NBP Narodowy Bank Polski

Narodowy Bank Polski

PKI NBP – Polityka Certyfikacji dla certyfikatów „ESCB Szyfrowanie”

OID: 1.3.6.1.4.1.31995.1.2.3.1
wersja 1.4

Departament Bezpieczeństwa NBP
Warszawa, 2017

Spis treści

1. Wstęp

1.1 Wprowadzenie

Niniejsza „Polityka Certyfikacji dla certyfikatów „ESCB Szyfrowanie" zwana dalej „Polityką" opisuje zasady wnioskowania, wydawania i wykorzystywania certyfikatów w systemie PKI NBP (czyli w systemie informatycznym infrastruktury klucza publicznego Narodowego Banku Polskiego) zgodnie z szablonem „ESCB Szyfrowanie". Zapisy Polityki mają zastosowanie dla wszystkich uczestników systemu PKI NBP tzn. Centrów Certyfikacji Kluczy, Punktów Rejestracji Użytkowników, podmiotów wnioskujących o certyfikat, Subskrybentów oraz stron ufających. Polityka wspólnie z Kodeksem Postępowania Certyfikacyjnego systemu PKI NBP określają zasady świadczenia usług zaufania, począwszy od rejestracji Subskrybentów, poprzez certyfikację ich kluczy publicznych i aktualizację kluczy i certyfikatów, a na unieważnianiu certyfikatów kończąc. Wspólnie stanowią one swego rodzaju „przewodnik" w relacjach pomiędzy systemem PKI NBP a jego użytkownikami. Z tego powodu wszyscy użytkownicy systemu PKI NBP powinni znać oba dokumenty i stosować się do zapisów w nich zawartych. W Kodeksie Postępowania Certyfikacyjnego systemu PKI NBP zawarte są informacje ogólne, dotyczące całego systemu i niezależne od typu certyfikatu (takie jak np. informacje dotyczące zabezpieczeń technicznych czy audytów systemu). W niniejszej Polityce zawarto informacjej szczegółowe i ściśle związane z certyfikatami wydawanymi z szablonu „ESCB Szyfrowanie".

Struktura i merytoryczna zawartość niniejszej Polityki są zgodne z dokumentem RFC 3647 Certificate Policy and Certificate Practice Statement Framework. W przypadku, gdy wymieniony element opisany jest w Kodeksie, w odpowiednim rozdziale wpisano „Zgodnie z Kodeksem Postępowania Certyfikacyjnego systemu PKI NBP". W przypadku, gdy dany element nie występuje w systemie PKI NBP w odpowiednim rozdziale wpisano „Nie dotyczy".

1.2 Nazwa dokumentu i jego identyfikacja

Nazwa dokumentu	Polityka Certyfikacji dla certyfikatów „ESCB Szyfrowanie"
Wersja dokumentu	1.4
Status dokumentu	Aktualny
Data wprowadzenia	07.03.2017
OID	1.3.6.1.4.1.31995.1.2.3.1
Lokalizacja	http://pki.nbp.pl/pki/pc_szyfrowanie.pdf

1.3 Strony Polityki

Zgodnie z Kodeksem Postępowania Certyfikacyjnego systemu PKI NBP.

1.4 Zakres stosowania certyfikatów

Certyfikaty wydane w szablonie „ESCB Szyfrowanie" mogą być wykorzystywane jedynie do szyfrowania danych przesyłanych pomiędzy użytkownikami systemów informatycznych Europejskiego Systemu Banków Centralnych (ESBC).

1.5 Administrowanie Polityką

1.5.1 Organizacja odpowiedzialna za administrowanie dokumentem

Właścicielem niniejszej Polityki jest:
Narodowy Bank Polski
ul. Świętokrzyska 11/21
00-919 Warszawa

1.5.2 Kontakt

Za zarządzanie Polityką odpowiedzialny jest:
Departament Bezpieczeństwa
Narodowego Banku Polskiego
ul. Świętokrzyska 11/21
00-919 Warszawa
tel. +48221851513 fax: +48221852336
mail: cck@nbp.pl

1.5.3 Procedura zatwierdzania dokumentu

Każda z wersji Polityki obowiązuje (posiada status aktualny) do czasu zatwierdzenia i opublikowania nowej wersji. Nowa wersja opracowywana jest przez pracowników Wydziału Kryptografii Departamentu Bezpieczeństwa i ze statusem „do uzgodnienia" jest przekazywana do Departamentu Informatyki i Telekomunikacji. Po uzgodnieniu dokumentu przez Departament Informatyki i Telekomunikacji nowa wersja Polityki zatwierdzana jest przez Dyrektora Departamentu Bezpieczeństwa.

1.6 Definicje i skróty

1.6.1 Definicje

Na użytek Polityki przyjmuje się następujące pojęcia :

- **Centrum Certyfikacji Kluczy**–moduł systemu PKI NBP, posługujący się własnym, wygenerowanym przez siebie, kluczem prywatnym służącym do elektronicznego podpisywania certyfikatów i list CRL, wystawiający, unieważniający i dystrybuujący certyfikaty zgodnie z zasadami określonymi w niniejszym Kodeksie,
- **certyfikat klucza publicznego (certyfikat)** – elektroniczne zaświadczenie, za pomocą którego klucz publiczny jest przyporządkowany do Subskrybenta, umożliwiające jednoznaczną jego identyfikację,
- **identyfikator wyróżniający**– informacja zamieszczona w certyfikacie, pozwalająca na jednoznaczną identyfikację subskrybenta w ramach zbioru Subskrybentów obsługiwanych przez CCK,
- **integralność** – właściwość świadcząca o tym, że informacje nie zostały zmienione od momentu ich podpisania do momentu zweryfikowania podpisania,
- **klucz kryptograficzny** – parametr, który steruje operacjami szyfrowania\deszyfrowania lub podpisywania\weryfikacji podpisu informacji,
- **klucz prywatny** – klucz kryptograficzny do wyłącznego użytku subskrybenta, służący do składania podpisu lub deszyfracji informacji,

- **klucz publiczny** – klucz kryptograficzny publicznie znany, powiązany z kluczem prywatnym, który jest stosowany do weryfikowania podpisu lub szyfrowania informacji,
- **lista CRL** – lista unieważnionych lub zawieszonych certyfikatów, których okres ważności jeszcze nie upłynął,
- **niezaprzeczalność** – właściwość polegająca na tym, że nadawca informacji nie może zanegować faktu jej nadania,
- **poufność** – właściwość polegająca na tym, że informacje są niedostępne dla nieupoważnionych osób,
- **Punkt Rejestracji Użytkowników** –moduł systemu PKI NBP, służący w szczególności do: weryfikacji, rejestracji, generowania kluczy kryptograficznych Subskrybentów,
- **Subskrybent** – osoba fizyczna[1] posiadająca certyfikat wydany w systemie PKI NBP,
- **uwierzytelnienie** - właściwość umożliwiająca potwierdzenie deklarowanej tożsamości nadawcy informacji.

1.6.2 Skróty

Wykaz stosowanych w Polityce skrótów wraz z ich objaśnieniami

Skrót	Objaśnienie
CCK	Centrum Certyfikacji Kluczy
CRL	Lista unieważnionych certyfikatów (ang. Certificate Revocation List)
DN	Identyfikator wyróżniający (ang. distinguished name)
HSM	Sprzętowy moduł bezpieczeństwa (ang. Hardware Security Module)
NBP	Narodowy Bank Polski
OCSP	Usługa weryfikacji statusu certyfikatu on-line (ang. On-line Certificate Status Protocol)
PKI	Infrastruktura Klucza Publicznego (ang. Public Key Infrastructure)
PRU	Punkt Rejestracji Użytkowników
UPN	Nazwa główna użytkownika (ang. User Principal Name)

[1] Zasady opisane w niniejszej Polityce Certyfikacji odnoszą się do certyfikatów wystawianych dla osób fizycznych. Certyfikaty wydawane dla elementów infrastruktury NBP (serwery, stacje robocze) wydawane są na innych zasadach.

2. Odpowiedzialność za publikację i repozytorium

2.1 Repozytorium

W systemie PKI NBP wyróżnić można dwa oddzielne repozytoria:
Repozytorium wewnętrzne znajdujące się w usłudze katalogowej Active Directory oraz repozytorium zewnętrzne znajdujące się na stronie internetowej http://pki.nbp.pl/pki
Wewnątrz domen NBP - certyfikaty CCK i listy CRL są dystrybuowane automatycznie.
W przypadku repozytorium zewnętrznego:

Certyfikaty CCK dostępne są pod następującymi adresami:

- http://pki.nbp.pl/pki/rca.crt - główny urząd certyfikacji (NBP Root CA) – certyfikat wystawiony w dniu 20 listopada 2008 roku.
- http://pki.nbp.pl/pki/rca(1).crt - główny urząd certyfikacji (NBP Root CA) – certyfikat wystawiony w dniu 2 czerwca 2014 roku.
- http://www.nbp.pl/pki/rca(2).crt - główny urząd certyfikacji (NBP Root CA) – certyfikat wystawiony z wykorzystaniem funkcji skrótu SHA-256.
- http://pki.nbp.pl/pki/eca(1).crt – pośredni urząd certyfikacji (NBP Enterprise CA) – certyfikat wystawiony w dniu 9 czerwca 2011 roku.
- http://pki.nbp.pl/pki/eca(2).crt - pośredni urząd certyfikacji (NBP Enterprise CA)- certyfikat wystawiony w dniu 2 czerwca 2014 roku.
- http://www.nbp.pl/pki/eca(3).crt - pośredni urząd certyfikacji (NBP Enterprise CA)- certyfikat wystawiony w dniu 10 października 2016 roku.

Listy CRL dostępne są pod następującymi adresami:

- http://pki.nbp.pl/pki/rca.crl - lista CRL urzędu NBP Root CA (odpowiadająca certyfikatowi wystawionemu w dniu 20 listopada 2008 roku).
- http://pki.nbp.pl/pki/rca(1).crl - lista CRL urzędu NBP Root CA (odpowiadająca certyfikatowi wystawionemu w dniu 2 czerwca 2014 roku).
- http://pki.nbp.pl/pki/eca(1).crl – lista CRL urzędu NBP Enterprise CA (odpowiadająca certyfikatowi wystawionemu w dniu 9 czerwca 2011 roku),
- http://pki.nbp.pl/pki/eca(2).crl – lista CRL urzędu NBP Enterprise CA (odpowiadająca certyfikatowi wystawionemu w dniu 10 października 2016 roku).

Dokumenty związane z systemem PKI NBP dostępne są pod następującymi adresami:

- http://pki.nbp.pl/pki/kodeks.pdf - Kodeks Postępowania Certyfikacyjnego systemu PKI NBP.
- http://pki.nbp.pl/pki/PC_podpis.pdf - Polityka certyfikacji dla certyfikatów „ESCB Podpis".
- http://pki.nbp.pl/pki/PC_logowanie.pdf - Polityka certyfikacji dla certyfikatów „ESCB Logowanie".

- http://pki.nbp.pl/pki/PC_szyfrowanie.pdf - Polityka certyfikacji dla certyfikatów „ESCB Szyfrowanie".
- http://pki.nbp.pl/pki/zasady.pdf - informacja o warunkach użycia certyfikatu wydanego w systemie PKI NBP.
- http://pki.nbp.pl/pki/zamowienie.pdf - zamówienie na usługę kryptograficzną.

Dodatkowo, pod adresem http://ocsp.nbp.pl/ocsp dostępna jest usługa OCSP. Powyższy adres jest wspólny dla użytkowników wewnątrz domen NBP jak i dla użytkowników zewnętrznych.

2.2 Informacje publikowane w repozytorium

Zgodnie z zapisami rozdziału 2.1.

2.3 Częstotliwość publikacji

Zgodnie z Kodeksem Postępowania Certyfikacyjnego systemu PKI NBP.

2.4 Kontrola dostępu do repozytorium

Zgodnie z Kodeksem Postępowania Certyfikacyjnego systemu PKI NBP.

3. Identyfikacja i uwierzytelnianie

Zgodnie z Kodeksem Postępowania Certyfikacyjnego systemu PKI NBP.

3.1 Nadawanie nazw

Zgodnie z Kodeksem Postępowania Certyfikacyjnego systemu PKI NBP.

3.1.1 Typy nazw

Dokładna struktura identyfikatora wyróżniającego certyfikatów wydanych zgodnie z szablonem „ESCB Szyfrowanie" przedstawiona jest w Załączniku A.

W celu zapewnienia jednoznacznego wskazania właściciela certyfikatu (np. w przypadku Subskrybentów o identycznych imionach i nazwiskach) identyfikator wyróżniający certyfikatu zawiera dodatkowo adres email Subskrybenta, a pole „alternatywna nazwa podmiotu" zawiera UPN.

3.1.2 Konieczność używania nazw znaczących

Zgodnie z Kodeksem Postępowania Certyfikacyjnego systemu PKI NBP.

3.1.3 Zasady interpretacji różnych form nazw

Zgodnie z Kodeksem Postępowania Certyfikacyjnego systemu PKI NBP.

3.1.4 Unikalność nazw

Zgodnie z Kodeksem Postępowania Certyfikacyjnego systemu PKI NBP.

3.1.5 Rozpoznawanie, uwierzytelnianie oraz rola znaków towarowych

Nie dotyczy.

3.2 Początkowa walidacja tożsamości

3.2.1 Dowód posiadania klucza prywatnego

Klucze kryptograficzne Subskrybenta generowane są przez Operatora PRU a następnie zapisywane na karcie elektronicznej dostarczonej przez Subskrybenta.

3.2.2 Uwierzytelnienie tożsamości osób prawnych

Nie dotyczy.

3.2.3 Uwierzytelnienie tożsamości osób fizycznych

W przypadku, gdy karta elektroniczna do zapisania kluczy kryptograficznych i certyfikatów dostarczana jest osobiście przez Subskrybenta, Operator PRU weryfikuje jego tożsamość przed wystawieniem certyfikatu.

W przypadku, gdy kartę elektroniczną Subskrybenta dostarcza osoba przez niego upoważniona, Operator PRU ma obowiązek osobiście dostarczyć kartę do Subskrybenta i przed jej przekazaniem dokonać weryfikacji jego tożsamości.

W obu przypadkach weryfikacja tożsamości Subskrybenta polega na porównaniu osoby odbierającej kartę z dokumentem tożsamości zawierającym zdjęcie i wskazanym we wniosku o wydanie certyfikatu.

3.2.4 Dane subskrybenta niepodlegające weryfikacji

Wszystkie dane Subskrybenta umieszczane w certyfikacie są weryfikowane przez PRU.

3.2.5 Walidacja urzędów i organizacji

Nie dotyczy.

3.2.6 Kryteria interoperacyjności

Nie dotyczy.

3.3 Identyfikacja i uwierzytelnienie w przypadku żądania aktualizacji kluczy

W przypadku certyfikatów do szyfrowania danych przesyłanych pomiędzy użytkownikami systemów informatycznych ESBC, funkcje identyfikacji i uwierzytelniania są zawsze takie same jak podczas generowania pierwszych kluczy kryptograficznych dla Subskrybenta. Zastosowanie mają zapisy rozdziału 3.2.

3.3.1 Identyfikacja i uwierzytelnienie w przypadku normalnej aktualizacji kluczy

Identycznie jak w przypadku generowania pierwszych kluczy kryptograficznych dla Subskrybenta.

3.3.2 Identyfikacja i uwierzytelnienie w przypadku żądania aktualizacji kluczy po ich unieważnieniu

Identycznie jak w przypadku generowania pierwszych kluczy kryptograficznych dla Subskrybenta.

4. Wymagania funkcjonalne

Zgodnie z Kodeksem Postępowania Certyfikacyjnego systemu PKI NBP.

4.1 Składanie wniosków

Wszystkie wnioski Subskrybenta są składane do PRU, a następnie (po ich weryfikacji) przekazywane są do CCK.

4.1.1 Kto może złożyć wniosek o wydanie certyfikatu ?

Wniosek, w postaci elektronicznej lub papierowej jako „Zamówienie na usługę kryptograficzną", może złożyć dowolny pracownik NBP lub firmy współpracującej z NBP. Wniosek musi być zatwierdzony przez dyrektora departamentu lub oddziału okręgowego Subskrybenta lub przez dyrektora departamentu lub oddziału okręgowego, który podpisał umowę z firmą, w której zatrudniony jest Subskrybent.

4.1.2 Proces składania wniosków i związane z tym obowiązki

Subskrybent zgłaszając się do PRU ma obowiązek dostarczyć zatwierdzony wniosek o wydanie certyfikatu, dokument tożsamości zawierający zdjęcie oraz kartę elektroniczną, na której zapisane zostaną klucze kryptograficzne i certyfikaty.

Operator PRU ma obowiązek zweryfikować tożsamość Subskrybenta poprzez porównanie osoby z dokumentem tożsamości oraz z danymi zawartymi we wniosku o wydanie certyfikatu oraz sprawdzić poprawność wniosku o wydanie certyfikatu.

4.2 Przetwarzanie wniosków

4.2.1 Realizacja funkcji identyfikacji i uwierzytelniania

Tożsamość Subskrybenta jest zawsze sprawdzana przez Operatora PRU poprzez porównanie osoby, której wydany ma zostać certyfikat, z danymi w dokumencie tożsamości zawierającym zdjęcie i wskazanym we wniosku o wydanie certyfikatu.

4.2.2 Przyjęcie lub odrzucenie wniosku

Centrum Certyfikacji Kluczy przyjmie wniosek o wydanie certyfikatu Subskrybentowi jeśli zostaną spełnione trzy warunki:

- PRU otrzyma poprawny wniosek o wydanie certyfikatu,
- PRU poprawnie zweryfikuje tożsamość Subskrybenta,
- Operator PRU zatwierdzi (za pomocą swojego klucza prywatnego) wniosek wysłany do CCK.

Jeżeli chociaż jeden z tych warunków nie zostanie spełniony wniosek zostaje odrzucony.

4.2.3 Okres oczekiwania na przetworzenie wniosku

Zgodnie z Kodeksem Postępowania Certyfikacyjnego systemu PKI NBP.

4.3 Wydanie certyfikatu

4.3.1 Czynności CCK wykonywane podczas wydawania certyfikatu

Procedura wydawania certyfikatu przebiega następująco:

- po otrzymaniu z PRU potwierdzonego żądania wygenerowania certyfikatu, CCK generuje klucze kryptograficzne Subskrybenta w bezpiecznym środowisku,
- po wygenerowaniu kluczy CCK wystawia certyfikat i zleca jego podpisanie modułowi kryptograficznemu, a następnie zapisuje certyfikat w swojej bazie danych,
- klucze kryptograficzne i certyfikat są instalowane na karcie elektronicznej.

4.3.2 Informowanie subskrybenta o wydaniu certyfikatu

O wydaniu certyfikatu Subskrybenta informuje Operator PRU podczas przekazywania karty elektronicznej z kluczami kryptograficznymi i certyfikatem.

Dodatkowo, Operator PRU przekazuje Subskrybentowi informację nt. procedury awaryjnego unieważniania certyfikatów (patrz Rozdział 4.9) oraz prosi o ustalenie hasła wykorzystywanego w ramach tej procedury. Hasło to, służące do uwierzytelnienia osoby składającej żądanie unieważnienia, jest zapisywane na „Protokole przekazania kluczy kryptograficznych" (patrz Załącznik B). Jeden egzemplarz „Protokołu przekazania kluczy kryptograficznych" przechowywany jest w PRU, drugi otrzymuje Subskrybent.

4.4 Akceptacja certyfikatu

4.4.1 Potwierdzenie akceptacji certyfikatu

Składając podpis na „Protokole przekazania kluczy kryptograficznych" (patrz Załącznik B) Subskrybent potwierdza akceptację odbieranych kluczy kryptograficznych i certyfikatu. Podpis ten jest jednocześnie potwierdzeniem zapoznania się i akceptacji „Informacji o warunkach użycia certyfikatu wydanego w systemie PKI NBP".

Podpisane przez Subskrybenta zasady użycia certyfikatu, obowiązują przez cały okres ważności certyfikatu, którego dotyczą.

W przypadku odmowy złożenia podpisu wynikającej z braku akceptacji certyfikatu lub zasad użycia certyfikatu, Operator PRU unieważnia wygenerowany certyfikat oraz usuwa go (wraz z kluczami kryptograficznymi) z karty elektronicznej.

Zarówno „Zamówienie na usługę kryptograficzną" jak i „Protokół przekazania kluczy kryptograficznych" oraz „Informacja o warunkach użycia certyfikatu wydanego w systemie PKI NBP" przechowywane są w PRU przez okres 5 lat.

4.4.2 Publikowanie certyfikatu przez CCK

Certyfikaty wydane w systemie PKI NBP zgodnie z szablonem „ESCB Szyfrowanie" nie są publikowane w repozytorium.

4.4.3 Informowanie innych podmiotów o wydaniu certyfikatu

CCK nie informuje innych podmiotów o wydaniu certyfikatu, jednak Subskrybent powinien udostępnić swój certyfikat osobom, z którymi wymieniać będzie zaszyfrowane informacje.

4.5 Stosowanie kluczy oraz certyfikatów

4.5.1 Stosowanie kluczy i certyfikatów przez subskrybenta

Subskrybenci, w tym Operatorzy PRU muszą używać kluczy prywatnych i certyfikatów:

- zgodnie z ich przeznaczeniem, określonym w niniejszej Polityce i zgodnym z treścią certyfikatu (pola keyUsage oraz extendedKeyUsage),
- zgodnie z treścią opcjonalnej umowy zawartej pomiędzy Subskrybentem a NBP.

4.5.2 Stosowanie kluczy i certyfikatu przez stronę ufającą

Strony ufające, w tym Operatorzy PRU muszą używać kluczy publicznych i certyfikatów:

- zgodnie z ich zastosowaniem, określonym w niniejszej Polityce (rozdział 1.4) i zgodnym z treścią certyfikatu (pola keyUsage oraz extendedKeyUsage),
- tylko po zweryfikowaniu ich statusu (patrz rozdz. 4.9) oraz wiarygodności podpisu CCK, które wystawiło certyfikat,
- tylko w okresie ich ważności,
- tylko do momentu unieważnienia lub zawieszenia certyfikatu.

4.6 Recertyfikacja

Nie dotyczy, gdyż przy każdym generowaniu certyfikatu generowana jest nowa para kluczy Subskrybenta.

4.7 Odnowienie certyfikatu

Zgodnie z Kodeksem Postępowania Certyfikacyjnego systemu PKI NBP. W przypadku certyfikatów „ESCB Szyfrowanie" procedura odnawiania certyfikatu jest identyczna jak procedura wydania pierwszego certyfikatu.

4.7.1 Okoliczności odnowienia certyfikatu

Żądanie odnowienia certyfikatu może wystąpić z następujących powodów:

- wygaśnięcie poprzedniego certyfikatu,
- unieważnienie poprzedniego certyfikatu,
- zmiana danych zawartych w certyfikacie.

4.7.2 Kto może żądać odnowienia certyfikatu?

Zgodnie z zapisami rozdziału 4.1.1.

4.7.3 Przetwarzanie wniosku o odnowienie certyfikatu

Zgodnie z zapisami rozdziału 4.2.

4.7.4 Informowanie o wydaniu nowego certyfikatu

Zgodnie z zapisami rozdziału 4.3.2.

4.7.5 Potwierdzenie akceptacji nowego certyfikatu

Zgodnie z zapisami rozdziału 4.4.

4.7.6 Publikowanie nowego certyfikatu

Certyfikaty wydane w systemie PKI NBP zgodnie z szablonem „ESCB Szyfrowanie" nie są publikowane w repozytorium.

4.7.7 Informowanie o wydaniu certyfikatu innych podmiotów

CCK nie informuje innych podmiotów o wydaniu certyfikatu, jednak Subskrybent powinien udostępnić swój certyfikat osobom, z którymi wymieniać będzie zaszyfrowane informacje

4.8 Modyfikacja certyfikatu

Każda modyfikacja certyfikatu wymaga jego odnowienia i w tym przypadku zastosowanie mają zapisy rozdziału 4.7.

4.9 Unieważnienie i zawieszenie certyfikatu

Ogólne zasady dotyczące unieważniania i zawieszania certyfikatów systemu PKI NBP zostały opisane w Kodeksie Postępowania Certyfikacyjnego systemu PKI NBP. Dla certyfikatów wydanych zgodnie z szablonem „ESCB Szyfrowanie" obowiązuje zarówno standardowa procedura unieważniania certyfikatów, jak i procedura awaryjna.

W przypadku konieczności unieważnienia certyfikatu poza godzinami pracy PRU, Subskrybent przesyła na skrzynkę mailową cck@nbp.pl wiadomość email zawierającą żądanie unieważnienia certyfikatu. Żądanie to powinno zawierać:

- dane subskrybenta
- nazwę szablonu certyfikatu do unieważnienia
- określenie przyczyny unieważnienia
- hasło ustalone w PRU w czasie wydawania certyfikatu (pozwala ono na potwierdzenie uprawnienia osoby zgłaszającej do unieważnienia certyfikatu).

Po zweryfikowaniu danych zawartych w żądaniu unieważnienia (w szczególności hasła), Operator CCK zawiesza wskazany certyfikat oraz publikuje nową listę CRL.

W przypadku certyfikatów wydanych zgodnie z szablonem „ESCB Szyfrowanie" maksymalny czas pomiędzy otrzymaniem żądania unieważnienia certyfikatu, a publikacją zaktualizowanej listy CRL wynosi 24 godziny.

Po unieważnieniu lub zawieszeniu certyfikatu Subskrybent automatycznie zostaje o tym fakcie powiadomiony za pomocą poczty email.

Subskrybent, lub osoba upoważniona, o której mowa w rozdziale 4.9.2 Kodeksu Postępowania Certyfikacyjnego systemu PKI NBP ma obowiązek niezwłocznego (najpóźniej w ciągu 3 dni roboczych od uruchomienia procedury awaryjnej) dostarczenia „Zamówienia na usługę kryptograficzną", które będzie podstawą do unieważnienia lub uchylenia zawieszenia zawieszonego certyfikatu..

4.10 Usługi weryfikacji statusu certyfikatu

Zgodnie z Kodeksem Postępowania Certyfikacyjnego systemu PKI NBP.

4.11 Zakończenie subskrypcji

Zgodnie z Kodeksem Postępowania Certyfikacyjnego systemu PKI NBP.

4.12 Deponowanie i odtwarzanie klucza

Klucze prywatne Subskrybentów służące do szyfrowania danych przesyłanych pomiędzy użytkownikami systemów informatycznych Europejskiego Systemu Banków Centralnych są deponowane w postaci zaszyfrowanej w bazie danych urzędu certyfikacji. Dodatkowe informacje znajdują się w rozdziale 4.3.1 oraz 6.1.1.
Odtworzenie klucza może być wykonane tylko przez AOK i jest realizowane na podstawie prawidłowo wypełnionego „Zamówienia na usługę kryptograficzną". Po odtworzeniu klucza jest on instalowany na nowej karcie elektronicznej, która następnie przekazywana jest Subskrybentowi. Przekazanie potwierdzone jest „Protokołem przekazania kluczy kryptograficznych".

5. Zabezpieczenia techniczne, organizacyjne i operacyjne

Zgodnie z Kodeksem Postępowania Certyfikacyjnego systemu PKI NBP.

6 Procedury bezpieczeństwa technicznego

6.1 Generowanie pary kluczy i jej instalowanie

6.1.1 Generowanie pary kluczy

Klucze kryptograficzne Subskrybentów służące do szyfrowania danych przesyłanych pomiędzy użytkownikami systemów informatycznych Europejskiego Systemu Banków Centralnych generowane są w bezpiecznym środowisku, a następnie są instalowane na kartach elektronicznych posiadających certyfikat ITSEC E3 High lub FIPS 140-2 level 3. Klucze kryptograficzne generowane są przez Operatorów PRU na wydzielonych do tego celu stacjach roboczych znajdujących się w PRU.

6.1.2 Przekazywanie klucza prywatnego subskrybentowi

Klucze kryptograficzne generowane na karcie elektronicznej są przekazywane Subskrybentowi przez Operatora PRU niezwłocznie po ich wygenerowaniu. Potwierdzeniem przekazania kluczy kryptograficznych są podpisy Operatora PRU oraz Subskrybenta umieszczone na „Protokole przekazania kluczy kryptograficznych".

6.1.3 Dostarczanie klucza publicznego do wystawcy

Przekazanie klucza publicznego do wystawcy odbywa się automatycznie, bez udziału Subskrybenta.

6.1.4 Przekazywanie klucza publicznego CCK

Klucze publiczne urzędów NBP Root CA oraz NBP Enterprise CA są dostępne w repozytorium (patrz rozdział 2.1). W szczególnych przypadkach mogą być dostarczone drogą mailową lub na nośniku elektronicznym.

6.1.5 Długości kluczy

Klucze kryptograficzne służące do uwierzytelniania w systemach ESCB mają długość 2048 bitów.

6.1.6 Parametry generowania klucza publicznego oraz weryfikacja jakości

Klucze publiczne są kodowane zgodnie z RFC 5280 i PKCS#1. Wszystkie generowane klucze kryptograficzne są kluczami algorytmu RSA.

6.1.7 Akceptowane zastosowanie kluczy (zgodnie z polem KeyUsage w X.509 v3)

Zgodnie z informacją zawartą w Załączniku A.

6.2 Ochrona klucza prywatnego oraz nadzorowanie mechanizmów modułu kryptograficznego

6.2.1 Standardy modułów kryptograficznych

Klucze kryptograficzne Subskrybentów służące do szyfrowania danych przesyłanych pomiędzy użytkownikami systemów informatycznych Europejskiego Systemu Banków Centralnych zapisane są na kartach elektronicznych posiadających certyfikat ITSEC E3 High lub FIPS 140-2 level 3. Do komunikacji z kartami elektronicznymi wykorzystywane są biblioteki PKCS#11.

6.2.2 Podział klucza prywatnego na części

Klucze prywatne Subskrybentów nie podlegają operacji dzielenia na części.

6.2.3 Deponowanie klucza prywatnego

Patrz rozdział 4.12.

6.2.4 Kopie zapasowe klucza prywatnego

Kopie zapasowe kluczy prywatnych służących do odszyfrowywania danych są deponowane w sposób bezpieczny w bazie danych CCK. Patrz rozdział 4.12.

6.2.5 Archiwizowanie klucza prywatnego

Ze względu na fakt, iż kopia klucza prywatnego jest deponowana w bazie danych CCK zastosowanie mają zapisy dotyczące kopii archiwalnych wykonywanych w systemie PKI NBP. Patrz Kodeks Postępowania Certyfikacyjnego PKI NBP.

6.2.6 Wprowadzenie lub pobieranie klucza prywatnego do/z modułu kryptograficznego

Nie dotyczy gdyż klucze prywatne Subskrybentów służące do szyfrowania danych przesyłanych pomiędzy użytkownikami systemów informatycznych Europejskiego Systemu Banków Centralnych generowane są w bezpiecznym środowisku, a przechowywane są na kartach elektronicznych. Po zainstalowaniu przez CCK kluczy kryptograficznych i certyfikatu na karcie elektronicznej, nie mogą zostać one z niej wyeksportowane.

6.2.7 Przechowywanie klucza prywatnego w module kryptograficznym

Klucze prywatne Subskrybentów służące do szyfrowania danych przesyłanych pomiędzy użytkownikami systemów informatycznych Europejskiego Systemu Banków Centralnych generowane są w bezpiecznym środowisku, a przechowywane są na kartach elektronicznych.

6.2.8 Metoda aktywacji klucza prywatnego

Po zapisaniu na karcie elektronicznej kluczy kryptograficznych oraz po zainstalowaniu na niej certyfikatu, klucz prywatny jest aktywowany dopiero po podaniu kodu PIN chroniącego tą kartę.

6.2.9 Metoda dezaktywacji klucza prywatnego

Klucz prywatny znajdujący się na karcie elektronicznej jest dezaktywowany w momencie wyjęcia tej karty z czytnika. W przypadku części systemów możliwe jest zdefiniowanie czasu bezczynności po jakim klucz prywatny zostanie automatycznie dezaktywowany nawet, gdy karta elektroniczna znajduje się w czytniku.

6.2.10 Metoda niszczenia klucza prywatnego

Niszczenie kluczy prywatnych Subskrybentów zapisanych na karcie elektronicznej polega na ich bezpiecznym usunięciu z karty elektronicznej lub na fizycznym zniszczeniu karty. Usunięcie kluczy kryptograficznych zdeponowanych w bazie danych urzędu certyfikacji dokonywane jest przez Operatorów CCK po otrzymaniu pisemnego wniosku od Subskrybenta.

6.2.11 Ocena modułu kryptograficznego

Patrz pkt. 6.2.1.

6.3 Inne aspekty zarządzania kluczami

6.3.1 Archiwizowanie kluczy publicznych

Zgodnie z Kodeksem Postępowania Certyfikacyjnego systemu PKI NBP.

6.3.2 Okresy stosowania klucza publicznego i prywatnego

Maksymalny okres ważności certyfikatów wydanych z szablonu „ESCB Szyfrowanie" oraz odpowiadających im pary kluczy kryptograficznych to 2 lata, jednak w szczególnych przypadkach możliwe jest wystawienie takiego certyfikatu na okres krótszy.

6.4 Dane aktywujące

Zgodnie z Kodeksem Postępowania Certyfikacyjnego systemu PKI NBP.

6.4.1 Generowanie danych aktywujących i ich instalowanie

Po dostarczeniu przez Subskrybenta karty elektronicznej do PRU, karta jest dodawana do specjalnej „bazy bezpieczeństwa" co pozwala na jej późniejsze wykorzystanie w systemie PKI NBP. Wystawienie certyfikatu na karcie elektronicznej nie znajdującej się w bazie bezpieczeństwa jest niemożliwe. Dane aktywujące klucz prywatny Subskrybenta (PIN chroniący kartę elektroniczną) są ustalane przez Operatora PRU w momencie generowania kluczy kryptograficznych. Podczas przekazywania kluczy kryptograficznych Subskrybentowi,

Operator PRU informuje go, iż powinien zmienić te dane na ustalone przez siebie. Na prośbę Subskrybenta, Operator PRU ma obowiązek pomóc Subskrybentowi dokonać zmiany kodu PIN.

6.4.2 Ochrona danych aktywujących

Operator PRU po wygenerowaniu danych aktywujących przekazuje informacje na ich temat Subskrybentowi. Żadna kopia tych danych nie jest przechowywana w PRU, a w przypadku zablokowania karty elektronicznej jej odblokowanie możliwe jest tylko przy udziale Operatora PRU.

6.4.3 Inne problemy związane z danymi aktywującymi

Dane służące do zmiany danych aktywujących (kody PUK do kart elektronicznych) są zapisane w „bazie bezpieczeństwa" w postaci zaszyfrowanej (algorytm 3DES) . Podczas odblokowywania karty elektronicznej przez Operatora PRU kod PUK jest przesyłany bezpośrednio do aplikacji zarządzającej kartami elektronicznymi i nie jest wyświetlany. Aplikacja zarządzająca kartami elektronicznymi po otrzymaniu kodu PUK pozwala Operatorowi PRU jedynie na odblokowanie karty i ustawienie nowego kodu PIN.

6.5 Nadzorowanie bezpieczeństwa systemu komputerowego

Zgodnie z Kodeksem Postępowania Certyfikacyjnego systemu PKI NBP.

6.6 Cykl życia zabezpieczeń technicznych

Zgodnie z Kodeksem Postępowania Certyfikacyjnego systemu PKI NBP.

6.7 Nadzorowanie zabezpieczeń sieci komputerowej

Zgodnie z Kodeksem Postępowania Certyfikacyjnego systemu PKI NBP.

6.8 Znakowanie czasem

Nie dotyczy.

7. Profile certyfikatów oraz list CRL

Profile certyfikatów oraz list unieważnionych certyfikatów są zgodne z formatami określonymi w normie ITU-T X.509 v3.

7.1 Profil certyfikatu

Zgodnie z Kodeksem Postępowania Certyfikacyjnego systemu PKI NBP oraz Załącznikiem A.

7.2 Profil listy unieważnionych certyfikatów (CRL)

Zgodnie z Kodeksem Postępowania Certyfikacyjnego systemu PKI NBP.

8. Audyt zgodności i inne oceny

Zgodnie z Kodeksem Postępowania Certyfikacyjnego systemu PKI NBP.

9. Inne kwestie biznesowe i prawne

Zgodnie z Kodeksem Postępowania Certyfikacyjnego systemu PKI NBP.

10. Ochrona danych osobowych

Zgodnie z Kodeksem Postępowania Certyfikacyjnego systemu PKI NBP.

Załącznik A – Szablon certyfikatów ESCB Szyfrowanie w systemie PKI NBP

Wersja	V3
Numer seryjny	Numer seryjny unikalny w systemie
Algorytm podpisu	Sha256RSA

Wystawca	`CN = NBP Enterprise CA`
	`OU = Centrum Certyfikacji Kluczy NBP`
	`O = Narodowy Bank Polski`
	`L = Warszawa`
	`C = PL`

Ważny od - do	`Maksymalnie 2 lata`
Podmiot	Konstruowany na podstawie danych z Active Directory, łącznie z adresem e-mail. W poszczególnych polach DN są kolejne węzły katalogu LDAP prowadzące do obiektu konta użytkownika w tym katalogu
Klucz publiczny	`RSA 2048 bitów`

Możliwości edytora SMIME	[1]Możliwości SMIME: Identyfikator obiektu=2.16.840.1.101.3.4.1.42 [2]Możliwości SMIME: Identyfikator obiektu=2.16.840.1.101.3.4.1.45 [3]Możliwości SMIME: Identyfikator obiektu=2.16.840.1.101.3.4.1.22 [4]Możliwości SMIME: Identyfikator obiektu=2.16.840.1.101.3.4.1.25 [5]Możliwości SMIME: Identyfikator obiektu=2.16.840.1.101.3.4.1.2 [6]Możliwości SMIME: Identyfikator obiektu=2.16.840.1.101.3.4.1.5 [7]Możliwości SMIME: Identyfikator obiektu=1.2.840.113549.3.7 [8]Możliwości SMIME: Identyfikator obiektu=1.3.14.3.2.7 [9]Możliwości SMIME: Identyfikator obiektu=1.2.840.113549.3.2 Parametry=02 02 00 80 [10]Możliwości SMIME: Identyfikator obiektu=1.2.840.113549.3.4 Parametry=02 02 02 00
Zasady aplikacji	[[1]Zasady certyfikatu aplikacji: Identyfikator zasad=Bezpieczna poczta e-mail
Informacja o szablonie certyfikatu	Szablon=ESCB Szyfrowanie(1.3.6.1.4.1.311.21.8.8041467.6109741.1199773.5170465.10588945.146.5233154.16470863) Główny numer wersji=100 Numer podrzędny wersji=72
Dostęp do informacji o urzędach	[1]Dostęp do informacji o urzędzie Metoda dostępu=Protokół stanu certyfikatu online (1.3.6.1.5.5.7.48.1) Nazwa zapasowa: Adres URL=http://ocsp.nbp.pl/ocsp [2]Dostęp do informacji o urzędzie

	Metoda dostępu=Urząd certyfikacji - wystawca (1.3.6.1.5.5.7.48.2) Nazwa zapasowa: Adres URL=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]Dostęp do informacji o urzędzie Metoda dostępu=Urząd certyfikacji - wystawca (1.3.6.1.5.5.7.48.2) Nazwa zapasowa: Adres URL=http://pki.nbp.pl/pki/eca(3).crt
Identyfikator klucza podmiotu	160 bitowy skrót z klucza publicznego Subskrybenta
Alternatywna nazwa podmiotu	Nazwa główna= UPN Subskrybenta, Nazwa RFC822= adres e-mail Subskrybenta
Punkty dystrybucji listy CRL	[1]Punkt dystrybucji CRL Nazwa punktu dystrybucji: Pełna nazwa: Adres URL=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 Adres URL=http://pki.nbp.pl/pki/eca(2).crl
Zasady certyfikatu	[1]Zasady certyfikatu: Identyfikator zasad=1.3.6.1.4.1.31995.1.1.2 [1,1]Informacje o kwalifikatorze zasad: Identyfikator kwalifikatora zasad=CPS Kwalifikator: http://pki.nbp.pl/pki/ [2]Zasady certyfikatu: Identyfikator zasad=1.3.6.1.4.1.31995.1.2.3.1 [2,1]Informacje o kwalifikatorze zasad: Identyfikator kwalifikatora zasad=CPS Kwalifikator: http://pki.nbp.pl/pki/

Identyfikator klucza urzędu	160 bitowy skrót z klucza publicznego urzędu NBP Enterprise CA
Użycie klucza rozszerzonego	Bezpieczna poczta e-mail (1.3.6.1.5.5.7.3.4)
Użycie klucza (*)	Szyfrowanie klucza, szyfrowanie danych
Podstawowe warunki ograniczające (*)	Typ podmiotu=Jednostka końcowa Warunki ograniczające długość ścieżki = Brak

(*) – rozszerzenie krytyczne

Załącznik B – Informacja o warunkach użycia certyfikatu wydanego w systemie PKI NBP

.....dnia .....

Protokół przekazania kluczy kryptograficznych

W dniu ..... Operator PRU .....
(data) (nazwa PRU)

przekazał Subskrybentowi ..... klucze kryptograficzne i certyfikat:
(nazwa Subskrybenta)

☐ wygenerowany zgodnie z szablonem „ESCB Logowanie"

☐ wygenerowany zgodnie z szablonem „ESCB Podpis"

☐ wygenerowany zgodnie z szablonem „ESCB Szyfrowanie"

Hasła do awaryjnego unieważnienia certyfikatów:

ESCB Logowanie ……

ESCB Podpis ……

ESCB Szyfrowanie ……

Akceptacja certyfikatów

Składając podpis na niniejszym „Protokole przekazania kluczy kryptograficznych" Subskrybent:

- przyjmuje certyfikat,
- potwierdza, iż został poinformowany o fakcie, iż zasady obowiązujące w systemie PKI NBP opisane zostały w Kodeksie Postępowania Certyfikacyjnego Systemu PKI NBP oraz Politykach Certyfikacji. Dokumenty te dostępne są na stronie http://pki.nbp.pl/pki/ ,
- potwierdza zapoznanie się i akceptuje „Informację o warunkach użycia certyfikatu wydanego w systemie PKI NBP" zamieszczoną na następnej stronie niniejszego Protokołu.

(Imię i nazwisko osoby przekazującej) (Imię i nazwisko Subskrybenta)

(podpis) (podpis)

Informacja o warunkach użycia certyfikatu wydanego w systemie PKI NBP

1. Certyfikaty systemu PKI NBP wydawane są osobom zatrudnionym w NBP lub w firmach wykonujących zadania na rzecz NBP.
2. Zasady obowiązujące w systemie PKI NBP (w tym prawa i obowiązki Subskrybentów, stron ufających, a także Centrum Certyfikacji Kluczy oraz Punktów Rejestracji Użytkowników) określone są w Kodeksie Postępowania Certyfikacyjnego oraz w Politykach Certyfikacji.
3. Subskrybent ma obowiązek używania kluczy kryptograficznych i certyfikatów tylko zgodnie z ich przeznaczeniem określonym w Polityce Certyfikacji wskazanej w tym certyfikacie.
4. Zakres stosowania certyfikatów wydawanych w systemie PKI NBP jest następujący:
   - Certyfikaty zgodne z szablonem „ESCB Logowanie" – do uwierzytelniania Subskrybenta w systemach informatycznych Europejskiego Systemu Banków Centralnych (ESBC);
   - Certyfikaty zgodne z szablonem „ESCB Podpis" – do składania podpisu elektronicznego w systemach informatycznych Europejskiego Systemu Banków Centralnych (ESBC);
   - Certyfikaty zgodne z szablonem „ESCB Szyfrowanie" – do szyfrowania informacji przesyłanych pomiędzy użytkownikami systemów informatycznych Europejskiego Systemu Banków Centralnych (ESBC);
5. Subskrybent ma obowiązek:
   - niezwłocznie informować PRU o wszelkich zmianach danych zawartych w certyfikacie,
   - przestrzegać zapisów Kodeksu Postępowania Certyfikacyjnego Systemu PKI NBP oraz odpowiednich Polityk Certyfikacji,
   - zapewnić należytą ochronę swojego klucza prywatnego oraz danych służących do jego aktywacji,
   - wykorzystywać klucze kryptograficzne i certyfikaty systemu PKI NBP tylko w zakresie określonym w certyfikacie oraz opisanym w punkcie 4 powyżej,
   - natychmiast żądać unieważnienia swojego certyfikatu w przypadku kompromitacji odpowiadającego mu klucza prywatnego.

6. W przypadku naruszenia przez Subskrybenta zasad określonych w niniejszej „Informacji o warunkach użycia certyfikatu wydanego w systemie PKI NBP" jego certyfikat może zostać unieważniony.
7. NBP nie jest kwalifikowanym dostawcą usług zaufania, a certyfikaty wystawiane w systemie PKI NBP nie są kwalifikowanymi certyfikatami.

Załącznik C – Historia zmian dokumentu

Lp.	Data	Wersja	Osoba	Opis wykonanych prac
1.	10.09.2013	0.1		Utworzenie dokumentu
2.	13.09.2013	0.2		Przegląd i uzupełnienie dokumentu
3.	13.09.2013	0.3		Przegląd dokumentu
4.	17.09.2013	0.4		Przegląd i uzupełnienie dokumentu
5.	20.09.2013	0.5		Przegląd dokumentu
6.	23.09.2013	0.6		Przegląd dokumentu
7.	**02.10.2013**	**1.0**		**Zatwierdzenie dokumentu**
8.	03.06.2014	1.01		Zmiany w rozdziale 2 oraz Załączniku A w związku z wymianą kluczy kryptograficznych urzędów w systemie
9.	03.06.2014	1.01		Przegląd dokumentu
10.	03.06.2014	1.01		Przegląd dokumentu
11.	06.06.2014	1.01		Przegląd dokumentu
12	**10.06.2014**	**1.1**		**Zatwierdzenie dokumentu**
13	05.02.2015	1.11		Dostosowanie dokumentu do zapisów Uchwały nr 1/2015 Zarządu NBP
14	06.02.2015	1.12		Przegląd dokumentu
15	20.10.2016	1.21		Zmiany w związku z wymianą funkcji skrótu wykorzystywanej w systemie oraz dostosowanie do uchwały nr 53/2016 Zarządu NBP
16	**16.12.2016**	**1.3**		**Zatwierdzenie dokumentu**
17	20.02.2017	1.31		Zmiany w związku z uwagami otrzymanymi z PKI Assessment Body (EBC)
18	27.02.2017	1.31		Przegląd dokumentu
19	02.03.2017	1.32		Przegląd dokumentu

Uzgodnienie dokumentu

Data	Wersja	Osoba	Podpis
	1.4	Dyrektor Departamentu Informatyki i Telekomunikacji	

Zatwierdzenie dokumentu

Data	Wersja	Osoba	Podpis
	1.4	Dyrektor Departamentu Bezpieczeństwa	