NBP Narodowy Bank Polski

Certification Practice Statement of the PKI NBP System

OID: 1.3.6.1.4.1.31995.1.1.2
version 2.1

Security Departament NBP
Warsaw, 2018

Table of Contents

1. Introduction

1.1 Overview

This Certification Practice Statement (hereinafter referred to as the "Statement") describes the operation of IT system of the public key infrastructure of the Narodowy Bank Polski (hereinafter referred to as "PKI NBP system"). This Statement is applicable to all PKI NBP system participants, i.e. Key Certification Centres (Certification Authorities), User Registration Points (Registration Authorities), Certificate Applicants, Subscribers and Relying Parties. The Statement lays down the rules of providing certification services, starting from Subscriber registration, public key certification, through certificate renewal, to certificate revocation. The Statement is a kind of "guide" for the relations between the PKI NBP system and its users. Consequently, all PKI NBP system users must be aware of the Statement and act in compliance with its provisions.

The structure and substantive content of this Statement are compliant with the RFC 3647 Certification Policy and Certificate Practice Statement Framework. The Statement contains all the elements detailed in the RFC 3647 in order to give the document a clear structure and more user-friendly for readers. Where a given element is not present in the PKI NBP system, the phrase "Not applicable" has appeared in a respective chapter of the Statement.

1.2 Document Name and Identification

Document name	Certification Practice Statement of the PKI NBP System
Document version	2.1
Document status	valid
Date of issue	07.06.2018
OID	1.3.6.1.4.1.31995.1.1.2
Location	http://pki.nbp.pl/pki/CPS.pdf

1.3 Certification Practice Statement Participants

1.3.1 Narodowy Bank Polski

Narodowy Bank Polski is the owner of the PKI NBP system. All the operational members in the system are NBP employees. Elements of the PKI NBP system are located at centres owned by NBP.

NBP is responsible for the operation of the entire PKI NBP system. Selected elements of the PKI NBP system may be subject to maintenance and support agreements concluded by NBP with external providers, however the trust services within the system are provided exclusively by NBP employees. The scope of duties and responsibilities of external providers is each time set out by a respective agreement.

1.3.2 Security Department

The NBP Security Department is responsible for the preparation, updating and publication of this Statement and for appointing:

- Key Certification Centre Operators,
- HSM Administrators,
- HSM Operators,
- Data Recovery Agents,
- Key Recovery Agents,
- System Security Inspectors,
- System Auditors,
- User Registration Point Operators at the NBP Head Office.

Additionally, the Security Department is responsible for the administration of access control system to the NBP facilities housing the elements of the PKI NBP system and for providing Subscribers with smartcards for cryptographic keys and certificates.

1.3.3 Information Technology and Telecommunications Department

The Information Technology and Telecommunications Department holds responsibility for securing hardware and system infrastructure for a proper operation of the system, for system administration, appointment of System Administrators and for the maintenance and repair of IT hardware, system software and data bases.

1.3.4 NBP Regional Branches

Regional branches are in charge of designating User Registration Point Operators.

1.3.5 Key Certification Centre

Key Certification Centre Operator is in charge of the issuance, revocation and publication of Subscribers' certificates. The Security Department is responsible for the operation of the Key Certification Centre in the PKI NBP system.

1.3.6 User Registration Point

User Registration Point Operator is responsible for verification of Subscribers as well as sending on Subscribers' behalf the applications to issue, renew or revoke certificates to a Key Certification Centre. In the PKI NBP system, the NBP regional branches are responsible for the operation of User Registration Points at the regional branches.
The Security Department is responsible for the operation of the User Registration Point at the NBP Head Office.

1.3.7 Subscribers

A Subscriber may be an individual on whose behalf a certificate has been issued in the PKI NBP system.

1.3.8 Relying parties

A relying party is a person or an entity other than the Subscriber who accepts and relies on a certificate issued in the PKI NBP system.

1.4 Certificate usage

In accordance with a respective Certification Policy.

1.5 Certification Practice Statement Administration

1.5.1 Organisation responsible for document administration

This Statement is owned by:
Narodowy Bank Polski
ul. Świętokrzyska 11/21
00-919 Warszawa

1.5.2 Contact data

This Statement is managed by:
Security Department
Narodowy Bank Polski
ul. Świętokrzyska 11/21
00-919 Warszawa
telephone. +48221851513 fax: +48221852336
E- mail address : cck@nbp.pl

1.5.3 Document Approval Procedure

The general rules for the provision of trust services in the PKI NBP system are laid down in Resolution No. 53/2016 of the NBP Management Board. The Resolution contains, in particular, information associated with the responsibility of NBP as a provider of trust services, information on the division of tasks between particular departments and NBP Regional Branches as well as information on control and audit. This Statement has been developed based on Appendix 3 to the Resolution and is approved by Director of the Security Department.

Each version of the Statement is in force (has a status of a valid document) until a new version of the Statement has been approved and released. A new version is developed by PKI Management Division staff of the Security Department and is delivered with the status "to be agreed" to the Information Technology and Telecommunications Department. After the document has been agreed with the Information Technology and Telecommunications Department, the new version of the Statement is approved by the Director of the Security Department.

Whenever the provisions of Resolution No. 53/2016 of the NBP Management Board are amended, the resolution has to be amended before a new version of the Statement is developed. The resolution is amended in accordance with the rules in force at NBP.

Security Department staff perform a validity review of the Statement and Certification Policies at least once a year, or whenever a change has been implemented in the PKI NBP system.

1.6 Definitions and Acronyms

1.6.1 Definitions

For the purpose of this Policy, the following definitions have been adopted:

- **Authentication** – the attribute that enables confirmation of the identity declared by the sender of information,
- **Certification Authority** (Key Certification Centre) – a certificate issuing module of the PKI NBP system that uses an own private key it has generated itself that serves to create an electronic signature and to sign CRLs; the centre also issues, revokes and distributes certificates,
- **Confidentiality** – this attribute means that information is inaccessible to unauthorised persons,
- **CRL** – the list of revoked or suspended certificates whose validity is yet to expire,
- **Cryptographic Key** – the parameter that controls the operations of enciphering, deciphering or placing/verifying the signature of the information,
- **Distinguished Name** – information included in the certificate that enables unambiguous identification of a subscriber within the directory of subscribers operated by the CCK,
- **Integrity** – the attribute that shows that the information has not been altered from the time of signing it to the time of verifying the signature,
- **Non-repudiation** – this attribute means that the sender of information cannot deny that it has been sent,
- **Private Key** – a cryptographic key, to be used exclusively by a subscriber, that serves to create a signature or decipher information,
- **Public Key Certificate** (certificate) – an electronic attestation which links a public key to a subscriber and is capable of unambiguously identifying the subscriber,
- **Public Key** – a publicly known cryptographic key associated with the private key that is used to verify a signature or encipher information,
- **Registration Authority** (User Registration Point) – a module of the PKI NBP system that serves, in particular, to verify, register and generate cryptographic keys of subscribers,
- **Subscriber** – an individual[1] holding a certificate issued in the PKI NBP system.

[1] The rules described in this Statement and Certification Policies apply to certificates issued for individuals. Certificates issued for NBP infrastructure components (servers, workstations) are issued according to separate rules.

1.6.2 Acronyms

The table below lists acronyms used in the Statement and their meanings

Acronym	Meaning
CCK	Key Certification Centre\Certification Authority
CRL	Certificate Revocation List
DIT	Information Technology and Telecommunications Department
DN	Distinguished Name
DB	Security Department
HSM	Hardware Security Module
OCSP	On-line Certificate Status Protocol
PKI	Public Key Infrastructure
PRU	User Registration Point\ Registration Authority
UPN	User Principal Name

2. Publication and Repository Responsibilities

2.1 Repositories

Two separate repositories can be distinguished in the PKI NBP system:

An internal **repository** which is in the Active Directory catalogue service and an external repository at the http://pki.nbp.pl/pki website.

As regards an **external repository**:

CCK certificates are available at the following addresses:

- http://pki.nbp.pl/pki/rca.crt – the main certification authority (NBP Root CA) - – the certificate issued on 20 November 2008,
- http://pki.nbp.pl/pki/rca(1).crt – the main certification authority (NBP Root CA) - – the certificate issued on 2 June 2014,
- http://www.nbp.pl/pki/rca(2).crt – the main certification authority (NBP Root CA) – a certificate issued using the SHA-256 hash functions,
- http://pki.nbp.pl/pki/eca(2).crt – the subordinate certification authority (NBP Enterprise CA) – the certificate issued on 2 June 2014.
- http://www.nbp.pl/pki/eca(3).crt – the subordinate certification authority (NBP Enterprise CA) – a certificate issued on 10 October 2016.

CRLs are available at the following addresses:

- http://pki.nbp.pl/pki/rca.crl – CRL of NBP Root CA (corresponding to the certificate issued on 20 November 2008),
- http://pki.nbp.pl/pki/rca(1).crl – CRL of NBP Root CA (corresponding to the certificate issued on 2 June 2014),
- http://pki.nbp.pl/pki/eca(2).crl – CRL of NBP Enterprise CA (corresponding to the certificate issued on 10 October 2016).

Documents related to the PKI NBP system are available at the following addresses:

- http://pki.nbp.pl/pki/CPS.pdf – the Certification Practice Statement of the PKI NBP system.
- http://pki.nbp.pl/pki/CP_signature.pdf – the Certification Policy for ESCB Signature certificates.
- http://pki.nbp.pl/pki/CP_authentication.pdf – the Certification Policy for ESCB authentication certificates.
- http://pki.nbp.pl/pki/CP_encryption.pdf – the Certification Policy for ESCB encryption certificates.
- http://pki.nbp.pl/pki/information.pdf – information on the usage terms of a certificate issued in the PKI NBP system.
- http://pki.nbp.pl/pki/service_order.pdf – a cryptographic service order form.

In addition, an OCSP service is available at the address http://ocsp.nbp.pl/ocsp. The above-mentioned address is common for internal users of NBP domains as well as for external users.

2.2 Information Published in Repository

In accordance with the provisions of Chapter 2.1

2.3 Publication Frequency

CCK certificates are published immediately following their creation. CRLs created by the NBP Root CA are released and published at least once every 6 months and immediately following the revocation of any certificate issued by that CA. In addition, the PRU Operator may at any moment manually generate and publish the CRLs of the NBP Enterprise CA.

CRLs created by the NBP Enterprise CA are released on an hourly basis.

2.4 Repository Access Controls

Access to http://pki.nbp.pl/pki is limited to "read only" mode and secured against unauthorised content alteration.

3. Identification and Authentication

Presented below are the general rules for Subscribers' authentication applied by the CCK when issuing certificates. The rules, which are based on specific types of information contained in a certificate, define measures essential for ensuring that the information is precise and reliable at the time the certificate is issued.

The Subscriber authentication procedure is carried out in line with the Certification Policy for individual types of certificates.

3.1 Naming

Certificates issued by the CCK comply with the X.509 v3 standard. This means, in particular, that both the certificate issuer and the PRU acting on CCK behalf accept only such Subscribers' names that conform to the X.509 standard (with reference to the X.500 series recommendations).

3.1.1 Types of names

In accordance with a respective Certification Policy.

3.1.2 The need for the names to be meaningful

In the PKI NBP system, all the names contained in Subscriber's distinguished name must be meaningful in Polish or in English.

3.1.3 Rules for interpreting various name formats

Subscribers' distinguished names are interpreted in line with the ISO/IEC 9595 (X.500) Distinguished Name (DN) standard.

3.1.4 Uniqueness of names

A certificate identifier that precisely and unambiguously designates a Subscriber is the distinguished name together with a given Subscriber's alternate name placed in that certificate (containing UPN).

NBP ensures that the Distinguished Name placed in a CCK certificate is assigned to one CCK only and that after the cessation of the CCK activities it will not be re-assigned.

3.1.5 Recognition, identification and the role of trademarks

Not applicable.

3.2 Initial Identity Validation

3.2.1 Means of proof of possession of the private key

In accordance with a respective Certification Policy.

3.2.2 Identity authentication for an entity

Not applicable.

3.2.3 Identity authentication for an individual

In accordance with a respective Certification Policy.

3.2.4 Non-verified subscriber information

All Subscriber's data detailed in the certificate are verified by the PRU.

3.2.5 Validation of offices and organisations

Not applicable.

3.2.6 Criteria for interoperability

Not applicable.

3.3 Identification and Authentication for Re-key Requests

In accordance with a respective Certification Policy.

3.3.1 Identification and authentication requirements for routine re-key

In accordance with a respective Certification Policy.

3.3.2 Identification and authentication requirements for re-key after the certificate revocation

In accordance with a respective Certification Policy.

4. Certificate Life-Cycle Operational Requirements

Submission of a respective application by a Subscriber is the basic formal requirement. Based on the application, the CCK takes an appropriate decision, either rendering the required service or refusing to render it. The submitted applications should contain information that is necessary for a proper identification of the Subscriber.

4.1 Certificate Application

Subscriber's applications may be submitted to the CCK directly or via PRU.

The PRU Operator plays a dual role: a Subscriber and a person authorised to represent the CCK. In the former role, the PRU Operator may file applications, just as any other Subscriber. In the latter role, it may confirm applications submitted by other Subscribers and, in justified cases, create applications to revoke certificates of the Subscribers who are in breach of this Statement. Applications are submitted in electronic or other form – e.g. as "Cryptographic Service Order Form".

4.1.1 Who can submit a certificate application ?

In accordance with a respective Certification Policy.

4.1.2 Enrolment process and applicants' responsibilities

In accordance with a respective Certification Policy.

4.2 Certificate Application Processing

4.2.1 Performance of identification and authentication procedures

In accordance with a respective Certification Policy.

4.2.2 Approval or rejection of certificate applications

In accordance with a respective Certification Policy.

4.2.3 Time limit for processing the certificate applications

Both CCK and PRU do their utmost to process certificate applications submitted by Subscribers as soon as possible Requests to issue a new certificate are handled during the PRU office hours (on business days from 7.30 a.m. to 4.00 p.m.), and the maximum processing time is 2 hours. Rules for applications for revocation of certificate are described in section 4.9.

4.3 Certificate Issuance

4.3.1 Actions performed by the CCK during the issuance of the certificate

In accordance with a respective Certification Policy.

4.3.2 Notification of the subscriber of certificate issuance

In accordance with a respective Certification Policy.

4.4 Certificate Acceptance

4.4.1 Confirmation of certificate acceptance

In accordance with a respective Certification Policy.

4.4.2 Publication of the certificate by the CCK

In accordance with a respective Certification Policy.

4.4.3 Notification of certificate issuance to other entities

Not applicable.

4.5 Key and Certificate Usage

4.5.1 Subscriber's use of keys and certificates

In accordance with a respective Certification Policy.

4.5.2 Relying party's use of the keys and certificate

In accordance with a respective Certification Policy.

4.6 Certificate Renewal

Not applicable, as each time a certificate is generated a new key pair of a Subscriber is generated as well.

4.7 Certificate Rekey

Certificate renewal with key changeover is made each time a Subscriber (already registered) creates a new key pair (or solicits key pair creation to the CCK) and claims issuance of a new certificate that confirms the newly created public key belongs to him/her.

Certificate renewal each time concerns a specific certificate clearly referred to in the application. Therefore, a new certificate has exactly the same content as the certificate to which it relates. It only differs in respect of: a new key pair, a new certificate serial number, a new validity period and a new CCK signature. Furthermore, changes to the certificate's distinguished name are acceptable.

CCK certificates are also subject to certificate renewal with key changeover procedure. New cryptographic keys and the CCK certificate are generated not later than:

- two years before expiry date of the currently used certificate (in the case of NBP Enterprise CA)
- ten years before expiry date of the currently used certificate (in the case of NBP Root CA)

The procedure is performed by CCK Operators and HSM Operators under the supervision of an System Security Inspector of the PKI NBP system.

4.7.1 Circumstances for certificate renewal with key changeover

A certificate renewal may be requested may for the following reasons:

- expiry of the previous certificate,
- revocation of the previous certificate,
- change of data contained in the certificate,
- change of format (e.g. change of private key carrier).

4.7.2 Who may request certificate renewal?

In accordance with a respective Certification Policy.

4.7.3 Procedures for processing certificate renewal request

In accordance with a respective Certification Policy.

4.7.4 Notification of new certificate issuance

In accordance with a respective Certification Policy.

4.7.5 Confirmation of acceptance of a new certificate

In accordance with a respective Certification Policy.

4.7.6 Publication of a new certificate

In accordance with a respective Certification Policy.

4.7.7 Notification of issuance of certificates to other entities

Not applicable.

4.8 Certificate Modification

Any modification of a certificate requires its renewal, and so the provisions of Chapter 4.7 shall apply.

4.9 Certificate Revocation and Suspension

This chapter sets out the conditions that must be met or occur, for the CCK to have the grounds for certificate revocation or suspension. Although certificate suspension is a special form of revocation, in the chapters to follow we shall distinguish these two terms to emphasize a significant difference between the two: certificate suspension may be cancelled, whereas certificate revocation is final.

Certificate revocation or suspension has a special impact on certificates and the obligations of the subscriber using them. In the course of certificate suspension, or immediately following certificate revocation, the certificate is deemed to be invalid. Certificate revocation or suspension has no impact onto previously incurred liabilities or obligations arising from the observance of the Certification Practice Statement.

Certificate suspension is temporary (it usually continues until the doubts which gave grounds to suspension are clarified). For instance, if a Subscriber has lost control over a private key carrier, s/he should immediately notify the PRU or CCK of this fact, requesting suspension of the certificate related to the key . In case the carrier is found and certainty that the private key has not been compromised, the certificate may be unsuspended (on Subscriber's request), which means its reactivation.

In the case of certificate revocation or suspension, the related private key, if still under control of the Subscriber, should continue to be protected in a manner which secures its credibility for the entire period of certificate suspension and, after it has been revoked, should be stored safely until its physical destruction.

4.9.1 Circumstances of revocation

The basic reasons for certificate revocation include:

- loss of control over a private key associated to the certificate,
- a breach by a Subscriber of the provisions of the Certification Practice Statement or a Certification Policy,
- replacement of a certificate (e.g. data contained in it have changed),
- private key disclosure ,
- termination of the agreement between the NBP and the Subscriber,
- any request for certificate revocation submitted by the person referred to in 4.9.2,
- discontinuity of CCK activities (in such a case, all the certificates issued by the CCK, as well as the certificate of the CCK, are revoked prior to the declared date the discontinuity of CCK activities),
- CCK private key compromise.
- compromise of a cryptographic algorithm (or the associated parameters) related to a given certificate.

4.9.2 Who can request revocation?

Revocation of a Subscriber's certificate can be only requested by:

- the Subscriber indicated in the certificate,
- the director of a department or NBP Regional Branch employing the Subscriber (if the Subscriber is an NBP employee),
- In the case of Subscribers who are not NBP employees – the director of a department or NBP Regional Branch which concluded an agreement with the Subscriber-employing company,
- PRU Operator who can request in the name of the Subscriber or on its own initiative, if s/he has information justifying certificate revocation,
- the CCK Operator – only if CCK ceases its activities or CCK key has been compromised.

The Subscriber indicated in the certificate to be revoked must be notified without delay of the fact that his/her certificate has been revoked.

4.9.3 Procedure for certificate revocation

In the PKI NBP system, there are two procedures enabling certificate revocation:

- **Standard procedure –** used for all certificate templates only during the PRU working hours (7.30-16.00 on week days). Under the standard procedure, an authorised person (referred to in 4.9.2) notifies a PRU of the need to revoke a certificate via a "Cryptographic Service Order Form". The PRU Operator revokes the certificate on the date indicated in the delivered "Cryptographic Service Order Form" or, where no date has been set in the "Order Form", on the first business day following the receipt of the "Order Form".
- **Emergency procedure –** used on business days outside PRU working hours and on holidays. The procedure can be resorted to only as regards specified certificate templates. A detailed description of the emergency procedure for a given certificate template is set out in a respective Certification Policy.

Information whether a specific certificate template is covered by an emergency procedure is contained in the Certification Policy for that certificate template.

4.9.4 Revocation request grace period

Revocation shall be carried out immediately following the processing of the revocation request.

4.9.5 Time limit for the processing of revocation request

Under the standard procedure, revocation request are processed not later than on the first business day following the receipt of such a request.

Under the emergency procedure, revocation requests are processed at a time specified in the applicable Certification Policy.

4.9.6 Requirement to check CRL by the Relying Party

Prior to the use of a certificate issued in the PKI NBP system, a relying party must verify the status of the certificate. It can be made by checking the CRL or via an OCSP service.

Should it be unable to use the OCSP service, the relying party should check the certificate status using the latest valid CRL.

4.9.7 CRL issuance frequency

Each CCK within the PKI NBP system issues a separate CRL. The CRL of the NBP Root CA is updated at least once in 6 months (or without delay following the revocation of a certificate issued by this CA) and is published manually. The CRL of the NBP Enterprise CA is updated every hour and is published automatically. Additionally, in case of certificate revocation related to private key disclosure, a CRL is generated and published by the CCK Operator immediately following the certificate revocation.

4.9.8 Maximum delay in the publication of CRLs

CRLs are published in repositories without undue delay immediately following their generation.

4.9.9 OCSP accessibility

The OCSP service of the PKI NBP system is accessible via http://ocsp.nbp.pl/ocsp.

The website address is accessible both from the NBP intranet and via Internet.

4.9.10 On-line revocation checking requirements

Prior to the use of a certificate issued in the PKI NBP system, a relying party is required to verify the certificate status. It may be done through checking a CRL or using the OCSP service.

4.9.11 Other forms of revocation alerts available

Not applicable.

4.9.12 Special requirements for the revocation of compromised keys

In case private key owned by any CCK has been compromised or is suspected to have been compromised, all measures available are put into action to immediately advise the fact to relying parties referring to the information kept in the PKI NBP-managed repository.

4.9.13 Causes for suspension

A Subscriber's certificate can be suspended in the following cases:

- suspected disclosure of a private key ,
- a request by the Subscriber indicated in a certificate or by some other person listed in 4.9.14.
- when the PRU Operator receives a request to revoke a certificate but is unable to verify the authorisation of the person submitting the request (e.g. under the emergency procedure).

4.9.14 Who can request certificate suspension ?

Suspension of a Subscriber's certificate can be requested solely by:

- the Subscriber indicated in the certificate,
- the director of a department or NBP Regional Branch employing the Subscriber (if the Subscriber is an NBP employee),
- In the case of Subscribers who are not NBP employees – the director of a department or NBP Regional Branch which concluded an agreement with the Subscriber-employing company, the PRU Operator, submitting the request in the name of the Subscriber, or on its own initiative, if s/he has information justifying certificate.

4.9.15 Procedure for requesting certificate suspension and unsuspension

An authorised person (listed in 4.9.14) notifies the PRU of the need to suspend a certificate via a "Cryptographic Service Order Form". Having received the information on this need, the PRU Operator delivers to the CCK a respective request, confirmed with his/her signature, and then notifies the certificate owner of the change in his/her certificate status.

PKI NBP system certificates are also suspended in case of the emergency procedure referred to in 4.9.3. As emergency procedure does not allow for a complete identity verification of the notifying person, a CCK Operator suspends a certificate until the receipt of a respective "Cryptographic Service Order Form" (the "Order Form" may concern the request for either a certificate revocation or unsuspension).

4.9.16 Suspension period limits

A certificate suspension period is not limited.

4.10 Certificate Status Verification Services

4.10.1 Operational characteristics

Information on the status of certificates issued in the PKI NBP system can be obtained based on CRLs published in a repository (see Chapter 2.1), or the OCSP service accessible at http://ocsp.nbp.pl/ocsp.

Information on certificate revocation is provided on each list published within the validity period of this certificate and on the first list published after that period lapses.

4.10.2 Service availability

Certificate status validation services are available 24 hours a day.

4.10.3 Additional features

Not applicable.

4.11 End of Subscription

A Subscriber is deemed to have ceased using trust services in the following cases:

- the Subscriber's certificate validity has expired and the Subscriber has not undertaken actions aimed at renewing the key or modifying the certificate,
- the Subscriber's certificate has been revoked and has not been replaced by another certificate.

4.12 Key Escrow and Recovery

In the PKI NBP system, only private keys used by Subscribers for encryption may be put in escrow (and recovered). CCK private keys and Subscribers' private keys used for creating electronic signatures or authentication are not put in escrow.
Additional information is detailed in respective Certification Policies.

5. Facility, Management and Operational Controls

This Chapter contains the most important information regarding physical, organisational and operational security measures used in the PKI NBP system, among others, during cryptographic key creation, Subscribers' authentication, certificates' publication and revocation, in the course of an audit and creation of backup copies.

5.1 Physical Security Controls

5.1.1 Site location and construction

Elements of the PKI NBP system are located at two centres owned by NBP that are significantly distant from each other.

5.1.2 Physical access

Facilities in which PKI NBP system is located are subject to access control system and are monitored 24 hours a day. Only authorised persons have access to the PKI NBP system infrastructure.

Persons, who are not NBP employees, are allowed to work in the system in the discharge of tasks, specified in agreements concluded by the NBP. The agreements contain provisions that ensure an appropriate level of security of maintenance and repair work, carried out strictly under the supervision of the NBP staff having access to the PKI NBP system.

5.1.3 Power and air-conditioning

To prevent disruptions in business activity caused by black-outs (or power cuts) the PKI NBP system is equipped with a back-up power supply system of power generators.

Adequate air temperature and humidity required in the facilities of the main and back-up centres are provided by air-conditioning systems.

5.1.4 Water exposure

The PKI NBP system's critical elements are located in the facilities with low exposure to flooding risk, also as a result of a damage of the water and central heating system in the building. Should a risk of flooding occur, actions are taken in accordance with the procedures in force in NBP.

5.1.5 Fire prevention and protection

Facilities housing the PKI NBP system components are protected by an automatic fire prevention system. In case of fire hazard, actions are taken in line with the procedures in force in NBP.

5.1.6 Storage system

All devices enabling recording and transmitting information are subject to special control measures, including restricted movement between security zones, in computer centres. 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, are scanned for computer viruses and other malicious software.

Procedures have been put in place for creating back-up copies of system's critical data.

5.1.7 Waste disposal

Redundant paper documents, electronic documents and other data carriers used in the PKI NBP system are destroyed safely, in accordance with regulations in force at NBP.

5.1.8 Back-up copy and archived copy storage

Back-up copies and archived copies are stored in two separate locations. The back-up centre, which secures a complete reconstruction of functionalities of the system, located in the main centre, as well as storage of archived copies is accessible to authorized persons 365 days a year. 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 in the PKI NBP system:

- System Administrators – responsible for the administration of the operation system of servers and workstations within the PKI NBP system, creation of back-up copies and hardware management,
- CCK Operators – responsible for the operation of the Certification Authority,
- HSM Administrators – responsible for the administration of hardware security modules,
- HSM Operators – responsible for the operation of hardware security modules,
- PRU Operators – responsible for Subscriber registration, generation, suspension and revocation of certificates,
- Data Recovery Agents – responsible for the recovery of data encrypted by Subscribers in case of a loss of their private keys,
- Key Recovery Agents – responsible for the recovery of lost private keys used for encryption of Subscriber's mail,
- System Auditors – responsible for reviewing event logs related to CCK activities,
- System Security Inspectors – responsible for system security level oversight.

5.2.2 Number of individuals required to perform each task

All tasks related to the operation and administration of hardware security modules require the presence of at least two persons with appropriate smart cards.

5.2.3 Identification and authentication of each role

Identification and authentication of System Administrators are carried out using a login/password procedure or with the use of cryptographic keys and a certificate.

Other operational members in the PKI NBP system are identified by a certificate, and for authentication they use PIN-protected smart cards.

5.2.4 Roles that require separation of duties

The role of System Administrator must not be combined with any other role.

The role of System Security Inspector must not be combined with any other role.

The role of System Auditor must not be combined with any other role.

5.3 Personnel Controls

5.3.1 Requirements concerning professional qualification, knowledge and experience

Persons playing trusted roles in the PKI NBP system are selected according to their professional qualifications and employed in accordance with the rules of employment in force at NBP. They have knowledge and skills necessary to render services related to electronic signature, hardware and software used for electronic data processing, automatic data processing in telecommunications networks and systems. The persons are appointed by the Director of the Information Technology and Telecommunications Department, the Director of the Security Department or the Director of the NBP Regional Branch, respectively.

5.3.2 Background checks and clearing procedures

In accordance with the rules of employment in force at NBP.

5.3.3 Training requirements

In accordance with the rules of training of NBP staff, the persons playing trusted roles in the PKI NBP system receive training related to the system operation, and, in particular, they:

- become acquainted with the Certification Practice Statement, Certification Policies and the system documentation and procedures;

- attend training courses on the administration of the operational systems installed on PKI NBP servers and workstations;
- participate in training courses on cryptography and the Public Key Infrastructure

5.3.4 Retaining requirements and frequency

In accordance with the rules of training NBP employees.

5.3.5 Frequency and sequence for job rotation

Not applicable.

5.3.6 Sanctions for unauthorised actions

All actions performed in the PKI NBP system are documented and controlled, which enables, in particular, to detect possible unauthorised actions by persons who play trusted roles in the PKI NBP system.

Any breach of security rules, applicable regulations and policies is subject to disciplinary or criminal responsibility set out in separate laws.

5.3.7 Requirements for third party contracting

Not applicable as all persons playing trusted roles in the PKI NBP system are NBP staff.

5.3.8 Documentation supplied to personnel

Personnel performing tasks in the PKI NBP system must have access to the following documents:

- Certification Practice Statement,
- Certification Policies,
- System documentation (in the scope required by the employee's role),
- Procedures relating to the role,
- Scope of duties and authorisations assigned to the performed function.

5.4 Audit Logging Procedures

All significant events that may have an impact on the system security and operation, individual PKI NBP system applications or security systems are logged in the PKI NBP system. Recorded events are archived.

5.4.1 Types of events recorded

The following types of events are identified in the PKI NBP system:

- **Error**: A serious problem, e.g. loss of data or functionality. Error may be instantiated by a failure to load a service at autostart,
- **Warning**: An event which although of minor importance as such may indicate a problem that may arise in the future. Warning may be exemplified by information that there is little space left on the system drive.
- **Information**: Any event which indicates correct operation of an application, driver or service. Correct loading of network interface card is an example of the information event.
- **Audit Success**: Any event subject to audit which was successful. An example of Audit Success is a successful logging-in by a user in the system.
- **Audit Failure**: Any event subject to audit which ended in failure. An example of Audit Failure is a failed attempt to access network drive.

In addition, information on events directly related to CCK activity is sent to the mailboxes of System Auditors:

- Subscriber certificate generation,
- Subscriber certificate revocation/suspension,
- Initiation of CCK operation,
- Termination of CCK operation.

5.4.2 Frequency with which audit logs are processed

Monitoring software has been installed on PKI servers which monitors on an on-going basis the status of the operational system and services related to CCK operations and generates reports for System Administrators. System Administrators analyse the reports as they receive them and, if need be, browse logs directly in the server.

As their daily procedure, System Administrators look through the events a notification of which has been sent to their mailboxes. If necessary, a detailed description of registered events is made.

5.4.3 Period for which audit logs are kept

Event logs are stored for at least 1 month. Additionally, they are archived and archived copies are stored for at least 5 years.

5.4.4 Audit log protection

Only system administrators and auditors have access to event logs.

5.4.5 Audit log backup procedures

Full back-up copies are made once a week, incremental backup copies are created on all business days. Back-up copies and archived copies are stored in the main centre and back-up centre.

5.4.6 Audit data collection system (internal vs. external)

An internal register of audit data stores information on current events for a period of at least 1 month. An external back-up system makes back-up copies of audit data on a daily basis, and generates an archive copy once a month. This enables quick access to audit data from the past 5 years.

5.4.7 Notification to the subject who caused the event

The external monitoring system notifies system administrators of the events taking place. An administrator takes further steps aimed at clarifying the incident and minimizing losses. Moreover, information on the events related to CCK activity (issuance, revocation and suspension of certificates, initiation or termination of CCK operation) is sent to System Auditors' mailboxes.

5.4.8 Vulnerability assessment

The PKI NBP system is subject to periodic internal safety audit. All irregularities detected are corrected. The System Security Inspector is responsible for the system security.

5.5 Records Archival

5.5.1 Types of records archived

The PKI NBP system archives CCK data bases and event logs as well as paper documentation related to PRU activity, in particular to the registration and issuance of Subscriber certificates, that is:

- "Cryptographic Service Order Form"
- "Cryptographic Key Handover Protocol"

5.5.2 Archive retention period

Back-up copies are stored for a period of at least 5 years.

5.5.3 Archive protection

Back-up copies are stored in facilities protected by the access control system.

5.5.4 Archive backup procedures

Archival copies are created once a month.

5.5.5 Requirements for time-stamping records

The PKI NBP system guarantee logging of the time at which the log entries were made. This applies both to the operating system events and to actions like backup copy or archive copy creation. The moment in time in the system comes from an external secure source that establishes the date and time.

5.5.6 Audit data archive system (internal vs. external)

Archived copies are created by an external back-up system.

5.5.7 Procedures to obtain and verify archived information

Only back-up system administrators have access to archived data. Periodic tests are performed to recover selected archived data.

5.6 Key Changeover

Change of the CA keys requires publication of a new public key in the repositories, and notification of Subscribers and relying parties.

To secure the proper operation of PKI NBP system, a new key pair of NBP Enterprise CA is generated not later than 2 years before the expiry date of the currently used CA certificate.

CA's private key is destroyed not later than 3 months after the expiry of a given CA certificate.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and compromise handling procedures

In NBP, there are procedures in place that govern incident handling, inclusive the recovery of the whole system from back-up copies. In the event of a suspected incident, a System Security Inspector is notified. In agreement with a System Administrator, s/he takes appropriate preventive and corrective actions in line with procedures. Actions taken by the Inspector and the Administrator aim to identify the original cause of the incident and, if possible, to prevent their recurrence.

5.7.2 Corruption of computing resources, software and/or data

Individual elements of the PKI NBP system are located in an environment that ensures high accessibility and are deployed at two computing centres distant from each other. If one of the machines fails, its tasks are automatically taken over by the remaining machines. In case of data damage, the data are recovered from back-up copies.

5.7.3 Action procedures in the event of compromise to Authority's private key (CCK or PRU)

In the event a PRU private key is compromised, it is immediately revoked and a new CRL is published. Additionally, CCK log analysis is carried out in order to determine whether the compromised key has been used from the time it is thought to have been compromised to its revocation. In the event over that period the key was illegally used for the issue of certificates – the certificates are revoked as well.

The compromise of a CCK private key entails the inevitable revocation of all certificates signed by the CKK with this compromised private key and publication of a new CRL. Next, new cryptographic keys and a new

of CKK certificate are generated (distinguished name may remain the same, though not necessarily), and cryptographic keys and Subscribers' certificates are subsequently changed. All Subscribers and relying parties should be notified of CKK private key compromise.

5.7.4 Ensuring business continuity following disasters

In order to prevent the impact of a disaster, individual elements of the PKI NBP system are located in an environment that ensures high accessibility and are deployed in two computing centres that are distant from each other. In case of a failure of one of the centres, the other one takes over its role. A business continuity plan has been developed for the system, which contains emergency procedures specifying actions that need to be taken to secure system continuity (in particular, to restore the ability to revoke certificates as soon as possible).

5.8 CCK or PRU Termination

5.8.1 CCK

Prior to terminating its activities, the CCK is required to:

- notify (at least 90 days in advance) all the Subscribers who have valid certificates issued by this CCK and relying parties that use certificates issued by this CCK of its intention to cease activities
- do its utmost for the termination of its activity to cause least possible damage to the Subscribers and relying parties.

Upon the termination of its activities, the CCK is obliged to:

- revoke all certificates that remain valid, irrespective of whether the Subscriber has submitted a revocation request or not,
- notify all Subscribers, PRU and relying parties of the termination of its activities.

A CCK is obliged to destroy its private keys not later than 3 months after the termination of its activities.

5.8.2 PRU

At least 90 days prior to the scheduled termination of its activities, the PRU is required to notify the CCK to that effect. Immediately following the termination of its activities, the PRU is obliged to transfer all documentation concerning the Subscribers to the CCK (or to some other PRU designated by the CCK).

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

Cryptographic keys of NBP Root CA and NBP Enterprise CA are generated in hardware security modules with the FIPS 140-2 Level 3 certification.

Rules governing the generation of Subscribers' cryptographic keys are detailed in respective Certification Policies.

6.1.2 Delivery of private keys to subscribers

In accordance with a respective Certification Policy.

6.1.3 Delivery of the public key to the certificate issuer

In accordance with a respective Certification Policy.

6.1.4 Delivery of the public key to the CKK

Public keys of NBP Root CA and NBP Enterprise CA are available in the repository (see Chapter 2.1). In special cases, they may be delivered to a Subscriber or a relying party via e-mail or on a carrier.

6.1.5 Key sizes

Cryptographic keys of NBP Root CA are 4096 bits and NBP Enterprise CA keys are 2048 bits. The size of Subscribers' cryptographic keys is detailed in a respective Certification Policy.

6.1.6 Public key generation parameters and quality checks

Public keys are encoded pursuant to RFC 5280 and PKCS#1.

The algorithm of all generated cryptographic keys is the RSA.

6.1.7 Key usage purposes (KeyUsage field in X.509 v3)

In accordance with a respective Certification Policy.

Cryptographic keys of NBP Root CA and NBP Enterprise CA may be used exclusively to:

- Certificate Signing,
- CRL Signing,

- Off-line CRL Signing.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards

NBP Root CA and NBP Enterprise CA use separate hardware security modules certified with FIPS 140-2 Level 3 certificate.

All operations related to management of security modules, including those involving cryptographic keys contained in the modules, require the use of smart cards assigned to HSM Administrator or HSM Operators.

6.2.2 Private key multi-person (k of n) control

The private keys of the NBP Root CA and NBP Enterprise CA are exclusively protected by the so-called indirect secret sharing scheme. Under the scheme, a symmetric key used for encrypting the CA private key is shared. A symmetric key is divided into 9 parts saved on PIN-secured smart cards delivered to HSM Operators. It is necessary to use at least two such cards to reconstitute the key, and is possible to do so only inside the HSM device.

6.2.3 Escrow of private keys

See Chapter 4.12.

6.2.4 Private key back-up copies

Copies of the CCK private keys are created by means of the mechanisms built in hardware security modules used by the PKI NBP system and are protected in a similar way as private keys protected by cryptographic modules.

6.2.5 Private key archive

The CCK private keys are not archived.

The rules of archiving Subscribers' private keys are laid down in respective Certification Policies.

6.2.6 Private key transfer into or from a cryptographic module.

Outside the cryptographic module, the private keys of the NBP Root CA and NBP Enterprise CA are only in an encrypted form, and their decryption requires the use of two cards of CCK Operators and is possible only inside the cryptographic module. The transfer of the CCK private key into a cryptographic module consists in its encrypted version being downloaded into the cryptographic module, re-constitution of a symmetric key (from the CCK Operators' cards) used to encrypt the private key and decryption of the

private key. Transferring of a private key from the cryptographic module also requires the use of two cards of CCK Operators and consists in exporting the encrypted form of a CCK private key to a file.

6.2.7 Private key storage in a cryptographic module

The private keys of the NBP Root CA and NBP Enterprise CA are generated directly in the hardware security module and occur in an unencrypted form only inside the module. When the CCK private key is transferred from a cryptographic module, it is encrypted and its decryption requires the use of two CCK Operators' cards and is only possible inside the cryptographic module.

6.2.8 Private key activation method

The CCK private key is activated by its being transferred into a cryptographic module and next decrypted inside the module. This operation involves at least two HSM Operators who have smart cards with parts of the deciphering key. The deciphered CCK private key is active until the end of CA's work session (e.g. server restart or shutdown, stopping the service).

6.2.9 Private key deactivation method

Deactivation of the NBP Enterprise CA key is possible only by ending the CA work session (e.g. server restart or shutdown, stopping the service). It can be done only by the System Administrator or CCK Operator.

6.2.10 Private key destruction method

A CCK private key is destroyed by its secure deletion from the cryptographic module. This can be done via software attached to the module or by a "suicide button" which is in the module's front panel.

In accordance with the procedures, CCK cryptographic keys are destroyed not later than 3 months after the related certificate has expired (or has been revoked). The "suicide button" serves to immediately clear the module memory and is used in case of direct threat to the security of the CCK private key.

In addition, all data stored in the cryptographic module memory are deleted when the module is in transport, delivered to an external business (e.g. due to necessary repair work) or it is withdrawn from use.

6.2.11 Cryptographic module classification

See 6.2.1.

6.3 Other Aspects of Key Management

6.3.1 Public key archive

Public keys are archived (as certificates), and archive copies are stored for at least 5 years.

6.3.2 Usage periods for public and private keys

The lifetime of the public key is specified in the Validity field of each public key certificate (see 7.1). The validity period of the private key is the same as that of the public key.

The table below presents the CCK usage periods:

CCK keys usage periods:

Name of CCK	Type of key	Usage period[2]
NBP Root CA	Public/private	15 years / 25 years
NBP Enterprise CA	Public/private	5 years / 7 years / 10 years

The usage periods of Subscribers' keys are set out in Certification Policies.

6.4 Activation Data

Activation data are used for the activation of private keys of the PRU, CCK and Subscribers. They are mostly used for subject authentication and private key access control.

In the PKI NBP system, there are two types of activation data:

- passwords and PIN codes that secure Subscribers' private keys,
- smart cards with components of shared secret, which after installation in the system enable the reconstitution of the CCK private key.

6.4.1 Generation and installation of activation data

Data activating Subscriber's private key (password or PIN) are set by the PRU Operator at the time of generating a cryptographic key. When cryptographic keys are delivered to a Subscriber, s/he is informed by the PRU Operator that they should change the data and set them themselves.

Shared secrets used for the protection of the CCK private keys are generated in accordance with the requirements specified in Chapter 6.2, and are saved on smart cards assigned to HSM Operators. Smart cards are PIN protected.

[2] The first value corresponds to the keys generated before 2 June 2014, and the second value corresponds to the keys generated after 2 June 2014. In the case of NBP Enterprise CA, the third value corresponds to the keys generated in 2016.

6.4.2 Activation data protection

Activation data in the form of passwords and PINs should be remembered (and not saved) by a Subscriber. If the need arises to save the data, this data carrier should not be stored together with the private key to which the data pertain. Smart cards used in the PKI NBP system are blocked after a PIN is entered erroneously 5 times. The card must be unblocked through the PRU.

Smart cards with components of a shared secret are stored by HSM Operators in facilities protected by an access control system. PIN codes protecting the cards are not stored at the same place as the cards.

Additionally, CCK private key activation requires the use of at least two cards assigned to HSM Operators, and in order to perform the activation the cryptographic module needs to be configured accordingly.

6.4.3 Other activation data aspects

Not applicable.

6.5 Computer System Security Controls

Information related to control of computer systems security at NBP is subject to secrecy and can only be revealed to authorised persons. All elements of the PKI NBP system are protected in line with NBP internal regulations, including the provisions of the Security Policy at NBP. All components of the PKI NBP system, in particular, are subject to antivirus protection.

6.5.1 Specific security technical requirements

Information related to the technical requirements for computer systems' specific security at NBP is subject to secrecy and can only be revealed to authorised persons.

6.5.2 Computer security evaluation

Information related to evaluation of computer systems' security at NBP is subject to secrecy and can only be revealed to authorised persons.

6.6 Life Cycle Security Controls

Information related to the life cycle of computer systems technical security at NBP is subject to secrecy and can only be revealed to authorised persons.

6.6.1 System development controls

The PKI NBP system is monitored on an on-going basis by the System Security Inspector (IBS). Prior to implementation of any changes into the system, they are consulted with the IBS, and tests (including security tests) are carried out. After the changes are implemented, the system documentation is updated.

6.6.2 Security management controls

In accordance with the NBP internal regulations.

6.6.3 Life cycle security controls

This Statement does not stipulate any requirements in this respect.

6.7 Network Security Controls

Information related to computer network security controls at NBP is subject to secrecy and can only be revealed to authorised persons.

6.8 Time stamping

Not applicable.

7. Certificate and CRL Profiles

Profiles of certificates and CRLs comply with the formats laid down by ITU-T X.509 v3 standard.

7.1 Certificate Profile

In compliance with X.509 v.3 standard, a certificate is a sequence of three fields, of which the first one contains certificate content (tbsCertificate), the second one – information on the type of algorithm used for signing the certificate (signatureAlgorithm), and the third one – a digital signature, entered on the certificate by the CCK (signatureValue).

The content of the certificate contains values of main fields and extensions (standardized, specified by the norm, and private ones, specified by a certification authority).

- In the PKI NBP system, certificates contain the following main fields:
- Version: the third version (X.509 v3) of certificate format,
- Serial Number: certificate serial number,
- Signature Algorithm: identifier of the algorithm used by the CCK ,
- Issuer: CCK distinguished name,
- Validity Period: the certificate validity date specified by the commencement (not before) and end (not after) dates,
- Subject: subscriber's distinguished name,
- Public Key: value of the public key and algorithm identifier,
- Signature: s signature generated and encoded pursuant to the RFC 5280 standard

Field values of certificates issued in the PKI NBP system are assigned in accordance with the table below:

Name of Field	Field Content	
Version	V3	
Serial Number	Unique certificate serial number within CCK	
Signature Algorithm	SHA1RSA[3]/Sha256RSA[4]	
Issuer	Common name (CN)	NBP Root CA / NBP Enterprise CA
	Organisational Unit (OU)	Centrum Certyfikacji Kluczy NBP
	Organisation (O)	Narodowy Bank Polski

[3] For certificates issued before 10.10.2016.
[4] For certificates issued after 10.10.2016.

	Locality (L)	Warszawa
	Country (C)	PL
Not before	Universal Time Coordinated based	
Not after	Universal Time Coordinated based	
Subject	Subscriber's distinguished name compliant with X.501 requirements. Detailed information regarding the content of this field is contained is a respective Certification Policy	
Public Key	Field is encoded in compliance with RFC 5280 and contains information on the RSA public key (key identifier, size and value)	
Signature	A certificate signature generated and encoded in compliance with RFC 5280 requirements	

7.1.1 Version number

All certificates issued in the PKI NBP system comply with X.509 v3.

7.1.2 Certificate extensions

An extension in a certificate may be classified as critical or non-critical. If an extension is defined as critical, the application supporting certificate usage must reject every certificate containing an unrecognized critical extension. On the other hand, extensions defined as non-critical may be omitted.

Certificates issued in the PKI NBP system have the following extensions:

- KeyUsage
- Extended KeyUsage
- Subject Key Identifier
- Authority Key Identifier
- Certificate Template Information (or "Certificate Template")
- CRL Distribution Points
- Authority Information Access
- Application Policies
- Subject Alternative Name
- SMIME editor option (certificates related to encryption only)
- Basic Constraints (selected certificates only)

Depending on a certificate template, extensions may be critical. Detailed information is presented in respective Certification Policies.

7.1.3 Algorithm Object Identifiers

The field contains a cryptographic algorithm identifier which describes the algorithm used by a certification authority to place a digital signature on a certificate.

In the certificates issued in the PKI NBP system, the field has the following value:

For certificates issued before 10.10.2016

Sha1RSA OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

For certificates issued after 10.10.2016

sha256RSA OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

7.1.4 Name formats

In accordance with a respective Certification Policy.

7.1.5 Name constraints

In accordance with a respective Certification Policy.

7.1.6 Certification Policy Object Identifiers

In accordance with a respective Certification Policy.

Certification Policies in the PKI NBP system have identifiers that start with 1.3.6.1.4.1.31995.1

7.1.7 Use of the "PolicyConstraints" extension

Not applicable.

7.1.8 Syntax and semantics of the "PolicyQualifier"

"Application rules" extension contained in a certificate includes the URL address indicating the Certification Practice Statement and Certification Policy that governs the certificate.

7.1.9 Processing semantics for the critical "CertificatePolicy" extension

To secure the highest compatibility, the "Application rules" extension is non-critical.

7.2 CRL Profile

CRL consists of three fields. The first field (tbsCertList) contains information on revoked certificates, the second one (signatureAlgorithm) – information on the type of algorithm used for signing the list, and the third one (signatureValue) – a digital signature placed on a CRL by the CCK.

Text field tbsCertList is a sequence of mandatory and optional fields. Mandatory fields denote a CRL issuer, whereas optional ones contain information on revoked certificates and CRL extensions.

The table below presents principal fields with a description and CRL extensions:

Name of field	Contents	
Version	V2	
Issuer	Common name (CN)	NBP Root CA / NBP Enterprise CA
	Organisational Unit (OU)	Centrum Certyfikacji Kluczy NBP
	Organisation (O)	Narodowy Bank Polski
	Locality (L)	Warszawa
	Country (C)	PL
Effective date	Universal Time Coordinated based	
Next Update	Universal Time Coordinated based	
Revoked Certificates	Serial number	Unique certificate serial number within CCK
	Revocation date	Primary time in UTC (Universal Coordinate Time)
	CRL Reason Code	Additional information on the cause of revocation (*) – optional field
Signature Algorithm	Sha256RSA	
Authority Key Identifier	Field encoded pursuant to RFC 5280, containing RSA key identifier used for authorising a signature under the list	
CA Version	Numerical field. Its value is increased any time a private key of the CCK issuing the list is changed.	

CRL Number	Subsequent number of the CRL
Next CRL Publish	Primary time in UTC (Universal Coordinate Time)
Signature	Signature under CRL generated and encoded in compliance with RFC 5280 requirements

(*) – The "Reason Code" field may contain the following entries:

- Key compromise (1)
- CA compromise (2)
- Affiliation changed (3)
- Superseded (4)
- Cessation of operation (5)
- Certificate hold (6)

8. Compliance Audit and Other Assessment

8.1 Frequency or Circumstances of Assessment

The PKI NBP system is subject to periodical internal or external audit, carried out at least every 3 years. Additionally, a System Security Inspector performs a Risk Analysis of the PKI NBP system with a frequency defined in separate regulations. The Risk Analysis aims to assess the level of risk of system security. The Risk analysis is carried out in compliance with the methodology in force at NBP.

8.2 Identity/Qualifications of the Auditor

Auditors must have knowledge and qualifications in the PKI.

8.3 Relationship between the Assessor and the Entity Being Assessed

An Internal Audit Department Auditor is an NBP employee and s/he audits a system managed at another department. An external auditor is by no means associated with the PKI NBP system.

8.4 Aspects Covered by Controls

The aim and scope of the audit work are specified in accordance with the laws in force at NBP and may, in particular, include: the operation of the system, compliance of the services provided with the Certification Practice Statement and Certification Policies, and compliance of actions with the laws in force.

8.5 Actions Taken as a Result of Deficiencies Found during an Audit

In accordance with the laws in force at NBP.

8.6 Notification of the Results

In accordance with the laws in force at NBP.

9. Other Business and Legal Matters

9.1 Fees

NBP charges no fees for the issue of cryptographic keys or certificates, granting access to the repository on the www.pki.nbp.pl/pki website, or for providing an OCSP service.

9.2 Financial Responsibility

The provision by NBP of trust services under the PKI NBP system does not require NBP to conclude a liability insurance contract against damage to the users of trust services incurred during the provision of trust services, unless the parties agree otherwise or such an obligation arises from generally applicable laws.

9.3 Confidentiality of Business Information

NBP guarantees that all information compiled for the purposes of the PKI NBP system is stored and processed pursuant to the applicable legal regulations .

Information restricted as business secrets of entities with which NBP has concluded a contract under the PKI NBP system is also protected.

9.3.1 Scope of confidential information

Any information related to trust services rendered by NBP in the PKI NBP system that has not been marked Public is treated as a business secret.

Information pertaining directly to the activities of CCK and PRU (including private keys, technical documentation, systemic and emergency procedures), is protected under the Act on Trust Services.

9.3.2 Non-confidential information

Information related to the trust services rendered by NBP under the PKI NBP system includes:

- Certification Practice Statement,
- Certification Policies,
- CCK Certificates,
- PRU and CCK contact data,
- CRL published in a repository.

9.3.3 Duty to maintain professional secrecy

All NBP employees performing tasks related to the provision of certification services are obliged to keep secret the information referred to in Chapter 9.3.1. As regards external entity staff performing tasks

commissioned by NBP, the obligation to keep the information secret is governed by the agreements concluded by those entities with NBP.

9.4 Representations and Warranties

The Chapter presents all obligations the parties to this Certification Practice Statement, i.e. CCK, PRU, Subscribers and Relying Parties are subject to.

9.4.1 Obligations of CCK

Within the framework of services it renders in the PKI NBP system, the CCK Operator is obliged to:

- observe the provisions of this Certification Practice Statement and of Certification Policies,
- protect CCK private keys and ensure security of the generation of Subscribers' cryptographic keys,
- generate and manage certificates pursuant to x.509 v3 standard,
- publish, without undue delay, generated CCK certificates in the repository referred to in Chapter 2.1,
- revoke certificates in accordance with the provisions of Chapter 4.9,
- publish, without undue delay, CRLs in the repository referred to in Chapter 2.1,
- Ensure accessibility of most recent CRLs, CCK certificates, Certification Practice Statement and Certification Policies in the repository referred to in Chapter 2.1,
- provide trust services in conformity with the provisions of law and in line with the approved PKI NBP procedures,
- ensure that any action related to trust services provided in the PKN NBP system is conducted by authorised persons only,
- electronically store and archive documents and data directly related to the provision of trust services in a manner that ensures security of the data and documents.

9.4.2 Obligations of PRU

As part of the services provided within the PKI NBP system, the PRU Operator is obliged to:

- observe the provisions of this Certification Practice Statement and Certification Policies,
- ensure that requests submitted to the CCK contain true data of a Subscriber and are free from error,
- notify CCK on an on-going basis of any problems found in the PKI NBP,
- electronically store and archive documents and data directly related to the provision of trust services in a manner that ensures security of the data and documents,
- carry out Subscriber verification in line with the provisions of a Certification Policy and the PKI NBP system procedures,
- cooperate with a Subscriber in the process of cryptographic key generation only after a correct verification of the Subscriber.

9.4.3 Obligations of Subscribers

A Subscriber is obliged to:

- provide all data required for the issue of a certificate in the PKI NBP system and confirm their veracity,
- immediately notify the PRU on any change to the above mentioned data,
- abide by the provisions of this Certification Practice Statement an respective Certification Policies,
- ensure due protection of his/her private key and key activation data,
- use the cryptographic keys and certificates of the PKI NBP system only in the scope defined in the certificate (KeyUsage and ExtKeyUsage fields),
- immediately request revocation of a certificate in case of compromise of its corresponding key.

9.4.4 Obligations of the Relying Party

A Relying Party which uses PKI NBP system certificates is obliged to:

- rely on the certificates only in the scope delineated in the certificate (KeyUsage and ExtKeyUsage fields),
- carry out a full verification of a Subscriber certificate before using it,
- notify the PRU or a CCK of any instance of the certificate being used by an unauthorised person or in an unintended manner.

9.5 NBP Liability Exemption

Issuance of a certificate in the PKI NBP system does not make NBP an agent, trustee or representative of the Subscriber for whom the certificate was issued.

9.6 Limitations of Liability

NBP shall bear no responsibility for the performance by a Relying Party of a correct and diligent verification of each signature and/or certificate which the Relying Party intends to rely on.

The Relying Party shall be held exclusively liable for relying on a signature or a certificate the verification of which has been incomplete or negative.

NBP shall bear no responsibility for the Subscriber's use of cryptographic keys and certificates not in accordance with their intended purpose laid down in this Statement or respective Certification Policies.

In its capacity as the PKI NBP system owner, NBP shall bear no liability or responsibility for the content of documents (or other data) signed or encrypted with the use of cryptographic keys and certificates generated in this system.

10. Personal Data Protection

In the PKI NBP system, personal data are processed both on paper and in an electronic form and are protected in accordance with the applicable law. Personal data incorporated into a Subscriber's distinguished name are imported from the Active Directory catalogue service or are manually entered into the system by the PRU Operator, based on submitted "Cryptographic Service Order Form".

Under the PKI NBP system, the Subscriber's data processed in paper form are the following:

- Subscriber's name and surname,
- ID series and number,
- place of employment,
- e-mail address,
- office phone number,
- signature.

Paper and electronic documents containing personal data to be used in the PKI NBP system are subject to safeguards to prevent abuse or unlawful access or transfer, as provided for in the applicable law.

Personal data related to PKI NBP are stored throughout the period of validity of the certificate and for 5 years (in the case of certificates for an electronic signature or authentication) or 10 years (in the case of certificates for encryption) after expiry of the certificate of the person who the data concerns. After this period, the certificates are removed from the PKI NBP system and archive copies containing these certificates are destroyed.

Attachment A – CCK Self-signed certificates

NBP Root CA self-signed certificate	
Date of issue	20 November 2008
Date of expiry	20 November 2018
Subject key identifier	8b c9 e4 49 27 49 69 01 6e f0 38 3a 24 99 18 9d 3f e9 d8 81
Certificate in base64 format	-----BEGIN CERTIFICATE----- MIIEmDCCA4CgAwIBAgIQJus6lT8+yo9He8+kWdi6IjANBgkqhkiG9w0BAQU FADB/MQswCQYDVQQGEwJQTDERMA8GA1UEBxMIV2Fyc3phd2ExHTAbBgNVBA oTFE5hcm9kb3d5IEJhbmsgUG9sc2tpMSgwJgYDVQQLEx9DZW50cnVtIENlc nR5ZmlrYWNqaSBLbHVjenkgTkJQMRQwEgYDVQQDEwtOQlAgUm9vdCBDQTAe Fw0wODExMjAyMTA3MzRaFw0xODExMjAyMTE1NTNaMH8xCzAJBgNVBAYTAlB MMREwDwYDVQQHEwhXYXJzemF3YTEdMBsGA1UEChMUTmFyb2Rvd3kgQmFuay BQb2xza2kxKDAmBgNVBAsTH0NlbnRydW0gQ2VydHlmaWthY2ppIEtsdWN6e SBOQlAxFDASBgNVBAMTC05CUCBSb290IENBMIIBIjANBgkqhkiG9w0BAQEF AAOCAQ8AMIIBCgKCAQEA39jrXwi+SZrBKGkUBqcKkHG55r/WQQ4zJmZk/Cp XY0qrJ79BX2c8mwPKd59hlux6QO08E/Bb+vTRk2rG8gweQSk/1SNEo6d+dI XMDJk1aGl7wXaVQLSo7gTwvVoOhuVSP6Fc9ycR1v1mLfKVHSUktDLkJ7UFE 2C3f2XmrbXZjPKB6J/1FQcosuLTFwK/hnD5bJz0l6LHJG6aDxmnjzdy1Xsf Rr9XM3Dkc0OZDYKJcbscPnQoIKRQHc3CCMDcuk15p0q9Wl8RKQxWfCEkkZn ef3F0Z9Em1syUIWBK9KHji01pZ8ekewQ4dtoDznlTBu4mmmImXweVOmK4v4 98rBAg5QIDAQABo4IBDjCCAQowCwYDVR0PBAQDAgGGMA8GA1UdEwEB/wQFM AMBAf8wHQYDVR0OBBYEFIvJ5EknSWkBbvA4OiSZGJ0/6diBMBAGCSsGAQQB gjcVAQQDAgEAMIG4BgNVHSAEgbAwga0wgaoGCysGAQQBgfl7AQEBMIGaMHQ GCCsGAQUFBwICMGgeZgBOAEEAUgBPAEQATwBXAFkAIABCAEEATgBLACAAUA BPAEwAUwBLAEkAIABDAGUAcgB0AGkAZgBpAGMAYQB0AGUAIABQAHIAYQBjA HQAaQBjAGUAIABTAHQAYQB0AGUAbQBlAG4AdDAiBggrBgEFBQcCARYWaHR0 cDovL3BraS5uYnAucGwvcGtpLzANBgkqhkiG9w0BAQUFAAOCAQEAdK2dzfm 7m0eL/a4mfgY2fTIrm3scoRyVi6AknaTnz8ie8aGdXm0H/fONQ6anFC854J zE/6PGUsxeBgr3sGD5cVOxziKYMjoObv42VNvYsQk9subjbUDKn8xOEawfH Gai+U5Xy4m7LDTfN8ujpcjnM3NC22sf3Y2WZnaCZQv/aJse5rd5v9kUNryU iZlCGHf4WV0Wq1cZ3zY0zIK2dhTHh7EdER/NLkR/u94rY0FyMhwxkFrHJZ/ MqEEXrzbyqPOqPAqdnCR3Q1kwc/V+mduHH1Iw9ffd538WYMXoqZEm0HprSz sd0ZyW1I8wP8cKnAl4b3GqmvdKmno8coXpSJIQdA== -----END CERTIFICATE-----

NBP Root CA self-signed certificate	
Date of issue	2 June 2014
Date of expiry	2 June 2034
Subject key identifier	7a 84 99 54 a5 27 11 4b 19 51 d5 a6 09 c2 e0 b4 0f 7e dc 7f
Certificate in base64 format	-----BEGIN CERTIFICATE----- MIIGyDCCBLCgAwIBAgIQH0b7yZ28J49K1aOLMcDvmjANBgkqhkiG9w0BAQUFADB/ MQswCQYDVQQGEwJQTDERMA8GA1UEBxMIV2Fyc3phd2ExHTAbBgNVBAoTFE5hcm9k b3d5IEJhbmsgUG9sc2tpMSgwJgYDVQQLEx9DZW50cnVtIENlcnR5ZmlrYWNqaSBL bHVjenkgTkJQMRQwEgYDVQQDEwtOQlAgUm9vdCBDQTAeFw0xNDA2MDIwODAwMjFa Fw0zNDA2MDIwODEwMjFaMH8xCzAJBgNVBAYTAlBMMREwDwYDVQQHEwhXYXJzemF3 YTEdMBsGA1UEChMUTmFyb2Rvd3kgQmFuayBQb2xza2kxKDAmBgNVBAsTH0NlbnRy dW0gQ2VydHlmaWthY2ppIEtsdWN6eSBOQlAxFDASBgNVBAMTC05CUCBSb290IENB MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAtYa0OpGqVgcOb2hYI3Ur 8X8odx414U/oWjAT0sXxt+LC0dyX9yLzq7ukpyOrpeVuya9PBBj0+t6iS2EYeCcl eK0+9EM4YlwEhAVs78SzaQZ9anIwgyr9JMzJOm4RFyI09pbNea/FWMIsOso8wf0T URDc1YLyjPGOEQHa7FnLsfm1CqdJ+1podMkKZ1B5XWus9J3xXS70c6u4kiBaui8h 4r9lOazLHBw3x0o0+zpsylXcHCORgIZsGzBJHImo3FHKyRS/hWF5koittfZQNf9I vNVWoKwUpRb2JweBHqG5hGT52jAlhDNRn0OxStqdLgynLmgo3tMtGR32Yy8WXXaR /k0/1foSaC0F+NBVjn+vZMsCqfi61Ze2VpzacNQJyEl6w0WCSJcBixWm2f5/jojr bamXTBtJa4ROquzGCybtctVnIKRHVoSRyVSlfIw6bZmlh+/3jIoWGzGtoZMBC9I4 qt1EH6rP+69lzZuUeaORFpVIKs02j2m1aoCe5BKO1XqW6YQYFDY55XPALBKaYYJT RPx3yGJ11d+fBetVdIXVpipfZLW18sZobJ/8zPNwKZ+kr9zeo9e3BaqwncO34YuP OhZeGPJfKRSjecarJyvjCNMB3H7VxTeSYcuAoEOG/qkuM4ydN3NDUSrwxGbWJSPP e9UKUt4Hec9pEwzZWOdosssCAwEAAaOCAT4wggE6MAsGA1UdDwQEAwIBhjAPBgNV HRMBAf8EBTADAQH/MB0GA1UdDgQWBBR6hJlUpScRSxlR1aYJwuC0D37cfzASBgkr BgEEAYI3FQEEBQIDAQABMIHBBgNVHSAEgbkwgbYwgasGCysGAQQBgfl7AQEBMIGb MHQGCCsGAQUFBwICMGgeZgBOAEEAUgBPAEQATwBXAFkAIABCAEEATgBLACAAUABP AEwAUwBLAEkAIABDAGUAcgB0AGkAZgBpAGMAYQB0AGUAIABQAHIAYQBjAHQAaQBj AGUAIABTAHQAYQB0AGUAbQBlAG4AdDAjBggrBgEFBQcCARYXaHR0cDovL3BraS5u YnAucGwvcGtpLwAwBgYEVR0gADAjBgkrBgEEAYI3FQIEFgQUFuKyXPpCWrxf4hM8 SvJyEbAY9m0wDQYJKoZIhvcNAQEFBQADggIBAGGymMtnADGmZJ1y8qsRwi1QabbY B5HP+r04LaIpuzH+/vB/2BJJ3y8ZMWdiYXKYJ9wxk/PxdYFiLi/zyBnthu094ryg bAs6Q3/J4tHXFxnZyaj0rwQff8CqozTVz0h6d9OhnTKz28D63TdglQNPJpgjmMEk NlnU8pRr3G9xocArqIO/qzyxZpdn0PCxI9mAuYC0oinVlQMHZK3HQGMsv9k26uBx x2zzRuhhXENP0pAvUwlUL9ZHKLOhssF+BVlv2oVfMFXc2BaYazL4GpSa8s13BqPZ dYSKIDVm5O2IelQjeft2BP0d/lOv0S3w5wBoq9La9P8LPUgC7GWKr56PdfuNJDoC ELmC4ZIAvCo+M7Y2ejsCLUhTsU8XBkMwzpHcNotnyGtP16oO6GDTz+KIKji47dGA g3G0fM/OrJNP7ETsDvjZqtSJZK8WFj4oJE8MqmfVfSh9bieNJ2Mi7GpNCiDHu/lJ nL81nv2YlmLOBlcud6G40vP0eloHiFTdElser3rgVdhhVcgwH28YIQLmwpaW1bb6 sN+fN62+uzNCdvt+Ff3P/ni5w7MidPVKmIZFmJmXGDQSMKUajvC+qYPKoPJeai8y 7RccQ0wZjZNRJ4wY0cOOZHypvNeUl8xWEZvICpWtpg9dgY9W13wu/0F5wbSfWr92 emAWBhkJQqf/p1Ak -----END CERTIFICATE-----

NBP Root CA self-signed certificate	
Date of issue	2 June 2014
Date of expiry	16 September 2036
Subject key identifier	7a 84 99 54 a5 27 11 4b 19 51 d5 a6 09 c2 e0 b4 0f 7e dc 7f
Certificate in base64 format	-----BEGIN CERTIFICATE----- MIIGyDCCBLCgAwIBAgIQRbh02uAa7rBAz/K54enudzANBgkqhkiG9w0BAQsFADB/ MQswCQYDVQQGEwJQTDERMA8GA1UEBxMIV2Fyc3phd2ExHTAbBgNVBAoTFE5hcm9k b3d5IEJhbmsgUG9sc2tpMSgwJgYDVQQLEx9DZW50cnVtIENlcnR5ZmlrYWNqaSBL bHVjenkgTkJQMRQwEgYDVQQDEwtOQlAgUm9vdCBDQTAeFw0xNDA2MDIwODAwMjFa Fw0zNjA5MTYxMzQ5MjhaMH8xCzAJBgNVBAYTAlBMMREwDwYDVQQHEwhXYXJzemF3 YTEdMBsGA1UEChMUTmFyb2Rvd3kgQmFuayBQb2xza2kxKDAmBgNVBAsTH0NlbnRy dW0gQ2VydHlmaWthY2ppIEtsdWN6eSBOQlAxFDASBgNVBAMTC05CUCBSb290IENB MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAtYa0OpGqVgcOb2hYI3Ur 8X8odx414U/oWjAT0sXxt+LC0dyX9yLzq7ukpyOrpeVuya9PBBj0+t6iS2EYeCcl eK0+9EM4YlwEhAVs78SzaQZ9anIwgyr9JMzJOm4RFyI09pbNea/FWMIsOso8wf0T URDc1YLyjPGOEQHa7FnLsfm1CqdJ+1podMkKZ1B5XWus9J3xXS70c6u4kiBaui8h 4r9lOazLHBw3x0o0+zpsylXcHCORgIZsGzBJHImo3FHKyRS/hWF5koittfZQNf9I vNVWoKwUpRb2JweBHqG5hGT52jAlhDNRn0OxStqdLgynLmgo3tMtGR32Yy8WXXaR /k0/1foSaC0F+NBVjn+vZMsCqfi61Ze2VpzacNQJyEl6w0WCSJcBixWm2f5/jojr bamXTBtJa4ROquzGCybtctVnIKRHVoSRyVSlfIw6bZmlh+/3jIoWGzGtoZMBC9I4 qt1EH6rP+69lzZuUeaORFpVIKs02j2m1aoCe5BKO1XqW6YQYFDY55XPALBKaYYJT RPx3yGJ11d+fBetVdIXVpipfZLW18sZobJ/8zPNwKZ+kr9zeo9e3BaqwncO34YuP OhZeGPJfKRSjecarJyvjCNMB3H7VxTeSYcuAoEOG/qkuM4ydN3NDUSrwxGbWJSPP e9UKUt4Hec9pEwzZWOdosssCAwEAAaOCAT4wggE6MAsGA1UdDwQEAwIBhjAPBgNV HRMBAf8EBTADAQH/MB0GA1UdDgQWBBR6hJlUpScRSxlR1aYJwuC0D37cfzASBgkr BgEEAYI3FQEEBQIDAQACMIHBBgNVHSAEgbkwgbYwgasGCysGAQQBgfl7AQEBMIGb MHQGCCsGAQUFBwICMGgeZgBOAEEAUgBPAEQATwBXAFkAIABCAEEATgBLACAAUABP AEwAUwBLAEkAIABDAGUAcgB0AGkAZgBpAGMAYQB0AGUAIABQAHIAYQBjAHQAaQBj AGUAIABTAHQAYQB0AGUAbQBlAG4AdDAjBggrBgEFBQcCARYXaHR0cDovL3BraS5u YnAucGwvcGtpLwAwBgYEVR0gADAjBgkrBgEEAYI3FQIEFgQUm6GXuIy6CD4n5xgP vRi218fNGPQwDQYJKoZIhvcNAQELBQADggIBAK2E1QvrTetbKTeliMEnY0j1W4N0 g5mrDv0ZbQZ7iYiSWbSJAEiPW7YUYcjJJgY6Vd6rhu2uiv8iOAxXOMhBgRtcFoIn qf3/U1Vj2Xlm8sILvkQ4UxBOyGEk3Qt69QnNtTKpjCm+mlyv92Dr6c5BnKrroHdi rxHSXfa53N3UbL+nnUOQBxwKqrgS8VG1OuHkxx/yfDSF+mhMDryhWTQW7P/S2kSN 2+rWiTW3bwzqw6tNEVjItq1So+pDgfX4XJT2gchfmdTw1rNPn7U2UURhlMubtEvx N38cCouOKuF+XWdy3lvKnnbpxrB2UdH1kei1A9+12E0EaV8iIWPNfahTESSZThWA A0GQBxjalckN/z6UdirfuqdoGI5mVAUPuzy0tjl5fk0R1e+Rk4pSPgP4Lm2Q7k3r rOy5w/cIGg6nOZ0EQJRoDxwyuW+xFvaEb/m/pfjaLhKpeq/FrE++Nkc8AdoePy9b Ih2pPIKfLDnOZ9ib9KCq6hIgaDmWoo22q1Oc/gjalqEIKU6EJYx25RgpduOBdEOs ilmLKpa8wlaHM8GXIBz2BDTpXQb6MlS5Y5JG5+YqeCsoGEzcUbBM1327J1+RR5NG SkPDV4Mf0B77Zd7jyqv3djf7//fZgzPbxrfjRpvddjgeJGGIGQUhbJroSJLhz6MJ suTlq0Z5uL6rw/a9 -----END CERTIFICATE-----

NBP Enterprise CA Certificate	
Date of issue	2 June 2014
Date of expiry	2 June 2021
Subject key identifier	d4 36 f2 2d d0 46 2c 20 33 13 84 6d 15 d7 4e 95 21 0b 0f 11
Certificate in base64 format	-----BEGIN CERTIFICATE----- MIIGeTCCBGGgAwIBAgIOGTrdrAf3vUkAAQAAAAowDQYJKoZIhvcNAQEFBQAwfzEL MAkGA1UEBhMCUEwxETAPBgNVBAcTCFdhcnN6YXdhMR0wGwYDVQQKExROYXJvZG93 eSBCYW5rIFBvbHNraTEoMCYGA1UECxMfQ2VudHJ1bSBDZXJ0eWZpa2FjamkgS2x1 Y3p5IE5CUDEUMBIGA1UEAxMLTkJQIFJvb3QgQ0EwHhcNMTQwNjAyMTQzNDQ2WhcN MjEwNjAyMTQzNDQ2WjCBhTELMAkGA1UEBhMCUEwxETAPBgNVBAcTCFdhcnN6YXdh MR0wGwYDVQQKExROYXJvZG93eSBCYW5rIFBvbHNraTEoMCYGA1UECxMfQ2VudHJ1 bSBDZXJ0eWZpa2FjamkgS2x1Y3p5IE5CUDEaMBgGA1UEAxMRTkJQIEVudGVycHJp c2UgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCvtsWnZMpf7sVa a9JYQfekM7ifDcQZxOzhswh+0VEGD4+r7iMnVVcaRlSd2rfajM2IRnuw9fTli3vI EfxZAzNZSkTXiUVvPj9cpR7SkPtK8MuTthnS+tBuClootFsTZ9k5G2T3rfixjY/o 9nxH0lUuzzVw96iIYHHKySNxEBarx0p0bPqSwPhPh4503hwZwI4gz1uIhnl34gzk OGkrUt3sPjHkHNiBhZXM8QQ3xf25w3wXqgTrH4+XFTf2eQjDO0QzcybaE+cCt14f EaN+R5cCmJ7sKQvIi+R8pJPJ6t0j6KLIZE3eqSFA4cLSojlMtJmJsOeIm1EhKLPG DTdhK7XNAgMBAAGjggHqMIIB5jASBgkrBgEEAYI3FQEEBQIDAgACMCMGCSsGAQQB gjcVAgQWBBTdNo7KCYF96qJN/maMKOK0jWu0LTAdBgNVHQ4EFgQU1DbyLdBGLCAz E4RtFddOlSELDxEwgcAGA1UdIASBuDCBtTCBqgYLKwYBBAGB+XsBAQIwgZowdAYI KwYBBQUHAgIwaB5mAE4AQQBSAE8ARABPAFcAWQAgAEIAQQBOAEsAIABQAE8ATABT AEsASQAgAEMAZQByAHQAaQBmAGkAYwBhAHQAZQAgAFAAcgBhAGMAdABpAGMAZQAg AFMAdABhAHQAZQBtAGUAbgB0MCIGCCsGAQUFBwIBFhZodHRwOi8vcGtpLm5icC5w bC9wa2kvMAYGBFUdIAAwGQYJKwYBBAGCNxQCBAweCgBTAHUAYgBDAEEwCwYDVR0P BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHwYDVR0jBBgwFoAUeoSZVKUnEUsZUdWm CcLgtA9+3H8wMQYDVR0fBCowKDAmoCSgIoYgaHR0cDovL3BraS5uYnAucGwvcGtp L3JjYSgxKS5jcmwwPAYIKwYBBQUHAQEEMDAuMCwGCCsGAQUFBzAChiBodHRwOi8v cGtpLm5icC5wbC9wa2kvcmNhKDEpLmNydDANBgkqhkiG9w0BAQUFAAOCAgEAo+aF +tO5ZtuLI7SvsopKHgGvT+/OrY+zrpvWa0pPHy7NKBTUkQ20eejmc93wrYqOSXrS JXqPeI5jQeqMJto6psWKYAsEfWxVbqoCl90c2/J1FkQRcB5tfBTKu5HKrZCklINm uYCb4CrM7REFIPIk3vbBbI3/jAXb/xcoLPowIjw54cfjFCimbAkeXzeqBuAEkkKi KUNz6ghemc+NTzUNQVdPQEvPjNihGh1cyMh7jTPHfXxBlylkh8hN9ggvuXbknoeJ d9o1HPPSgQBfa925GIh9pfcxP12ZlsR+PWPLW4+XYQnICOApdP8datVvwG7d8rTH Q9f0KhtjtV05Crummy9a7RlPWQhZAktJFh8AfIM9chwmZz6u3CrDyBX72uATeKE8 PACtSTExK+6DMnDcnbr5Zg2s+aeTesA/aL1DsWtTa8y5tCHhRuFiHjDN/ETmvHWH Dek/pYDBq29YJ62kPZcdUu99aOhg3AQPuJQaZJbCMnLgXh+obI67N2MK5orM3rrO loPB6A/31qcb0uOSEt1OPxW9YFSQFfNWz9QEaxZbAYpWSAVvt/6cjKJUKFGyVnjy nBbrnZllDslNZmi5GCGzgqw/C3PXdUgYAPbz2p+sF44JTzFZdymxnhcRbU3DnwrG I5q7fUL1G+8QQ5UdqcUqXKN19Nqp9Ar8VsdY+dI= -----END CERTIFICATE-----

NBP Enterprise CA Certificate	
Date of issue	10 October 2016
Date of expiry	10 October 2026
Subject key identifier	d4 36 f2 2d d0 46 2c 20 33 13 84 6d 15 d7 4e 95 21 0b 0f 11
Certificate in base64 format	-----BEGIN CERTIFICATE----- MIIGejCCBGKgAwIBAgIOGTrdrAf3vUkAAgAAAEswDQYJKoZIhvcNAQELBQAwfzEL MAkGA1UEBhMCUEwxETAPBgNVBAcTCFdhcnN6YXdhMR0wGwYDVQQKExROYXJvZG93 eSBCYW5rIFBvbHNraTEoMCYGA1UECxMfQ2VudHJ1bSBDZXJ0eWZpa2FjamkgS2x1 Y3p5IE5CUDEUMBIGA1UEAxMLTkJQIFJvb3QgQ0EwHhcNMTYxMDEwMTAzMjQyWhcN MjYxMDEwMTAzMjQyWjCBhTELMAkGA1UEBhMCUEwxETAPBgNVBAcTCFdhcnN6YXdh MR0wGwYDVQQKExROYXJvZG93eSBCYW5rIFBvbHNraTEoMCYGA1UECxMfQ2VudHJ1 bSBDZXJ0eWZpa2FjamkgS2x1Y3p5IE5CUDEaMBgGA1UEAxMRTkJQIEVudGVycHJp c2UgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCvtsWnZMpf7sVa a9JYQfekM7ifDcQZxOzhswh+0VEGD4+r7iMnVVcaRlSd2rfajM2IRnuw9fTli3vI EfxZAzNZSkTXiUVvPj9cpR7SkPtK8MuTthnS+tBuClootFsTZ9k5G2T3rfixjY/o 9nxH0lUuzzVw96iIYHHKySNxEBarx0p0bPqSwPhPh4503hwZwI4gz1uIhnl34gzk OGkrUt3sPjHkHNiBhZXM8QQ3xf25w3wXqgTrH4+XFTf2eQjDO0QzcybaE+cCt14f EaN+R5cCmJ7sKQvIi+R8pJPJ6t0j6KLIZE3eqSFA4cLSojlMtJmJsOeIm1EhKLPG DTdhK7XNAgMBAAGjggHrMIIB5zASBgkrBgEEAYI3FQEEBQIDAgADMCMGCSsGAQQB gjcVAgQWBBSYoPTCfyavsrVv/i8DGfbOobJYuDAdBgNVHQ4EFgQU1DbyLdBGLCAz E4RtFddOlSELDxEwgcEGA1UdIASBuTCBtjCBqwYLKwYBBAGB+XsBAQIwgZswdAYI KwYBBQUHAgIwaB5mAE4AQQBSAE8ARABPAFcAWQAgAEIAQQBOAEsAIABQAE8ATABT AEsASQAgAEMAZQByAHQAaQBmAGkAYwBhAHQAZQAgAFAAcgBhAGMAdABpAGMAZQAg AFMAdABhAHQAZQBtAGUAbgB0MCMGCCsGAQUFBwIBFhdodHRwOi8vcGtpLm5icC5w bC9wa2kvADAGBgRVHSAAMBkGCSsGAQQBgjcUAgQMHgoAUwB1AGIAQwBBMAsGA1Ud DwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB8GA1UdIwQYMBaAFHqEmVSlJxFLGVHV pgnC4LQPftx/MDEGA1UdHwQqMCgwJqAkoCKGIGh0dHA6Ly9wa2kubmJwLnBsL3Br aS9yY2EoMSkuY3JsMDwGCCsGAQUFBwEBBDAwLjAsBggrBgEFBQcwAoYgaHR0cDov L3BraS5uYnAucGwvcGtpL3JjYSgyKS5jcnQwDQYJKoZIhvcNAQELBQADggIBALTx MmAvXYP0gZlnA1onc6KpD/bXH03s7bw1y56J1i6S5cEEkSBW8wLlrJ2Fhc3YSUwK rhTLiyrsuWP+ddGNJXXqZyV8sGj15Ou98CCWUNf/aofbVplfrm9sCz/mS60TU6fg ZpPyF65yq8RppwLKVSqJQWGPwonV1EArvSufqr8IzlptQKMpL5Dfq5JY/nKhU0Uh TZh6JcQ4gErFFRl1pi+FR7IXRDZn8ZAe8/nuNkgNI427R3txib4zENEoopbLYEwz 74MaBss0ANchspAXCzRZ5b8A6mZQyaJeRp5WpQfylFiBsLgMA0oxrFjI74KfEB47 /dyOhsYwqE+KPDzo/KUUDBINK1wDOzrGN/Kx+hZvZvVEnfUgmIQU7ENXknAvNK7b kGR1ciOm7ft0tvYKqQgzbMHJlfIcCmd7ruoQcUUGVit+5KUu0B4/bDJzLClswwwT INI5x7f7hlnECLexu4FbbTCJ1kJwqWTyNXkDqKZnEHYUbTIden5WDCkWCwieXRcm dJirCX4EzPzNjTF6G2f9LY9kSNYj0RwKuFImFk5Coh96gk+e7FYvgMP2Y19eUnYZ rj4AHi+3cgBWAy4DMYLINLyYBOidNZ6/gJzIlQUHN4XxCOyyeOIv5gxKoil93emJ ws6XJAF0FdmxYYIGvE7yM0WJDBYQp/c8WJiWXITR -----END CERTIFICATE-----

Attachment B – Document Change Log

No.	Date	version	Person Responsible	Description of actions performed
1.	02.09.2011	0.1		Document creation
2.	20.09.2011	0.2		Amended chapters 2, 5.4, 5.5, 5.6, 5.7
3.	13.10.2011	0.3		Document review
4.	04.11.2011	0.4		Amended chapters 4.9.3, 4.9.15, 6.3.2, 6.4
5.	11.05.2012	0.5		Amended Chapters 8, 9, 10
6.	24.05.2012	0.6		Document review and proofreading
7.	22.08.2012	0.7		Document review and completion
8.	10.09.2012	0.8		Document review
9.	12.09.2012	0.9		Document review
10.	**18.09.2012**	**1.0**		**Document approval**
11.	11.10.2012	1.01		Document completion – comments by Internal Audit Department
12.	29.10.2012	1.02		Document review and completion
13.	30.10.2012	1.03		Document review
14.	30.10.2012	1.04		Document review
15.	05.11 2012	1.05		Document review
16.	**08.11.2012**	**1.1**		**Document approval**
17.	23.01.2013	1.11		Document completion – comments by ESCB auditors
18.	31.01.2013	1.12		Document review
19.	31.01.2013	1.13		Document review
20.	31.01.2013	1.14		Document review
21.	**19.02.2013**	**1.2**		**Document aproval**
22.	05.09.2013	1.21		Adaptation to the new visual template
23.	13.09.2013	1.22		Document review
24.	20.09.2013	1.23		Document review
25.	20.09.2013	1.24		Document review
26.	**02.10.2013**	**1.3**		**Document approval**
27.	03.06.2014	1.31		Amended chapters 2, 6.1.5, 6.3.2 and Attachment 2 due to CCK certificate renewal with key changeover
28.	03.06.2014	1.31		Document review
29.	03.06.2014	1.31		Document review
30.	06.06.2014	1.31		Document review

31.	**10.06.2014**	**1.4**	**Document approval**
32.	05.02.2015	1.41	Alignment of the document to the provisions of Resolution No. 1 /2015 of the NBP Management Board
33.	06.02.2015	1.42	Document review
34.	20.10.2016	1.51	Amendments due to changeover of the hash function used in the system and alignment to Resolution No. 53/2016 of the NBP Management Board
35.	**16.12.2016**	**1.6**	**Document approval**
36.	20.02.2017	1.61	Amendments due to comments by ESCB auditors
37.	03.02.2017	1.62	Document review
38.	23.05.2018	2.01	Amendments related to amendments of Resolution No. 53/2016 of the NBP Management Board Modification of information on the publication of the CRLs and certificates (chapter 2)

Document agreed by:

Date	Version	Person responsible	Signature
	2.1	Director of Information Technology and Telecommunications Department	

Document approved by:

Date	Version	Person responsible	Signature
	2.1	Director of Security Department	