NBP Narodowy Bank Polski

PKI NBP – Certification Policy for "ESCB Encryption" Certificates

OID: 1.3.6.1.4.1.31995.1.2.3.1
version 1.6

Security Department NBP
Warsaw, 2020

Table of Contents

1. Introduction

1.1 Overview

This "Certification Policy for 'ESCB Encryption' Certificates" (hereinafter referred to as "Policy") provides an overview of the policy on issuing and using certificates generated in the PKI NBP system (i.e. in the IT system of the Public Key Infrastructure of Narodowy Bank Polski) in compliance with the "ESCB Szyfrowanie" template. The provisions of the Policy are applicable to all participants in the PKI NBP system, i.e. Key Certification Centres, User Registration Points, Certificate Applicants, Subscribers and Relying Parties. The Policy, together with the Certification Practice Statement of the PKI NBP system, sets out the rules of providing trust services, starting from Subscriber registration, through Subscriber's public key certification, re-key and re-certification, to certificate revocation. Together they serve as 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 content of both documents and adapt their activities to the stipulations therein. The Certification Practice Statement of the PKI NBP system contains general information concerning the whole system and independent of the type of certificate (such as, e.g., information on technical security or system audits). This Policy contains detailed information that is strictly related to certificates issued from the "ESCB Szyfrowanie" template.

The structure and substantive content of this Policy are compliant with the RFC 3647 document Certificate Policy and Certificate Practice Statement Framework.

Where the element referred to is described in the Certification Practice Statement, the phrase "In accordance with the Certification Practice Statement of the PKI NBP System" has appeared in a respective chapter. Where a given element is not present in the PKI NBP system, the phrase "Not applicable" has appeared in a respective chapter.

1.2 Document Name and Identification

Document name	Certification Policy for "ESCB Encryption" Certificates
Document version	1.6
Document status	valid
Date of issue	29.09.2020
OID	1.3.6.1.4.1.31995.1.2.3.1
Location	http://pki.nbp.pl/pki/CP_encryption.pdf

1.3 Policy Participants

In accordance with the Certification Practice Statement of the PKI NBP system.

1.4 Certificate usage

Certificates issued in the "ESCB Szyfrowanie" template may be used only to encrypt data sent between ESCB IT systems users.

1.5 Policy Administration

1.5.1 Organisation responsible for document administration

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

1.5.2 Contact data

This Policy 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

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

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 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 holding a certificate issued in the PKI NBP system.

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
DN	Distinguished Name
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) – the 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) – the 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.

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

In accordance with the Certification Practice Statement of the PKI NBP system.

2.4 Repository Access Controls

In accordance with the Certification Practice Statement of the PKI NBP system.

3. Identification and Authentication

In accordance with the Certification Practice Statement of the PKI NBP system.

3.1 Naming

In accordance with the Certification Practice Statement of the PKI NBP system.

3.1.1 Types of names

The detailed structure of the distinguished name of certificates issued in accordance with "ESCB Szyfrowanie" template is presented in Attachment A.

To ensure the unambiguous identification of the certificate holder (e.g. in the case of different Subscribers with identical name and surname), a certificate distinguished name additionally the Subscriber's e-mail address, whereas the "Subject Alternative Name" field includes a UPN.

3.1.2 The need for the names to be meaningful

In accordance with the Certification Practice Statement of the PKI NBP system.

3.1.3 Rules for interpreting various name formats

In accordance with the Certification Practice Statement of the PKI NBP system.

3.1.4 Uniqueness of names

In accordance with the Certification Practice Statement of the PKI NBP system.

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

Cryptographic keys of a Subscriber are generated by the PRU operator on a smartcard delivered by the Subscriber.

3.2.2 Identity authentication for an entity

Not applicable.

3.2.3 Identity authentication for an individual

Where a Subscriber delivers in person his/her smartcard for cryptographic keys and certificates, the PRU Operator verifies the Subscriber's identity prior to issuing a certificate.

If a Subscriber's smartcard is delivered by a person authorised by the Subscriber, a PRU Operator is required to personally deliver it to the Subscriber after having verified the Subscriber's identity first.

In both cases, a PRU Operator verifies the identity of the Subscriber by comparing the person to receive the smartcard with the identity document with a photo referred to in the certificate application.

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 the case of certificates that serve to encrypt data sent between ESCB IT systems users, identification and authentication are always the same as at the time of generating the first cryptographic keys for the Subscriber. Provisions of Chapter 3.2 shall apply.

3.3.1 Identification and authentication requirements for routine re-key

Identical as in the case when the first cryptographic keys for the Subscriber are generated.

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

Identical as in the case when the first cryptographic keys for the Subscriber are generated.

4. Certificate Life-Cycle Operational Requirements

In accordance with the Certification Practice Statement of the PKI NBP system.

4.1 Certificate Application

All Subscriber's applications are lodged with the PRU and next (after their verification) are submited to the CCK.

4.1.1 Who can submit a certificate application ?

A request can be submitted by any employee of NBP or NBP's contractor. The application must be approved by the director of a department or a regional branch of the Subscriber or by the director of a department or a regional branch that has signed a contract with the company the Subscriber is employed at.

4.1.2 Enrolment process and applicants' responsibilities

The Subscriber who reports with the PRU is required to deliver the approved certificate application, an identity document with a photo and a smartcard for cryptographic keys and certificates.

The PRU Operator is required to verify the identity of the Subscriber (by comparing the person with the identity document and the data referred to in the certificate application and check the correctness of the certificate application.

4.2 Certificate Application Processing

4.2.1 Performance of identification and authentication procedures

The identity of the Subscriber is always checked by the PRU Operator by comparing the person who reports to pick up the certificate with the identity document with a photo and indicated in thecertificate application".

4.2.2 Approval or rejection of certificate applications

The Key Certification Centre will accept an application to issue a certificate to a Subscriber, if the following three conditions are met:

- the PRU receives a correct certificate application,
- the PRU positively verifies the identity of a Subscriber,
- the PRU Operator approves (by means of his/her private key) an application sent to the CCK.

If at least one of the conditions is not met, the application is rejected.

4.2.3 Time limit for processing the certificate applications

In accordance with the Certification Practice Statement of the PKI NBP system.

4.3 Certificate Issuance

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

The procedure for certificate issuance is as follows:

- after an approved request to generate a certificate is received from the PRU, the CCK generates cryptographic keys in the secure enviroment,
- after the keys have been generated, the CCK issues a certificate and orders the cryptographic module to sign it, and then saves the certificate in its data base,
- cryptographic keys and certificate are installed on the smartcard.

4.3.2 Notification of the subscriber of certificate issuance

The PRU Operator notifies the Subscriber of the issuance of a certificate during the handover of the smartcard with cryptographic keys and the certificate. In addition, the PRU Operator provides the Subscriber with the information on the emergency certificate revocation procedure (see Chapter 4.9) and asks the Subscriber to set a password to be used under this procedure. The password, used to authenticate the person submitting a certificate revocation request, is subsequently entered into the "Cryptographic Key Handover Protocol" (see Attachment B). One counterpart of the "Cryptographic Key Handover Protocol" is held at the PRU, while the Subscriber receives the other counterpart.

4.4 Certificate Acceptance

4.4.1 Confirmation of certificate acceptance

When creating a signature on the "Cryptographic Key Handover Protocol" (see Attachment B), the Subscriber confirms acceptance of the cryptographic keys and certificate received. At the same time, the signature confirms that the Subscriber has acquainted himself or herself with the "Information on the usage terms of a certificate issued in the PKI NBP system" and accepts the provisions thereof.

The rules governing the use of a certificate, signed by the Subscriber, are effective for the whole validity period of the certificate.

In the event of refusing to make a signature arising from the lack of acceptance of the certificate or the rules governing its use, the PRU Operator revokes the generated certificate and deletes it (alongside cryptographic keys) from the smartcard.

Requests for the issuance of a certificate, "Cryptographic Key Handover Protocol" and "Information on the usage terms of a certificate issued in the PKI NBP system" are stored in the PRU for up to 7 years.

4.4.2 Publication of the certificate by the CCK

Certificates issued in the PKI NBP system in compliance with the "ESCB Szyfrowanie" template are not published in a repository.

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

Subscribers, including PRU Operators, must use private keys and certificates:

- for their intended purpose, as set out in this Policy and compliant with the content of the certificate (of keyUsage and extendedKeyUsage fields),
- in accordance with the content of an optional contract concluded by the Subscriber and NBP.

4.5.2 Relying party's use of the keys and certificate

Relying parties, including PRU Operators, must use public keys and certificates:

- in accordance with their intended purpose laid down in this Policy (Chapter 1.4) and consistent with the content of a certificate (of keyUsage and extendedKeyUsage fields),
- only after verification of their status (see Chapter 4.9) and reliability of the signature of the CCK that issued a certificate,
- only during their validity period,
- only till the time of revocation or suspension of a certificate.

4.6 Certificate Renewal

Not applicable as a new pair of Subscriber's keys is generated each time a certificate is issued.

4.7 Certificate Rekey

In accordance with the Certification Practice Statement of the PKI NBP system. In the case of "ESCB Szyfrowanie" certificates the certificate rekey procedure is identical with that of first certificate issuance.

4.7.1 Circumstances for certificate renewal with key changeover

A certificate renewal request may be filed for the following reasons:

- the previous certificate has expired,
- the previous certificate has been revoked,

- data contained in the previous certificate have changed.

4.7.2 Who may request certificate renewal?

In accordance with provisions of Chapter 4.1.1.

4.7.3 Procedures for processing certificate renewal request

In accordance with provisions of Chapter 4.2.

4.7.4 Notification of new certificate issuance

In accordance with provisions of Chapter 4.3.2.

4.7.5 Confirmation of acceptance of a new certificate

In accordance with provisions of Chapter 4.4.

4.7.6 Publication of a new certificate

Certificates issued in the PKI NBP system in compliance with the "ESCB Szyfrowanie" template are not published in a repository.

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

General rules concerning PKI NBP system certificates revocation and suspension have been described in the Certification Practice Statement of the PKI NBP system. Both standard procedure and emergency procedure is applicable to certificates issued in compliance with the "ESCB Szyfrowanie" template.

Should the need arise to revoke a certificate outside PRU working hours, the Subscriber sends a message with a certificate revocation request to the following e-mail address: cck@nbp.pl. The request should contain:

- Subscriber data,
- name of the certificate template to be revoked,
- reason for revocation,
- password set out at the PRU at the time of certificate issuance (which allows to confirm the permission of the reporting person filling the request).

Having verified data contained in the certificate revocation request (the password in particular), the CCK Operator suspends the specified certificate and publishes a new CRL list. The Subscriber, or the authorised person referred to in Chapter 4.9.2. of the Statement is obliged to immediately (not later than within 3 business days from the initiation of the emergency procedure) deliver a request, which shall serve as the basis for the revocation or repeal of the suspended certificate.

As regards certificates issued in compliance with the "ESCB Szyfrowanie" template, a maximum period between the receipt of a certificate revocation request and the publication of an updated CRL is 24 hours. After the certificate has been suspended or revoked, the Subscriber is automatically advised to that effect via e-mail.

4.10 Certificate Status Verification Services

In accordance with the Certification Practice Statement of the PKI NBP system.

4.11 End of Subscription

In accordance with the Certification Practice Statement of the PKI NBP system.

4.12 Key Escrow and Recovery

Subscribers' private keys used to encrypt data sent between ESCB IT systems users are escrowed in the encrypted form in the database of the certification authority. Additional information can be found in chapters 4.3.1 and 6.1.1.
Key recovery may be peformed solely by the DRA and is done on the basis of a correctly completed request. Following key recovery it is installed on a new smartcard, which is subsequently handed over to the Subscriber. The handover shall be confirmed by an adequate entry in the register kept by the PRU.

5. Facility, Management and Operational Controls

In accordance with the Certification Practice Statement of the PKI NBP system.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

The Subscribers' cryptographic keys that serve to encrypt data sent between ESCB IT systems users are generated in secure environment and installed on smartcards with ITSEC E3 High or FIPS 140-2 level 3 certificates. The cryptographic keys are generated by PRU Operators on separate workstations reserved for that purpose at the PRU.

6.1.2 Delivery of private keys to subscribers

Cryptographic keys generated on a smartcard are delivered by the PRU Operator to a Subscriber immediately after they have been generated. The delivery of the cryptographic keys is confirmed by the signatures of the PRU Operator and a Subscriber put on the "Cryptographic Key Handover Protocol".

6.1.3 Delivery of the public key to the certificate issuer

The public key is delivered to the certificate issuer automatically, with no Subscriber involved in the delivery.

6.1.4 Delivery of the public key to the CKK

The public keys of the NBP Root CA and NBP Enterprise CA are available in the repository (see Chapter 2.1). In special cases, they can be delivered by e-mail or on the electronic carrier.

6.1.5 Key sizes

Cryptographic keys that serve to encrypt data sent between ESCB IT systems users are 2048 bits.

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 Accepted key usage (in compliance with KeyUsage field in X.509 v3)

In accordance with information included in Attachment A.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards

The Subscribers' cryptographic keys that serve to encrypt data sent between ESCB IT systems users are generated generated in secure environment and installed on smartcards with ITSEC E3 High or FIPS 140-2 Level 3 certificates. PKCS#11 libraries are used for communication with smartcards.

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

The private keys of Subscribers are not under multi-person control.

6.2.3 Escrow of private keys

See 4.12

6.2.4 Private key back-up copies

Private key back-up copies used to decrypt data are safely deposited in the CCK database. See4.12.

6.2.5 Private key archive

Due to the fact, that private key copies are deposited in the CCK database, provisions apply concerning archive copies made in the PKI NBP system. See Certification Practise Statement of the PKI NBP system.

6.2.6 Private key transfer into or from a cryptographic module.

Does not apply since Subscribers' private keys used to encrypt data sent between ESCB IT systems users are generated in secure environment and stored on smartcards. Following the installation of cryptographic keys and the certificate on the smartcard by the CCK, they cannot be exported from the card.

6.2.7 Private key storage in a cryptographic module

Subscribers' private keys used to encrypt data sent between ESCB IT systems users are generated in secure enviroment and stored on smartcards.

6.2.8 Private key activation method

After cryptographic keys have been generated and after certificate has been installed on the card, private key is activated only after a PIN code protecting the smartcard has been entered.

6.2.9 Private key deactivation method

The private key on a smart card is deactivated upon its withdrawal from the card reader. In some of the systems, it is possible to define an inactivity period after which the private key is deactivated automatically, even if the smartcard is inserted in the card reader.

6.2.10 Private key destruction method

The Subscribers' private keys are destroyed when they are safely deleted from the smartcard or when this smartcard is destroyed. Keys deposited in the database of the CA are removed by CCK Operators upon receipt of a written request from the Subscriber.

6.2.11 Cryptographic module classification

See 6.2.1.

6.3 Other Aspects of Key Management

6.3.1 Public key archive

In accordance with the Certification Practice Statement of the PKI NBP system.

6.3.2 Usage periods for public and private keys

The maximum validity period of certificates issued from the "ESCB Szyfrowanie" template and their corresponding cryptographic key pair is 2 years, however in special cases it is possible to issue such a certificate for a shorter period.

6.4 Activation Data

In accordance with the Certification Practice Statement of the PKI NBP system.

6.4.1 Generation and installation of activation data

After a smartcard is delivered by the Subscriber to the PRU, the card is added to a special "security base", which enables its subsequent use in the PKI NBP system. It is not possible to issue a certificate on a card that is not included in the security base. The Subscriber's private key activation data (a PIN that protects a smartcard) are set by the PRU Operator upon generation of cryptographic keys. During the delivery of cryptographic keys to the Subscriber, she/he is informed by the PRU Operator that she/he should change the data and set them herself/himself. The PRU Operator is required to assist the Subscriber, at his or her request, in changing the PIN code.

6.4.2 Activation data protection

After activation data are generated, the PRU Operator delivers this information to a Subscriber. No copy of the data is stored at the PRU, and in case a smartcard is blocked, it can be unblocked only with the participation of the PRU Operator.

6.4.3 Other activation data aspects

Data that serve to change activation data (PUK codes for smartcards are stored in the "security base" in encrypted form (3DES algorithm). In the process of unblocking an electronic card by the PRU Operator, PUK is sent directly to the electronic card management application and is not displayed. After receiving the PUK code, the application allows the PRU Operator only to unblock the card and set a new PIN code.

6.5 Computer System Security Controls

In accordance with the Certification Practice Statement of the PKI NBP system.

6.6 Life Cycle Security Controls

In accordance with the Certification Practice Statement of the PKI NBP system.

6.7 Network Security Controls

In accordance with the Certification Practice Statement of the PKI NBP system.

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 accordance with the Certification Practice Statement of the PKI NBP system and Attachment A.

7.2 CRL Profile

In accordance with the Certification Practice Statement of the PKI NBP system.

8. Compliance Audit and Other Assessment

In accordance with the Certification Practice Statement of the PKI NBP system.

9. Other Business and Legal Matters

In accordance with the Certification Practice Statement of the PKI NBP system.

10. Personal Data Protection

In accordance with the Certification Practice Statement of the PKI NBP system.

Attachment A – “ESCB Szyfrowanie” Certificate Template

Version	V3
Serial Number	Unique system serial number
Signature algorithm	Sha256RSA
Issuer	CN = NBP Enterprise CA OU = Centrum Certyfikacji Kluczy NBP O = Narodowy Bank Polski L = Warszawa C = PL
Valid from-to	Up to 2 years
Subject	Constructed on the basis of the Active Directory data, including e-mail, Subsequent nodes of LDAP, which lead to the user account object in this LDAP, are contained in individual DN fields.
Public key	RSA 2048 bits
SMIME Capabilities	[1]SMIME Capability Object ID=2.16.840.1.101.3.4.1.42 [2]SMIME Capability Object ID=2.16.840.1.101.3.4.1.45 [3]SMIME Capability Object ID=2.16.840.1.101.3.4.1.22

	[4]SMIME Capability Object ID=2.16.840.1.101.3.4.1.25 [5]SMIME Capability Object ID=2.16.840.1.101.3.4.1.2 [6]SMIME Capability Object ID=2.16.840.1.101.3.4.1.5 [7]SMIME Capability Object ID=1.2.840.113549.3.7 [8]SMIME Capability Object ID=1.3.14.3.2.7 [9]SMIME Capability Object ID=1.2.840.113549.3.2 Parameters=02 02 00 80 [10]SMIME Capability Object ID=1.2.840.113549.3.4 Parameters=02 02 02 00
Application policies	[[1]Application certificate policies: Policy identifier=Secure Email
Certificate template information	Template=ESCB Szyfrowanie((1.3.6.1.4.1.311.21.8.8041467.6109741.1199773.5170465.10588945.146.5233154.16470863)) Major version number=100 Minor version number=72
Authority Information Access	[1] Authority Info Access Access method=Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternate name: URL address=http://ocsp.nbp.pl/ocsp [2] Authority Info Access Access method=Certification authority issuer (1.3.6.1.5.5.7.48.2) Alternate name: URL address=ldap:///CN=NBP%20Enterprise%20CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=int,DC=nbp,DC=pl?cACertificate?base?objectClass=certificationAuthority [3] Authority Info Access

	Access method=Certification authority issuer (1.3.6.1.5.5.7.48.2) Alternate name: URL address=http://pki.nbp.pl/pki/eca(3).crt
Subject key identifier	160-bit hash of Subscriber’s public key
Subject alternative name	Principal name= UPN of Subscriber, RFC822 name= E-mail address of Subscriber
CRL distribution points	[1]CRL distribution point Name of distribution point: Full name: URL address=ldap:///CN=NBP%20Enterprise%20CA(2),CN=PKI,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=int,DC=nbp,DC=pl?certificateRevocationList?base?objectClass=cRLDistributionPoint URL address=http://pki.nbp.pl/pki/eca(2).crl
Certificate policies	[1]Certificate policy: Policy identifier=1.3.6.1.4.1.31995.1.1.2 [1,1]Policy qualifier Info: Policy qualifier Id=CPS Qualifier: http://pki.nbp.pl/pki/ [2]Certificate policy: Policy identifier=1.3.6.1.4.1.31995.1.2.3.1 [2,1]Policy qualifier Info: Policy qualifier Id=CPS Qualifier: http://pki.nbp.pl/pki/
Authority key identifier	160-bit hash of NBP Enterprise CA’s public key
Extended key usage	Secure Email (1.3.6.1.5.5.7.3.4)

Key usage (*)	Key Encipherment, Data Encipherment
Basic constraints (*)	Subject Type=End Entity Path Length Constraint= None

(*) – critical extension

Attachment B – Information on the usage terms of a certificate issued in the PKI NBP system

.....(date) .....

Cryptographic Key Handover Protocol

On ....., PRU Operator .....
(date) (name of PRU)

handed cryptographic keys over to the Subscriber..... and a certificate: (name of Subscriber)

☐ generated in compliance with the „ESCB Logowanie" template

☐ generated in compliance with the „ESCB Podpis" template

☐ generated in compliance with the „ESCB Szyfrowanie" template

Passwords for the emergency certificate revocation:

ESCB Logowanie ……

ESCB Podpis ……

ESCB Szyfrowanie ……

Acceptance of certificates

When signing this "Cryptographic Key Handover Protocol", the Subscriber:

- accepts the certificate
- confirms that s/he has been informed that the rules in force in the PKI NBP system are described in the Certification Practice Statement of the PKI NBP system and in Certification Policies. The documents are available at the http://pki.nbp.pl/pki/ website,
- represents that he or she has read and accepts the "Information on the usage terms of a certificate issued in the PKI NBP system" which is on the next page of this Protocol

(Name and surname of the PRU Operator)	(Name and surname of the Subscriber)	(Name and surname of the System Security Inspector)
(signature)	(signature)	(signature)

Information on the usage terms of a certificate issued in the PKI NBP system

1. PKI NBP system certificates are issued to persons employed at NBP or in entities performing tasks commissioned by NBP.

2. Rules applicable in the PKI NBP system (including the rights and obligations of Subscribers, Relying Parties, certificate applicants, a Key Certification Centre and User Registration Points) are laid down in the Certification Practice Statement and in Certification Policies.

3. A Subscriber is required to use cryptographic keys and certificates only for the intended purpose as set out by the Certification Policy referred to in the certificate.

4. The scope of use of certificates issued in the PKI NBP system is as follows:

- certificates conforming to the "ESCB Logowanie" template – to authenticate the Subscriber in the IT systems of the European System of Central Banks (ESCB);
- certificates conforming to the "ESCB Podpis" template – to create an electronic signature in the IT systems of the European System of Central Banks.
- certificates conforming to the "ESCB Szyfrowanie " template – to encrypt data sent between ESCB IT systems users

5. A Subscriber is required to:

- notify without delay the PRU of any changes to the data contained in the certificate,
- abide by the provisions of the Certification Practice Statement of the PKI NBP System and respective Certification Policies,
- ensure appropriate protection of his/her private key and the data that serve to activate it,
- use cryptographic keys and PKI NBP system certificates only within the scope delineated in the certificate and described in point 4 above,

- request without delay the revocation of the certificate in the event of a compromise of a respective private key.

6. In the event of breach by the Subscriber of the rules referred to in this “Information on the usage terms of a certificate issued in the PKI NBP system”, his or her certificate may be revoked.

7. NBP is not a qualified trust services provider, and certificates issued in the PKI NBP system are not qualified certificates.

Attachment C - Document Change Log

No.	Date	Version	Person responsible	Description of work perfomed
1.	10.09.2013	0.1		Document creation
2.	13.09.2013	0.2		Document review and completion
3.	13.09.2013	0.3		Document review
4.	17.09.2013	0.4		Document review and completion
5.	20.09.2013	0.5		Document review
6.	23.09.2013	0.6		Document review
7.	**02.10.2013**	**1.0**		**Document Approval**
8.	03.06.2014	1.01		Amended chapter 2 and Attachment A due to CCK certificate renewal with key changeover
9.	03.06.2014	1.01		Document review
10.	03.06.2014	1.01		Document review
11.	06.06.2014	1.01		Document review
12.	**10.06.2014**	**1.1**		**Document approval**
13.	05.02.2015	1.11		Alignment of the document to the provisions of Resolution No. 1 /2015 of the NBP Management Board
14.	06.02.2015	1.12		Document review
15.	20.10.2016	1.21		Amendments due to changeover of the hash function used in the system and alignment to Resolution No. 53/2016 of the NBP Management Board
16.	16.12.2016	1.3		**Document approval**
17.	20.02.2017	1.31		Amendments due to comments by ESCB auditors
18.	02.03.2017	1.32		Document review
19.	24.05.2018	1.41		Modification of information on the publication of the CRLs and certificates (chapter 2)
20.	03.09..2020	1.51		Change of the data retention period, withdrawal of the paper form of the Cryptographic Service Order Form

Document agreed by:

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

Document approved by:

Date	Version	Person responsible	Signature
	1.6	Director of Security Department	