeal affixed by the National Certification Centre. |
| **authorityCertIssuer** (*GeneralNames*) | Unique distinguishing name consistent with the **issuer** field. |
| **authorityCertSerialNumber** (*AuthorityCertSerialNumber*) | serial number from the certificate of the National Certification Centre. |
| **cRLNumber** ( *Integer (0..MAX)* ) | Serial number of the certificate revocation list. |
| **signatureAlgorithm (AlgorithmIdentifier)** | Algorithm identifier of the eSeal affixed by the National Certification Centre. |
| **algorithm** (*OBJECT IDENTIFIER*) | Object Identifier:<br>{ iso( 1 ) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 13 } |
| **parameters** | **null** |
| **signatureValue (*BIT STRING*)** | Value of the eSeal affixed by the National Certification Centre. |

## D.1 Reason for certificate revocation

A CRL issued by the National Certification Centre may contain the following values in the CRLReason field:

1. **unspecified**: the certificate was revoked for an unspecified reason; this does not exclude the possibility that the eSignature or eSeal creation data associated with the certificate have been, or are suspected to have been, compromised,
2. **keyCompromise**: the certificate was revoked, because the eSignature or eSeal creation data associated with the certificate have been or are suspected to have been compromised,
3. **cACompromise**: the certificate was revoked, because the eSeal creation data of the National Certification Centre have been compromised,
4. **affiliationChanged**: the certificate was revoked due to changes in certificate information; the reason for revocation indicates that the eSignature or eSeal creation data associated with the certificate is not compromised or is not suspected to be compromised,
5. **superseded**: the certificate was revoked due to the replacement of the eSignature or eSeal creation data associated with the certificate; the reason for revocation indicates that the eSignature or eSeal creation data associated with the certificate is not compromised or is not suspected to be compromised,
6. **cessationOfOperation**: the certificate was revoked, as it is no longer used for the purpose for which it was issued, and the situations referred to in items 4 and 5 did not occur; the reason for revocation indicates that the eSignature or eSeal creation data associated with the certificate have neither been, nor are suspected to have been, compromised,

# Attachment E – Document Change Log

| No. | Date | Version | Person responsible | Description of actions performed |
|---|---|---|---|---|
| 1. | 22/07/2016 | 2.51 | | Accommodation of the "National Certification Centre — Certification Policy ver. 2.5" to the provisions on trust services |
| 2. | 15/09/2016 | 2.52 | | Consideration of remarks submitted by Qualified Trust Service Providers |
| 3. | 01/12/2016 | 2.53 | | Addition of provisions related to cryptographic algorithm change |
| 4. | 08/12/2016 | 2.6 | | Change of procedure of certification request submission to NBP |
| 5. | 21/02/2017 | 3.01 | | Change in 6.1.5 – addition of provisions related to ECDSA |
| 6. | 13/03/2017 | 3.01 | | Document review |
| 7. | 27.07.2017 | 3.11 | | Consideration of remarks submitted by the external auditor. |
| 8. | May 2018 | 3.21 | | Changes in relation to the amendment to Resolution No. 53/2016 of the Management Board of NBP |
| 9. | May 2018 | 3.22 | | Submission of remarks to the document |

**Document approval**

| Date | Version | Person responsible | Signature |
|---|---|---|---|
| | 3.3 | Director of Security Department | |