NBP Narodowy Bank Polski

Kodeks Postępowania Certyfikacyjnego Systemu PKI NBP

OID: 1.3.6.1.4.1.31995.1.1.2
wersja 2.1

Departament Bezpieczeństwa NBP
Warszawa, 2018

Spis treści

1. Wstęp

1.1 Wprowadzenie

Niniejszy Kodeks Postępowania Certyfikacyjnego Systemu PKI NBP zwany dalej „Kodeksem" opisuje funkcjonowanie systemu informatycznego infrastruktury klucza publicznego Narodowego Banku Polskiego, zwanego dalej „systemem PKI NBP" i ma zastosowanie dla wszystkich użytkowników systemu PKI NBP tzn. Centrów Certyfikacji Kluczy, Punktów Rejestracji Użytkowników, podmiotów wnioskujących o certyfikat, Subskrybentów oraz stron ufających. Kodeks określa zasady świadczenia usług certyfikacyjnych, począwszy od rejestracji Subskrybentów, certyfikacji kluczy publicznych, aktualizacji kluczy i certyfikatów, a na unieważnianiu certyfikatów kończąc. Stanowi on swego rodzaju „przewodnik" w relacjach pomiędzy systemem PKI NBP a jego użytkownikami. Z tego powodu wszyscy użytkownicy systemu PKI NBP powinni znać Kodeks i stosować się do zapisów w nim zawartych.

Struktura i merytoryczna zawartość niniejszego Kodeksu są zgodne z dokumentem RFC 3647 *Certificate Policy and Certificate Practice Statement Framework*. W Kodeksie zostały zawarte wszystkie elementy opisane w RFC 3647. Zabieg ten ma na celu uczynienie dokumentu bardziej przejrzystym i bardziej przyjaznym dla czytelników. W przypadku, gdy wymieniony element nie występuje w systemie PKI NBP w odpowiednim rozdziale wpisano „Nie dotyczy".

1.2 Nazwa dokumentu i jego identyfikacja

Nazwa dokumentu	Kodeks Postępowania Certyfikacyjnego Systemu PKI NBP
Wersja dokumentu	2.1
Status dokumentu	Aktualny
Data wprowadzenia	07.06.2018
OID	1.3.6.1.4.1.31995.1.1.2
Lokalizacja	http://pki.nbp.pl/pki/kodeks.pdf

1.3 Strony Kodeksu Postępowania Certyfikacyjnego

1.3.1 Narodowy Bank Polski

Narodowy Bank Polski, zwany dalej „NBP", jest właścicielem systemu PKI NBP. Wszystkie osoby pełniące zaufane role w systemie PKI NBP są pracownikami NBP. Elementy systemu PKI NBP zlokalizowane są w ośrodkach będących własnością NBP.

NBP odpowiada za funkcjonowanie całości systemu PKI NBP. Wybrane elementy systemu PKI NBP mogą być objęte umowami serwisowymi i wsparcia, zawartymi pomiędzy NBP a firmami zewnętrznymi, jednak

usługi zaufania w tym systemie świadczone są wyłącznie przez pracowników NBP. Zakres obowiązków i odpowiedzialności firm zewnętrznych regulują odrębne umowy.

1.3.2 Departament Bezpieczeństwa

Departament Bezpieczeństwa, zwany dalej „DB" jest odpowiedzialny za opracowanie, aktualizację i publikację Kodeksu oraz za wyznaczenie:

- Operatorów Centrum Certyfikacji Kluczy,
- Administratorów HSM,
- Operatorów HSM,
- Agentów Odzyskiwania Danych,
- Agentów Odzyskiwania Kluczy,
- Inspektorów Bezpieczeństwa Systemu,
- Audytorów Systemu,
- Operatorów Punktów Rejestracji Użytkowników w Centrali NBP.

Dodatkowo DB odpowiedzialny jest za administrowanie systemem kontroli dostępu do pomieszczeń, w których znajdują się elementy systemu PKI NBP oraz za wyposażenie Subskrybentów w karty elektroniczne będące nośnikami kluczy kryptograficznych i certyfikatów .

1.3.3 Departament Informatyki i Telekomunikacji

Departament Informatyki i Telekomunikacji, zwany dalej „DIT" jest odpowiedzialny za zapewnienie infrastruktury sprzętowej i systemowej dla prawidłowego funkcjonowania systemu, administrowanie systemem, wyznaczenie Administratorów Systemu oraz za konserwację i serwis wykorzystywanego sprzętu informatycznego oraz oprogramowania systemowego i baz danych.

1.3.4 Oddziały Okręgowe NBP

Oddziały okręgowe NBP odpowiedzialne są za wyznaczenie Operatorów Punktów Rejestracji Użytkowników w tych oddziałach.

1.3.5 Centrum Certyfikacji Kluczy

Operator Centrum Certyfikacji Kluczy odpowiada za wydawanie, unieważnianie i publikację certyfikatów Subskrybentów. W systemie PKI NBP za funkcjonowanie Centrum Certyfikacji Kluczy odpowiada DB.

1.3.6 Punkt Rejestracji Użytkowników

Operator Punktu Rejestracji Użytkowników odpowiada za weryfikację tożsamości Subskrybentów, a także przesyła w ich imieniu wnioski o wydanie, odnowienie lub unieważnienie certyfikatów do Centrum Certyfikacji Kluczy. W systemie PKI NBP za funkcjonowanie Punktów Rejestracji Użytkowników w oddziałach okręgowych odpowiadają oddziały okręgowe NBP.
Za funkcjonowanie Punktu Rejestracji Użytkowników w Centrali NBP odpowiedzialne jest DB.

1.3.7 Subskrybenci

Subskrybentem może być osoba fizyczna dla której wystawiono w systemie PKI NBP certyfikat.

1.3.8 Strony ufające

Stroną ufającą jest osoba lub podmiot, inna niż Subskrybent, która akceptuje i ufa certyfikatowi wydanemu w systemie PKI NBP.

1.4 Zakres stosowania certyfikatów

Zgodnie z odpowiednią Polityką Certyfikacji.

1.5 Administrowanie Kodeksem Postępowania Certyfikacyjnego

1.5.1 Organizacja odpowiedzialna za administrowanie dokumentem

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

1.5.2 Kontakt

Za zarządzanie Kodeksem 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

Ogólne zasady świadczenia usług zaufania w systemie PKI NBP określone są w Uchwale nr 53/2016 Zarządu NBP. W szczególności zawarte są tam informacje związane z odpowiedzialnością NBP jako podmiotu świadczącego usługi zaufania, informacje dotyczące podziału zadań pomiędzy poszczególnymi departamentami i oddziałami okręgowymi NBP, a także informacje dotyczące kontroli i audytu. Niniejszy Kodeks powstał na bazie załącznika nr 3 do ww. Uchwały i jest zatwierdzany przez Dyrektora DB.

Każda z wersji Kodeksu obowiązuje (posiada status aktualny) do czasu zatwierdzenia i opublikowania nowej wersji. Nowa wersja opracowywana jest przez pracowników DB i ze statusem „do uzgodnienia" jest przekazywana do DIT. Po uzgodnieniu dokumentu, nowa wersja Kodeksu zatwierdzana jest przez Dyrektora DB.

W przypadku, zmiany zapisów Kodeksu mających swoje źródło w Uchwale nr 53/2016 Zarządu NBP - przed opracowaniem nowej wersji Kodeksu konieczne jest dokonanie niezbędnej zmiany uchwały. Zmiana uchwały odbywa się na zasadach obowiązujących w NBP.

Pracownicy DB nie rzadziej niż raz w roku, oraz w przypadku wprowadzania jakichkolwiek zmian w systemie PKI NBP dokonują przeglądu Kodeksu oraz Polityk Certyfikacji pod kątem ich aktualności.

1.6 Definicje i skróty

1.6.1 Definicje

Na użytek Kodeksu przyjmuje się następujące pojęcia:

- **Centrum Certyfikacji Kluczy** – moduł systemu PKI NBP wystawiający certyfikaty, 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 którego pomocą 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 przez CCK,
- **uwierzytelnienie** - właściwość umożliwiająca potwierdzenie deklarowanej tożsamości nadawcy informacji.

1.6.2 Skróty

Wykaz stosowanych w Kodeksie 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)

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

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)

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 .
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(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(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

Certyfikaty CCK publikowane są natychmiast po ich wygenerowaniu. Listy CRL generowane przez NBP Root CA publikowane są nie rzadziej niż raz na 6 miesięcy oraz niezwłocznie po unieważnieniu certyfikatu wydanego przez ten urząd. Listy CRL generowane przez NBP Enterprise CA są publikowane co godzinę. Dodatkowo, Operator PRU może w dowolnym momencie ręcznie wygenerować i opublikować listę CRL urzędu NBP Enterprise CA.

2.4 Kontrola dostępu do repozytorium

Dostęp do http://pki.nbp.pl/pki jest ograniczony tylko do odczytu i zabezpieczony przed nieautoryzowaną zmianą zawartości.

3. Identyfikacja i uwierzytelnianie

Poniżej przedstawiono ogólne zasady weryfikacji tożsamości Subskrybentów, którymi kieruje się CCK podczas wydawania certyfikatów. Zasady te oparte na określonych typach informacji, które umieszczane są w treści certyfikatu, definiują środki, które są niezbędne do uzyskania pewności, iż informacje te są precyzyjne i wiarygodne w momencie wydawania certyfikatu. Procedura weryfikacji tożsamości Subskrybenta jest przeprowadzana zgodnie z Polityką Certyfikacji dla poszczególnych typów certyfikatów.

3.1 Nadawanie nazw

Certyfikaty wydawane przez CCK są zgodne z normą X.509 v3. W szczególności oznacza to, że zarówno wystawca certyfikatu, jak też działający w jego imieniu PRU akceptują tylko takie nazwy Subskrybentów, które są zgodne ze standardem X.509 (z powołaniem się na zalecenia serii X.500).

3.1.1 Typy nazw

Zgodnie z odpowiednią Polityką Certyfikacji.

3.1.2 Konieczność używania nazw znaczących

W systemie PKI NBP wszystkie nazwy wchodzące w skład identyfikatora wyróżniającego Subskrybenta muszą posiadać swoje znaczenie w języku polskim lub angielskim.

3.1.3 Zasady interpretacji różnych form nazw

Identyfikatory wyróżniające Subskrybentów są interpretowane zgodnie z ISO/IEC 9595 (X.500) Distinguished Name (DN) standard.

3.1.4 Unikalność nazw

Wyróżnikiem certyfikatu, precyzyjnie i jednoznacznie określającym Subskrybenta, jest identyfikator wyróżniający wraz z alternatywną nazwą Subskrybenta (zawierającą UPN) umieszczone w tym certyfikacie.

NBP zapewnia, iż identyfikator wyróżniający znajdujący się w certyfikacie CCK jest przypisany tylko do jednego CCK i po zakończeniu jego pracy nie będzie nadawany powtórnie.

3.1.5 Rozpoznawanie, uwierzytelnianie oraz rola znaków towarowych

Nie dotyczy.

3.2 Początkowa walidacja tożsamości

3.2.1 Dowód posiadania klucza prywatnego

Zgodnie z odpowiednią Polityką Certyfikacji.

3.2.2 Uwierzytelnienie tożsamości osób prawnych

Nie dotyczy.

3.2.3 Uwierzytelnienie tożsamości osób fizycznych

Zgodnie z odpowiednią Polityką Certyfikacji.

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

Zgodnie z odpowiednią Polityką Certyfikacji.

3.3.1 Identyfikacja i uwierzytelnienie w przypadku normalnej aktualizacji kluczy

Zgodnie z odpowiednią Polityką Certyfikacji.

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

Zgodnie z odpowiednią Polityką Certyfikacji.

4. Wymagania funkcjonalne

Podstawowym wymogiem formalnym jest złożenie przez Subskrybenta stosownego wniosku. Na jego podstawie CCK podejmuje odpowiednią decyzję, realizując żądaną usługę, lub odmawiając jej realizacji. Składane wnioski powinny zawierać informacje, które są niezbędne do prawidłowego zidentyfikowania Subskrybenta.

4.1 Składanie wniosków

Wnioski Subskrybenta mogą być składane do CCK bezpośrednio lub pośrednio przy udziale PRU.
Operator PRU występuje w podwójnej roli: Subskrybenta oraz osoby upoważnionej do reprezentowania CCK. W pierwszej roli Operator PRU może składać takie same wnioski jak każdy inny Subskrybent. Z kolei w roli drugiej może potwierdzać wnioski innych Subskrybentów oraz, w uzasadnionych przypadkach, tworzyć wnioski o unieważnienie certyfikatów Subskrybentów, którzy naruszają niniejszy Kodeks.
Wnioski dostarczane są w postaci elektronicznej lub innej – np. jako „Zamówienie na usługę kryptograficzną".

4.1.1 Kto może złożyć wniosek o wydanie certyfikatu?

Zgodnie z odpowiednią Polityką Certyfikacji.

4.1.2 Proces składania wniosków i związane z tym obowiązki

Zgodnie z odpowiednią Polityką Certyfikacji.

4.2 Przetwarzanie wniosków

4.2.1 Realizacja funkcji identyfikacji i uwierzytelniania

Zgodnie z odpowiednią Polityką Certyfikacji.

4.2.2 Przyjęcie lub odrzucenie wniosku

Zgodnie z odpowiednią Polityką Certyfikacji.

4.2.3 Okres oczekiwania na przetworzenie wniosku

Zarówno CCK jak i PRU dokładają wszelkich starań, by wnioski składane przez Subskrybentów były przetwarzane w możliwie jak najkrótszym czasie. Wnioski o wydanie nowego certyfikatu obsługiwane są w godzinach pracy PRU (dni powszednie w godzinach 7:30-16:00), a maksymalny czas ich przetwarzania to 2 godziny. Zasady obsługi wniosków o unieważnienie certyfikatu opisane są w rozdziale 4.9.

4.3 Wydanie certyfikatu

4.3.1 Czynności CCK wykonywane podczas wydawania certyfikatu

Zgodnie z odpowiednią Polityką Certyfikacji.

4.3.2 Informowanie subskrybenta o wydaniu certyfikatu

Zgodnie z odpowiednią Polityką Certyfikacji.

4.4 Akceptacja certyfikatu

4.4.1 Potwierdzenie akceptacji certyfikatu

Zgodnie z odpowiednią Polityką Certyfikacji.

4.4.2 Publikowanie certyfikatu przez CCK

Zgodnie z odpowiednią Polityką Certyfikacji.

4.4.3 Informowanie innych podmiotów o wydaniu certyfikatu

Nie dotyczy.

4.5 Stosowanie kluczy oraz certyfikatów

4.5.1 Stosowanie kluczy i certyfikatów przez subskrybenta

Zgodnie z odpowiednią Polityką Certyfikacji.

4.5.2 Stosowanie kluczy i certyfikatu przez stronę ufającą

Zgodnie z odpowiednią Polityką Certyfikacji.

4.6 Recertyfikacja

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

4.7 Odnowienie certyfikatu

Odnowienie certyfikatu ma miejsce zawsze wtedy, gdy Subskrybent (już zarejestrowany) wygeneruje nową parę kluczy (lub zleci to CCK) i zażąda wystawienia nowego certyfikatu potwierdzającego przynależność do niego nowego klucza publicznego.
Odnowienie certyfikatu dotyczy zawsze ściśle określonego, wskazanego we wniosku, certyfikatu. Z tego powodu nowy certyfikat posiada identyczną treść jak związany z nim certyfikat, jedyne różnice to: nowa

para kluczy, nowy numer seryjny certyfikatu, nowy okres ważności certyfikatu oraz nowy podpis CCK. Dodatkowo dopuszczalne są zmiany w identyfikatorze wyróżniającym certyfikatu.
Procedurze odnowienia certyfikatu podlegają również certyfikaty CCK. Nowe klucze kryptograficzne i certyfikat CCK generowane są najpóźniej:

- na dwa lata przed końcem okresu ważności aktualnie wykorzystywanego certyfikatu (w przypadku urzędu NBP Enterprise CA),
- na dziesięć lat przed końcem okresu ważności aktualnie wykorzystywanego certyfikatu (w przypadku urzędu NBP Root CA).

Operacja ta wykonywana jest przez Operatorów CCK i Operatorów HSM pod nadzorem Inspektora Bezpieczeństwa Systemu PKI NBP.

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,
- zmiana formatu (np. zmiana nośnika kluczy prywatnych).

4.7.2 Kto może żądać odnowienia certyfikatu?

Zgodnie z odpowiednią Polityką Certyfikacji.

4.7.3 Przetwarzanie wniosku o odnowienie certyfikatu

Zgodnie z odpowiednią Polityką Certyfikacji.

4.7.4 Informowanie o wydaniu nowego certyfikatu

Zgodnie z odpowiednią Polityką Certyfikacji.

4.7.5 Potwierdzenie akceptacji nowego certyfikatu

Zgodnie z odpowiednią Polityką Certyfikacji.

4.7.6 Publikowanie nowego certyfikatu

Zgodnie z odpowiednią Polityką Certyfikacji.

4.7.7 Informowanie o wydaniu certyfikatu innych podmiotów

Nie dotyczy.

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

Niniejszy rozdział określa warunki, które muszą być spełnione, aby CCK miało podstawy do unieważnienia lub zawieszenia certyfikatu. Mimo, iż zawieszenie certyfikatu jest szczególną formą unieważnienia, w dalszej części rozróżniać będziemy te dwa pojęcia dla podkreślenia istotnej różnicy między nimi: zawieszenie certyfikatu może być cofnięte, a unieważnienie certyfikatu jest ostateczne.
Unieważnienie lub zawieszenie certyfikatu ma ściśle określony wpływ na certyfikaty oraz obowiązki posługującego się nim Subskrybenta. W trakcie trwania zawieszenia lub natychmiast po unieważnieniu certyfikatu Subskrybenta należy uznać, że certyfikat stracił ważność. Unieważnienie lub zawieszenie certyfikatu nie ma wpływu na wcześniej zaciągnięte zobowiązania lub obowiązki wynikające z przestrzegania niniejszego Kodeksu. Zawieszenie certyfikatu jest czasowe i trwa zwykle do czasu wyjaśnienia wątpliwości, które były podstawą do zawieszenia. Na przykład, jeśli Subskrybent straci kontrolę nad nośnikiem klucza prywatnego, to powinien natychmiast zgłosić ten fakt do PRU lub CCK z żądaniem zawieszenia certyfikatu powiązanego z tym kluczem. W przypadku odnalezienia nośnika oraz pewności, że nie zostało naruszone bezpieczeństwo klucza prywatnego, certyfikat może być (na wniosek Subskrybenta) odwieszony, co przywróci mu stan aktywności. W przypadku unieważnienia lub zawieszenia certyfikatu, klucz prywatny powiązany z tym certyfikatem, o ile pozostaje pod kontrolą Subskrybenta, powinien być przez niego nadal chroniony w sposób, który gwarantuje jego wiarygodność przez cały okres zawieszenia certyfikatu oraz przechowywany po unieważnieniu, aż do momentu fizycznego zniszczenia.

4.9.1 Okoliczności unieważnienia certyfikatu

Podstawowymi przyczynami unieważnienia certyfikatu mogą być:

- utrata kontroli nad kluczem prywatnym powiązanym z danym certyfikatem,
- naruszenie przez Subskrybenta zasad Kodeksu lub Polityki Certyfikacji,
- wymiana certyfikatu (np. w przypadku zmiany danych w nim zawartych),
- ujawnienie klucza prywatnego ,
- rozwiązanie umowy pomiędzy NBP a Subskrybentem,
- każde żądanie unieważnienia certyfikatu zgłoszone przez osobę wymienioną w punkcie 4.9.2,
- zakończenie działalności CCK (w takim przypadku unieważnia się wszystkie certyfikaty wydane przez to CCK przed upływem deklarowanego terminu zakończenia działalności, a także certyfikat samego CCK),
- kompromitacja klucza prywatnego CCK,
- kompromitacja algorytmu kryptograficznego (lub parametrów z nim związanych) powiązanego z danym certyfikatem.

4.9.2 Kto może żądać unieważnienia certyfikatu

Unieważnienia certyfikatu Subskrybenta mogą żądać jedynie:

- Subskrybent wskazany w tym certyfikacie,
- dyrektor departamentu lub oddziału okręgowego NBP, w którym zatrudniony jest Subskrybent (w przypadku, gdy jest on pracownikiem NBP),
- w przypadku Subskrybentów nie będących pracownikami NBP - dyrektor departamentu lub oddziału okręgowego NBP, z którym firma zatrudniająca Subskrybenta, podpisała umowę,
- Operator PRU, który może wystąpić z wnioskiem w imieniu Subskrybenta lub z własnej inicjatywy, jeśli jest w posiadaniu informacji, uzasadniającej unieważnienie certyfikatu,
- Operator CCK – tylko w przypadku zakończenia działalności CCK lub kompromitacji klucza CCK.

Subskrybent wskazany w unieważnianym certyfikacie jest niezwłocznie powiadamiany o fakcie unieważnienia jego certyfikatu.

4.9.3 Procedura unieważniania certyfikatu

W systemie PKI NBP funkcjonują dwie procedury pozwalające na unieważnienie certyfikatów:

- **Procedura standardowa** – stosowana tylko w czasie pracy PRU (dni powszednie w godzinach 7:30-16:00) dla wszystkich szablonów certyfikatów. W ramach tej procedury osoba uprawniona (wymieniona w punkcie 4.9.2) za pomocą „Zamówienia na usługę kryptograficzną" zgłasza do PRU konieczność unieważnienia certyfikatu. Operator PRU dokonuje unieważnienia w terminie wskazanym w dostarczonym „Zamówieniu na usługę kryptograficzną" lub, w przypadku braku terminu na „Zamówieniu", w pierwszym dniu roboczym po otrzymaniu tego „Zamówienia",
- **Procedura awaryjna** – stosowana w dni robocze poza godzinami pracy PRU oraz w dni wolne od pracy. Procedura ta dostępna jest tylko dla wybranych szablonów certyfikatów. Dokładny opis procedury awaryjnej dla danego szablonu certyfikatu znajduje się w odpowiedniej Polityce Certyfikacji .

Informacja o tym, czy dany szablon certyfikatu objęty jest procedurą awaryjną, znajduje się w Polityce Certyfikacji dla tego szablonu.

4.9.4 Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu

Unieważnienie certyfikatu wykonywane jest bez zbędnej zwłoki, natychmiast po przetworzeniu wniosku o unieważnienie.

4.9.5 Maksymalny dopuszczalny czas przetwarzania wniosku o unieważnienie

W przypadku procedury standardowej wnioski o unieważnienie realizowane są najpóźniej w pierwszym dniu roboczym po otrzymaniu takiego wniosku.

W przypadku procedury awaryjnej wnioski realizowane są w czasie określonym w Polityce Certyfikacji.

4.9.6 Obowiązek sprawdzania list CRL przez stronę ufającą

Strona ufająca przed użyciem certyfikatu wydanego w systemie PKI NBP zobowiązana jest do zweryfikowania statusu tego certyfikatu. Może być to wykonane za pomocą sprawdzenia listy CRL lub skorzystania z usługi OCSP.

W przypadku braku możliwości skorzystania z usługi OCSP, strona ufająca powinna sprawdzać status certyfikatu z użyciem najbardziej aktualnej listy CRL.

4.9.7 Częstotliwość publikowania list CRL

Każde z Centrów Certyfikacji Kluczy funkcjonujących w ramach systemu PKI NBP wydaje oddzielną listę unieważnionych certyfikatów. Lista CRL urzędu NBP Root CA uaktualniana jest nie rzadziej niż raz na 6 miesięcy (oraz niezwłocznie po unieważnieniu certyfikatu wydanego przez ten urząd) i jest publikowana ręcznie. Lista CRL urzędu NBP Enterprise CA uaktualniana jest co godzinę i jest publikowana automatycznie. Dodatkowo w przypadku konieczności unieważnienia certyfikatu związanego z ujawnieniem klucza prywatnego lista CRL jest generowana i publikowana przez Operatora CCK niezwłocznie po dokonaniu unieważnienia.

4.9.8 Maksymalne opóźnienie w publikowaniu list CRL

Listy CRL są publikowane w repozytorium bez zbędnej zwłoki natychmiast po ich wygenerowaniu.

4.9.9 Dostępność usługi OCSP

Usługa OCSP systemu PKI NBP dostępna jest pod adresem http://ocsp.nbp.pl/ocsp .

Adres ten dostępny jest zarówno z sieci wewnętrznej NBP jak i z internetu.

4.9.10 Obowiązek sprawdzania unieważnień w trybie on-line

Strona ufająca przed użyciem certyfikatu wydanego w systemie PKI NBP zobowiązana jest do zweryfikowania statusu tego certyfikatu. Może być to wykonane za pomocą sprawdzenia listy CRL lub skorzystania z usługi OCSP.

4.9.11 Inne dostępne formy ogłaszania unieważnień certyfikatów

Nie dotyczy.

4.9.12 Specjalne obowiązki w przypadku naruszenia ochrony klucza

W przypadku ujawnienia lub podejrzenia ujawnienia klucza prywatnego należącego do CCK stosuje się wszelkie dostępne środki w celu niezwłocznego poinformowania o tym fakcie stron ufających, odwołujących się do informacji zgromadzonej w repozytorium zarządzanym przez PKI NBP.

4.9.13 Okoliczności zawieszenia certyfikatu

Certyfikat Subskrybenta może zostać zawieszony w przypadku:

- podejrzenia ujawnienia klucza prywatnego ,
- gdy zażąda tego Subskrybent wskazany w certyfikacie lub inna osoba wymieniona w punkcie 4.9.14,
- gdy Operator PRU otrzyma żądanie unieważnienia certyfikatu lecz nie jest w stanie zweryfikować uprawnień osoby składającej to żądanie (np. w przypadku procedury awaryjnej).

4.9.14 Kto może żądać zawieszenia certyfikatu

Zawieszenia certyfikatu Subskrybenta mogą żądać jedynie:

- Subskrybent wskazany w tym certyfikacie,
- dyrektor departamentu lub oddziału okręgowego NBP, w którym zatrudniony jest Subskrybent (w przypadku Subskrybentów będących pracownikami NBP),
- dyrektor departamentu lub oddziału okręgowego NBP, który podpisała umowę z firmą zatrudniającą Subskrybenta,
- Operator PRU, występujący z wnioskiem w imieniu Subskrybenta lub z własnej inicjatywy, jeśli jest w posiadaniu informacji, uzasadniającej zawieszenie certyfikatu.

4.9.15 Procedura zawieszenia i uchylenia zawieszenia certyfikatu

Osoba uprawniona (wymieniona w punkcie 4.9.14) za pomocą „Zamówienia na usługę kryptograficzną" zgłasza do PRU konieczność zawieszenia certyfikatu. Operator PRU otrzymując informację o konieczności zawieszenia certyfikatu przekazuje do CCK odpowiednie żądanie, które potwierdza swoim podpisem, a następnie informuje właściciela certyfikatu o zmianie jego statusu.

Certyfikaty systemu PKI NBP są także zawieszane w przypadku zastosowania „procedury awaryjnej", o której mowa w rozdziale 4.9.3. Ze względu na fakt, iż w procedura awaryjna nie pozwala na pełną weryfikację tożsamości osoby zgłaszającej – Operator CCK zawiesza certyfikat do czasu otrzymania odpowiedniego „Zamówienia na usługę kryptograficzną" („Zamówienie" może dotyczyć zarówno unieważnienia certyfikatu jak i uchylenia zawieszenia).

4.9.16 Ograniczenia okresu zawieszenia certyfikatu

Okres zawieszenia certyfikatu nie jest ograniczony.

4.10 Usługi weryfikacji statusu certyfikatu

4.10.1 Charakterystyki operacyjne

Informację o statusie certyfikatów wydanych w systemie PKI NBP można uzyskać w oparciu listy CRL publikowane w repozytorium (patrz rozdział 2.1) lub usługę OCSP dostępną pod adresem http://ocsp.nbp.pl/ocsp .

Informacja o unieważnieniu certyfikatu umieszczana jest na każdej liście opublikowanej w okresie ważności tego certyfikatu oraz na pierwszej liście po tym okresie.

4.10.2 Dostępność usługi

Usługi weryfikacji statusu certyfikatu są dostępne 24 godziny na dobę.

4.10.3 Cechy opcjonalne

Nie dotyczy.

4.11 Zakończenie subskrypcji

O zakończeniu korzystania z usług zaufania przez Subskrybenta można mówić w następujących przypadkach:

- gdy minął okres ważności certyfikatu Subskrybenta, zaś Subskrybent nie podjął działań mających na celu aktualizację klucza, lub modyfikację certyfikatu,
- unieważniono certyfikat Subskrybenta i nie został on zastąpiony przez inny certyfikat.

4.12 Deponowanie i odtwarzanie klucza

W systemie PKI NBP operacji deponowania (i odtwarzania) podlegać mogą jedynie klucze prywatne Subskrybentów wykorzystywane do szyfrowania. Klucze prywatne CCK i klucze prywatne Subskrybentów służące do składania podpisu elektronicznego lub uwierzytelniania nie są deponowane. Dodatkowe informacje zamieszczone są w odpowiednich Politykach Certyfikacji.

5. Zabezpieczenia techniczne, organizacyjne i operacyjne

W niniejszym rozdziale zawarto najważniejsze informacje dotyczące zabezpieczeń fizycznych, organizacyjnych oraz operacyjnych stosowanych w systemie PKI NBP m.in. podczas generowania kluczy kryptograficznych, uwierzytelniania subskrybentów, publikacji i unieważnianiu certyfikatów oraz w trakcie przeprowadzania audytu i wykonywania kopii zapasowych.

5.1 Zabezpieczenia fizyczne

5.1.1 Lokalizacja i budynki

Elementy systemu PKI NBP zlokalizowane są w dwóch ośrodkach będących własnością NBP i znajdujących się w znacznym oddaleniu od siebie.

5.1.2 Dostęp fizyczny

Pomieszczenia, w których zlokalizowany jest system PKI NBP objęte są systemem kontroli dostępu oraz są monitorowane 24 godziny na dobę. Dostęp do elementów systemu PKI NBP posiadają wyłącznie osoby uprawnione. Dopuszcza się pracę w systemie osób niebędących pracownikami NBP, w związku z realizacją zadań określonych w umowach zawartych przez NBP. Umowy te zawierają zapisy zapewniające właściwy poziom bezpieczeństwa wykonywanych prac serwisowych i konserwacyjnych, które są wykonywane wyłącznie pod nadzorem pracowników NBP mających dostęp do systemu PKI NBP.

5.1.3 Zasilanie oraz klimatyzacja

W celu zapobiegnięcia przerwy w działaniu systemu na skutek braku (lub zakłóceń w dopływie) energii elektrycznej, system PKI NBP posiada system zasilania awaryjnego wyposażony w generatory prądotwórcze. Odpowiednia temperatura oraz wilgotność powietrza w pomieszczeniach ośrodka podstawowego oraz zapasowego zapewnione są przez systemy klimatyzacji.

5.1.4 Zagrożenie powodziowe

Krytyczne elementy systemu PKI NBP znajdują się w pomieszczeniach o małym ryzyku zalania, w tym w wyniku uszkodzenia instalacji budynku. W przypadku wystąpienia zagrożenia zalaniem, postępuje się zgodnie z procedurami obowiązującymi w NBP.

5.1.5 Ochrona przeciwpożarowa

Pomieszczenia, w których znajdują się elementy systemu PKI NBP są chronione przez automatyczną instalację przeciwpożarową. W przypadku wystąpienia zagrożenia pożarowego postępuje się zgodnie z procedurami obowiązującymi w NBP.

5.1.6 Nośniki informacji

Szczególnej kontroli, w tym ograniczeniu ruchu pomiędzy strefami bezpieczeństwa w centrach komputerowych, podlegają wszelkie urządzenia umożliwiające utrwalenie lub przesłanie informacji. Dostęp do nośników informacji jest ograniczony, a nośniki przechowywane są w nadzorowanych pomieszczeniach. Dane wprowadzane do systemu z zewnętrznych elektronicznych nośników informacji są, przed ich wprowadzaniem do systemu, badane na obecność wirusów komputerowych lub innego złośliwego oprogramowania. Dla systemu opracowano procedury wykonywania kopii zapasowych krytycznych danych.

5.1.7 Niszczenie zbędnych nośników informacji

Zbędne dokumenty papierowe, dokumenty w formie elektronicznej oraz inne nośniki informacji używane w systemie PKI NBP są niszczone w bezpieczny sposób, zgodnie z obowiązującymi w NBP przepisami.

5.1.8 Przechowywanie kopii zapasowych i kopii archiwalnych

Kopie zapasowe oraz kopie archiwalne są przechowywane w różnych lokalizacjach. Ośrodek zapasowy, zapewniający możliwość pełnego odtworzenia funkcjonalności systemu z ośrodka podstawowego oraz przechowywanie kopii archiwalnych, jest dostępny dla osób upoważnionych w trybie: 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku. Ośrodek zapasowy jest chroniony przy zastosowaniu analogicznych środków jak ośrodek podstawowy.

5.2 Zabezpieczenia organizacyjne

5.2.1 Zaufane role

W systemie PKI NBP wyróżnia się następujące role:

- Administratorzy Systemu – odpowiedzialni za administrowanie systemem operacyjnym serwerów i stacji roboczych w systemie PKI NBP, za wykonywanie kopii zapasowych danych oraz za administrowanie sprzętem,
- Operatorzy CCK – odpowiedzialni za administrowanie urzędem certyfikacji,
- Administratorzy HSM – odpowiedzialni za administrowanie sprzętowymi modułami bezpieczeństwa,
- Operatorzy HSM – odpowiedzialni za obsługę sprzętowych modułów bezpieczeństwa,
- Operatorzy PRU – odpowiedzialni za rejestrację Subskrybentów oraz za generowanie, zawieszanie i unieważnianie certyfikatów,
- Agenci Odzyskiwania Danych – odpowiedzialni za odzyskiwanie danych zaszyfrowanych przez Subskrybenta w przypadku utraty jego klucza prywatnego,
- Agenci Odzyskiwania Kluczy – odpowiedzialni za odzyskiwanie utraconych kluczy prywatnych służących do szyfrowania poczty Subskrybentów,
- Audytorzy Systemu – odpowiedzialni za przeglądanie dzienników zdarzeń związanych z działalnością CCK,
- Inspektorzy Bezpieczeństwa Systemu – odpowiedzialni za nadzorowanie poziomu bezpieczeństwa systemu.

5.2.2 Lista osób wymaganych podczas realizacji zadania

Wszelkie czynności związane z obsługą i administrowaniem sprzętowymi modułami bezpieczeństwa wymagają obecności minimum dwóch osób posiadających odpowiednie karty elektroniczne.

5.2.3 Identyfikacja oraz uwierzytelnianie każdej roli

Identyfikacja i uwierzytelnianie Administratorów Systemu odbywa się z użyciem mechanizmu login/ hasło lub z użyciem kluczy kryptograficznych i certyfikatów. Pozostałe osoby funkcyjne w systemie PKI NBP są identyfikowane na podstawie certyfikatów, a do uwierzytelniania wykorzystują karty elektroniczne zabezpieczone kodem PIN.

5.2.4 Role, które nie mogą być łączone

Rola Administratora Systemu nie może być łączona z żadną inną. Rola Inspektora Bezpieczeństwa nie może być łączona z żadną inną. Rola Audytora Systemu nie może być łączona z żadną inną rolą.

5.3 Nadzorowanie personelu

5.3.1 Kwalifikacje, doświadczenie oraz upoważnienia

Osoby pełniące zaufane role w systemie PKI NBP są dobierane zgodnie z kwalifikacjami oraz zatrudniane na zasadach obowiązujących w NBP. Posiadają niezbędną wiedzę i umiejętności w zakresie świadczenia usług związanych z podpisem elektronicznym, sprzętu i oprogramowania stosowanego do elektronicznego przetwarzania danych, automatycznego przetwarzania danych w sieciach i systemach teleinformatycznych. Osoby te powoływane są odpowiednio przez dyrektora DIT, dyrektora DB lub dyrektora oddziału okręgowego NBP.

5.3.2 Procedury weryfikacji przygotowania

Zgodnie z zasadami zatrudniania pracowników w NBP.

5.3.3 Szkolenie

Zgodnie z zasadami szkolenia pracowników NBP, osoby pełniące zaufane role w systemie PKI NBP przechodzą szkolenia związane z obsługą tego systemu, a w szczególności:

- zapoznają się z Kodeksem, Politykami Certyfikacji oraz z dokumentacją i procedurami systemu,
- uczestniczą w szkoleniach z zakresu administrowania systemami operacyjnymi zainstalowanymi na serwerach i stacjach roboczych systemu PKI NBP; uczestniczą w szkoleniach dotyczących kryptografii oraz infrastruktury klucza publicznego.

5.3.4 Częstotliwość powtarzania szkoleń oraz wymagania

Zgodnie z zasadami szkoleń pracowników NBP.

5.3.5 Częstotliwość rotacji stanowisk i jej kolejność

Nie dotyczy.

5.3.6 Sankcje z tytułu nieuprawnionych działań

Wszystkie czynności wykonywane w systemie PKI NBP są dokumentowane i nadzorowane. Umożliwia to w szczególności wykrycie ewentualnych nieuprawnionych działań osób pełniących zaufane role w systemie PKI NBP .

Naruszanie zasad bezpieczeństwa, obowiązujących regulaminów i polityk zagrożone jest odpowiedzialnością dyscyplinarną lub karną określoną w przepisach odrębnych.

5.3.7 Pracownicy kontraktowi

Nie dotyczy, gdyż wszystkie osoby pełniące zaufane role w systemie PKI NBP są pracownikami NBP.

5.3.8 Dokumentacja przekazana pracownikom

Pracownicy pełniący zaufane role w systemie PKI NBP muszą mieć dostęp do następujących dokumentów:

- Kodeks,
- Polityki Certyfikacji,
- Dokumentacja systemu (w zakresie wymaganym dla danej roli),
- Procedury związane z pełnioną rolą,
- Zakres obowiązków i uprawnień wynikających z pełnionej roli.

5.4 Procedury rejestrowania zdarzeń oraz audytu

W systemie PKI NBP rejestrowane są wszystkie istotne zdarzenia, które mogą mieć wpływ na bezpieczeństwo i funkcjonowanie systemu operacyjnego, poszczególnych aplikacji systemu PKI NBP oraz systemów zabezpieczeń. Zarejestrowane zdarzenia są archiwizowane.

5.4.1 Typy rejestrowanych zdarzeń

W systemie PKI NBP rozróżniamy następujące typy zdarzeń:

- **Błąd**: Poważny problem, taki jak utrata danych lub funkcjonalności. Przykładem Błędu jest niepowodzenie ładowania usługi w trakcie autostartu,

- **Ostrzeżenie:** Zdarzenie, które samo w sobie nie ma dużej wagi, lecz może wskazywać na problem, który pojawi się w przyszłości. Przykładem Ostrzeżenia jest informacja, iż na dysku systemowym jest mało wolnego miejsca,
- **Informacja**: Zdarzenie informujące o prawidłowym funkcjonowaniu aplikacji, sterownika lub usługi. Przykładem zdarzenia typu Informacja jest prawidłowe załadowanie sterownika karty sieciowej.
- **Inspekcja sukcesów**: Dowolne objęte inspekcją zdarzenie zabezpieczeń, które zakończyło się pomyślnie. Przykładem zdarzenia typu Inspekcja sukcesów jest udana próba zalogowania użytkownika w systemie,
- **Inspekcja niepowodzeń**: Dowolne objęte inspekcją zdarzenie, które zakończyło się niepomyślnie. Przykładem zdarzenia typu Inspekcja niepowodzeń jest nieudana próba uzyskania dostępu do dysku sieciowego.

Dodatkowo, informacje nt. zdarzeń związane bezpośrednio z działalnością CCK takie, jak:

- generowanie certyfikatów Subskrybentów,
- unieważnianie\zawieszenie certyfikatów Subskrybentów,
- uruchomienie pracy CCK,
- zakończenie pracy CCK,

są przesyłane na skrzynki pocztowe Audytorów Systemu.

5.4.2 Częstotliwość przetwarzania zapisów rejestrowanych zdarzeń

Na serwerach PKI zainstalowane jest oprogramowanie monitorujące, które na bieżąco sprawdza stan systemu operacyjnego oraz usług związanych z pracą CCK i generuje raporty dla Administratorów Systemu. Administratorzy Systemu na bieżąco analizują otrzymywane raporty i w razie potrzeby przeglądają logi bezpośrednio na serwerze. Audytorzy Systemu codziennie przeglądają zdarzenia przesłane na ich skrzynki pocztowe. Szczegółowy przegląd zapisów rejestrowanych zdarzeń dokonywany jest w razie potrzeby (np. w przypadku wystąpienia incydentu).

5.4.3 Okres przechowywania zapisów rejestrowanych zdarzeń

Zapisy rejestrowanych zdarzeń przechowywane są przez okres co najmniej 1 miesiąca. Dodatkowo, są one archiwizowane, a kopie archiwalne przechowywane są przez okres 5 lat.

5.4.4 Ochrona zapisów rejestrowanych zdarzeń

Jedynie Administratorzy Systemu oraz Audytorzy Systemu posiadają dostęp do zapisów rejestrowanych zdarzeń.

5.4.5 Procedury tworzenia kopii zapisów rejestrowanych zdarzeń

Pełne kopie zapasowe wykonywane są raz w tygodniu, kopie przyrostowe wykonywane są we wszystkie dni robocze. Kopie zapasowe oraz kopie archiwalne przechowywane są w ośrodkach podstawowym i zapasowym.

5.4.6 System gromadzenia zapisów rejestrowanych zdarzeń (wewnętrzny a zewnętrzny)

Wewnętrzny rejestr zdarzeń przechowuje aktualne zdarzenia z okresu przynajmniej 1 miesiąca. Zewnętrzny system backup'owy codziennie wykonuje backup zdarzeń, a raz w miesiącu wykonywana jest kopia archiwalna. Pozwala to na uzyskanie szybkiego dostępu do zapisów zdarzeń z okresu 5 lat.

5.4.7 Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenie

Zewnętrzny system monitorujący powiadamia Administratorów Systemu o zaistniałych zdarzeniach. Administrator podejmuje dalsze kroki w celu wyjaśnienia zaistniałego zdarzenia i minimalizacji strat. Dodatkowo, informacje nt. zdarzeń związanych z działalnością CCK (wystawianie, unieważnianie i zawieszanie certyfikatów, uruchamienie lub zatrzymanie pracy CCK) są przesyłane na skrzynki mailowe Audytorów Systemu.

5.4.8 Oszacowanie podatności na zagrożenia

System PKI NBP okresowo poddawany jest wewnętrznemu audytowi bezpieczeństwa. Wszystkie wykryte nieprawidłowości są korygowane. Nad bezpieczeństwem systemu czuwa Inspektor Bezpieczeństwa Systemu.

5.5 Zapisy archiwalne

5.5.1 Rodzaje archiwizowanych danych

W systemie PKI NBP archiwizowane są bazy danych CCK, dzienniki zdarzeń a także dokumenty papierowe związane z pracą PRU a w szczególności z rejestracją i wydawaniem certyfikatów dla Subskrybentów tj.:

- „Zamówienie na usługę kryptograficzną",
- „Protokół przekazania kluczy kryptograficznych".

5.5.2 Okres przechowywania archiwum

Kopie archiwalne przechowywane są co najmniej przez okres 5 lat.

5.5.3 Ochrona archiwum

Kopie archiwalne przechowywane są w pomieszczeniach zabezpieczonych systemem kontroli dostępu w obu ośrodkach obliczeniowych.

5.5.4 Procedury tworzenia kopii archiwalnych

Kopie archiwalne wykonywane są raz w miesiącu.

5.5.5 Wymaganie znakowania czasem kopii archiwalnych

System PKI NBP zapewnia odnotowywanie czasu wystąpienia wszystkich zdarzeń. Dotyczy to zarówno zdarzeń rejestrowanych w dziennikach zdarzeń, jak i np. operacji wykonywania kopii zapasowych lub archiwalnych. System PKI NBP korzysta z zewnętrznego, bezpiecznego źródła czasu.

5.5.6 Kopie archiwalne rejestrów zdarzeń (system wewnętrzny i zewnętrzny)

Kopie archiwalne są wykonywane przez zewnętrzny system backupowy.

5.5.7 Procedury dostępu oraz weryfikacji zarchiwizowanej informacji

Dostęp do zarchiwizowanych danych mają tylko Administratorzy Systemu backup'owego. Okresowo wykonywane są testy odtworzenia wybranych zabezpieczonych danych.

5.6 Zmiana klucza

Zmiana kluczy urzędów certyfikacji wymaga opublikowania w repozytoriach nowego publicznego klucza oraz powiadomienia o tym fakcie subskrybentów oraz stron ufających. By zapewnić prawidłową pracę systemu PKI NBP nowa para kluczy urzędu NBP Enterprise CA jest generowana nie później niż 2 lata przed końcem okresu ważności aktualnie wykorzystywanego certyfikatu tego urzędu. Nie później niż 3 miesiące po wygaśnięciu certyfikatu danego urzędu, jego klucz prywatny jest niszczony.

5.7 Naruszenie ochrony klucza i uruchamianie po awariach oraz klęskach żywiołowych

5.7.1 Procedury obsługi incydentów i reagowania na nie

NBP posiada procedury obsługi incydentów włącznie z odtworzeniem całego systemu z kopii zapasowych. W przypadku podejrzenia wystąpienia incydentu powiadamiany jest Inspektor Bezpieczeństwa Systemu, który w porozumieniu z Administratorem Systemu podejmuje czynności zaradczo naprawcze zgodnie z procedurami. Czynności podejmowane przez Inspektora Bezpieczeństwa Systemu i Administratora Systemu mają pozwolić na identyfikację pierwotnej przyczyny powstałego incydentu, a także, o ile to możliwe, wykluczyć możliwość jego powtórzenie się.

5.7.2 Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych

Poszczególne elementy systemu PKI NBP umieszczone są na środowisku zapewniającym wysoką dostępność i rozmieszczone są w dwóch odległych od siebie ośrodkach obliczeniowych. W przypadku uszkodzenia jednej z maszyn, jej zadania automatycznie przejmują pozostałe maszyny. W przypadku uszkodzenia danych, są one odtwarzane z kopii zapasowych.

5.7.3 Ujawnienie lub podejrzenie ujawnienia klucza prywatnego podmiotu (CCK lub PRU)

W przypadku ujawnienia klucza prywatnego PRU natychmiast następuje jego unieważnienie i publikacja nowej listy CRL. Dodatkowo dokonywana jest analiza zapisów CCK w celu ustalenia czy ujawniony klucz prywatny PRU nie był wykorzystany w okresie pomiędzy momentem jego ujawnienia a unieważnieniem. W przypadku, gdy został on w tym okresie bezprawnie użyty do wystawienia certyfikatów – one także zostają unieważnione.

Ujawnienie klucza prywatnego CCK pociąga za sobą konieczność unieważnienia wszystkich certyfikatów podpisanych przez to CCK za pomocą ujawnionego klucza prywatnego oraz opublikowania nowej listy CRL. W następnej kolejności zostają wygenerowane nowe klucze kryptograficzne oraz nowy certyfikat CCK (identyfikator wyróżniający może, lecz nie musi, pozostać bez zmian) oraz przystępuje się do wymiany kluczy kryptograficznych i certyfikatów Subskrybentów. O fakcie ujawnienia klucza prywatnego CCK należy poinformować wszystkich Subskrybentów oraz strony ufające.

5.7.4 Zapewnienie ciągłości działania po katastrofach

W celu zabezpieczenia się przez skutkami działania katastrof, poszczególne elementy systemu PKI NBP umieszczone są na środowisku zapewniającym wysoką dostępność i rozmieszczone są w dwóch odległych od siebie ośrodkach obliczeniowych. W przypadku uszkodzenia jednego ośrodka, drugi przejmuje jego rolę. Dla systemu opracowany został plan ciągłości działania zawierający procedury awaryjne opisujące działania konieczne do podjęcia w celu zapewnienia ciągłości działania systemu (w szczególności jak najszybszego przywrócenia możliwości unieważniania certyfikatów).

5.8 Zakończenie działalności CCK lub PRU

5.8.1 CCK

Przed zakończeniem działalności CCK zobowiązany jest do:

- Powiadomienia o zamiarze zakończenia działalności (co najmniej na 90 dni wcześniej) wszystkich Subskrybentów, którzy posiadają jeszcze ważny certyfikat wydany przez to CCK oraz stron ufających korzystających z certyfikatów wydanych przez to CCK,
- Uczynienia wszystkiego co możliwe by zakończenie działalności spowodowało jak najmniejsze szkody dla subskrybentów oraz stron ufających.

W momencie zakończenia działalności CCK zobowiązany jest do :

- Unieważnienia wszystkich certyfikatów, które pozostały aktywne, niezależnie od tego czy Subskrybent złożył wniosek o unieważnienie czy nie,
- Powiadomienia wszystkich Subskrybentów, PRU oraz stron ufających o zakończeniu działalności.

Nie później niż 3 miesiące po zakończeniu pracy CCK zobowiązany jest do zniszczenia swoich kluczy prywatnych.

5.8.2 PRU

Najpóźniej na 90 dni przez planowanym zakończeniem działalności PRU ma obowiązek poinformowania o tym fakcie CCK. Niezwłocznie po zakończeniu działalności PRU ma obowiązek przekazania do CCK (lub do wskazanego przez CCK innego PRU) dokumentacji dotyczącej Subskrybentów.

6. Procedury bezpieczeństwa technicznego

6.1 Generowanie pary kluczy i jej instalowanie

6.1.1 Generowanie pary kluczy

Klucze kryptograficzne urzędów NBP Root CA oraz NBP Enterprise CA są generowane w sprzętowych modułach bezpieczeństwa posiadających certyfikat FIPS 140-2 level 3. Zasady dotyczące generowania kluczy kryptograficznych Subskrybentów przedstawione są w odpowiednich Politykach Certyfikacji.

6.1.2 Przekazywanie klucza prywatnego subskrybentowi

Zgodnie z odpowiednią Polityką Certyfikacji.

6.1.3 Dostarczanie klucza publicznego do wystawcy

Zgodnie z odpowiednią Polityką Certyfikacji.

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 do Subskrybenta, lub strony ufającej drogą mailową lub na nośniku.

6.1.5 Długości kluczy

Klucze kryptograficzne urzędu NBP Root CA mają długośc 4096 bitów a klucze kryptograficzne urzędu NBP Enterprise CA mają długość 2048 bitów. Długość kluczy kryptograficznych Subskrybentów określona jest w odpowiedniej Polityce Certyfikacji.

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)

Akceptowane zastosowanie kluczy Subskrybentów opisane jest w odpowiednich Politykach Certyfikacji. Klucze kryptograficzne urzędów NBP Root CA oraz NBP Enterprise CA mogą być używane jedynie do:

- Podpisywania certyfikatu,
- Podpisywania listy CRL,
- Podpisywania listy CRL w trybie off-line.

6.2 Ochrona klucza prywatnego oraz nadzorowanie mechanizmów modułu kryptograficznego

6.2.1 Standardy modułów kryptograficznych

Urzędy NBP Root CA oraz NBP Enterprise CA wykorzystują oddzielne sprzętowe moduły bezpieczeństwa posiadające certyfikat FIPS 140-2 level 3. Wszystkie operacje związane z zarządzaniem modułami bezpieczeństwa w tym operacje związane z kluczami kryptograficznymi zapisanymi na nich wymagają użycia kart elektronicznych przypisanych Administratorom HSM lub Operatorom HSM.

6.2.2 Podział klucza prywatnego na części

Klucze prywatne urzędów NBP Root CA oraz NBP Enterprise CA, i tylko one, podlegają ochronie za pomocą tzw. schematu pośredniego podziału klucza na części. W schemacie tym podziałowi podlega klucz symetryczny użyty do zaszyfrowania klucza prywatnego urzędu. Klucz symetryczny podzielony jest na 9 części zapisanych na kartach elektronicznych zabezpieczonych kodem PIN i przekazanych Operatorom HSM. Do odtworzenia klucza konieczne jest użycie przynajmniej dwóch takich kart i możliwe jest to jedynie wewnątrz urządzenia HSM.

6.2.3 Deponowanie klucza prywatnego

Patrz rozdział 4.12.

6.2.4 Kopie zapasowe klucza prywatnego

Kopie kluczy prywatnych CCK są tworzone za pomocą mechanizmów wbudowanych w sprzętowe moduły bezpieczeństwa wykorzystywane w systemie PKI NBP i są chronione w sposób analogiczny jak klucze prywatne zabezpieczone modułami kryptograficznymi.

6.2.5 Archiwizowanie klucza prywatnego

Klucze prywatne CCK nie są archiwizowane. Zasady archiwizowania kluczy prywatnych Subskrybentów określone są w odpowiednich Politykach Certyfikacji.

6.2.6 Wprowadzenie lub pobieranie klucza prywatnego do/z modułu kryptograficznego

Poza modułem kryptograficznym klucze prywatne urzędów NBP Root CA oraz NBP Enterprise CA występują jedynie w postaci zaszyfrowanej a ich odszyfrowanie wymaga użycia dwóch kart Operatorów CCK i możliwe jest jedynie wewnątrz modułu kryptograficznego. Wprowadzenie klucza prywatnego CCK polega na wczytaniu jego zaszyfrowanej wersji do modułu kryptograficznego, odtworzenia (z kart Operatorów CCK) klucza symetrycznego, którym klucz prywatny został zaszyfrowany i odszyfrowania klucza prywatnego. Pobranie klucza prywatnego z modułu kryptograficznego również wymaga użycia dwóch kart Operatorów CCK i polega na wyeksportowaniu zaszyfrowanej postaci klucza prywatnego CCK do pliku.

6.2.7 Przechowywanie klucza prywatnego w module kryptograficznym

Klucze prywatne urzędów NBP Root CA oraz NBP Enterprise CA są generowane bezpośrednio w sprzętowym module bezpieczeństwa i w postaci niezaszyfrowanej występują jedynie w tym urządzeniu. W przypadku pobierania klucza prywatnego CCK z modułu kryptograficznego jest on szyfrowany a jego odszyfrowanie wymaga użycia dwóch kart Operatorów CKK i możliwe jest jedynie w module kryptograficznym.

6.2.8 Metoda aktywacji klucza prywatnego

Aktywacja klucza prywatnego CCK polega na jego wczytaniu do modułu kryptograficznego a następnie odszyfrowaniu wewnątrz tego modułu. Operacja ta wymaga udziału przynajmniej dwóch Operatorów HSM posiadających karty elektroniczne z częściami klucza deszyfrującego. Odszyfrowany klucz prywatny CCK jest aktywny do czasu zatrzymania pracy urzędu (np. restart lub wyłączenie serwera, zatrzymanie usługi).

6.2.9 Metoda dezaktywacji klucza prywatnego

Dezaktywacja klucza prywatnego urzędu NBP Enterprise CA jest możliwa poprzez zatrzymanie pracy urzędu (np. restart lub wyłączenie serwera, zatrzymanie usługi). Może jej dokonać jedynie Administrator Systemu lub Operator CCK.

6.2.10 Metoda niszczenia klucza prywatnego

Niszczenie klucza prywatnego CCK polega na jego bezpiecznym usunięciu z modułu kryptograficznego. Może to być wykonane poprzez oprogramowanie dołączone do tego modułu lub poprzez „przycisk samobójcy" znajdujący się na przednim panelu modułu. „Przycisk samobójcy" służy do natychmiastowego wyczyszczenia pamięci modułu i jest używany w przypadku bezpośredniego zagrożenia bezpieczeństwa klucza prywatnego CCK .

Zgodnie z procedurami klucze kryptograficzne CCK są niszczone nie później niż 3 miesiące po wygaśnięciu związanego z nimi certyfikatu (lub po jego unieważnieniu). Dodatkowo, wszystkie dane zapisane w pamięci modułu kryptograficznego są z niego usuwane w przypadku przewożenia tego modułu, jego przekazywaniu firmie zewnętrznej (np. w związku z koniecznością przeprowadzenia prac serwisowych) lub w przypadku wycofywania modułu z użycia.

6.2.11 Ocena modułu kryptograficznego

Patrz pkt. 6.2.1.

6.3 Inne aspekty zarządzania kluczami

6.3.1 Archiwizowanie kluczy publicznych

Klucze publiczne są archiwizowane (w postaci certyfikatów), a kopie archiwalne są przechowywane przez okres przynajmniej 5 lat.

6.3.2 Okresy stosowania klucza publicznego i prywatnego

Okres życia klucza publicznego określony jest przez pole „validity" każdego certyfikatu klucza publicznego (patrz 7.1). Okres ważności klucza prywatnego jest identyczny jak w przypadku klucza publicznego.

Okresy stosowania kluczy CCK przedstawione są w poniższej tabeli:

Okresy stosowania kluczy CCK

Nazwa CCK	Typ klucza	Okres stosowania[2]
NBP Root CA	Publiczny/prywatny	15 lat / 25 lat
NBP Enterprise CA	Publiczny/prywatny	5 lat / 7 lat/ 10 lat

Okresy stosowania kluczy Subsrybentów przedstawione są w Politykach Certyfikacji.

6.4 Dane aktywujące

Dane aktywujące stosowane są do uaktywniania kluczy prywatnych stosowanych przez CCK, PRU oraz Subskrybentów. Najczęściej używane są na etapie uwierzytelnienia podmiotu i kontroli dostępu do klucza prywatnego. W systemie PKI NBP można wyróżnić dwa rodzaje danych aktywujących:

- Hasła i kody PIN zabezpieczające klucze prywatne Subskrybentów,
- Karty elektroniczne z częściami sekretu współdzielonego, który po zainstalowaniu w systemie umożliwia odtworzenie klucza prywatnego CCK.

6.4.1 Generowanie danych aktywujących i ich instalowanie

Dane aktywujące klucz prywatny Subskrybenta (hasło lub PIN) 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.

Sekrety współdzielone używane do ochrony kluczy prywatnych CCK generowane są zgodnie z wymaganiami określonymi w rozdz. 6.2 i zapisywane są na kartach elektronicznych przydzielonych Operatorom HSM. Karty elektroniczne chronione są kodem PIN.

6.4.2 Ochrona danych aktywujących

Dane aktywujące w postaci haseł lub kodów PIN powinny być danymi pamiętanymi (nie zapisywanymi) przez Subskrybenta. Jeżeli zachodzi potrzeba ich zapisania, to nośnik z tą informacją nie powinien być

[2] Pierwsza wartość dotyczy kluczy wygenerowanych przed 2 czerwca 2014 roku, a druga wartość dotyczy kluczy wygenerowanych od dnia 2 czerwca 2014 roku. W przypadku NBP Enterprise CA trzecia wartość dotyczy kluczy wygenerowanych w 2016 r.

przechowywany razem z kluczem prywatnym, którego dotyczy. Karty elektroniczne wykorzystywane w systemie PKI NBP ulegają zablokowaniu po 5-krotnym błędnym wpisaniu kodu PIN. Odblokowanie karty musi być wykonane za pośrednictwem PRU.

Karty elektroniczne z elementami sekretu współdzielonego przechowywane są przez Operatorów HSM w pomieszczeniach zabezpieczonych systemem kontroli dostępu. Kody PIN chroniące te karty nie są przechowywane razem z kartami. Dodatkowo, aktywacja klucza prywatnego CCK wymaga użycia co najmniej dwóch kart Operatorów HSM i do jej przeprowadzenia konieczny jest odpowiednio skonfigurowany moduł kryptograficzny.

6.4.3 Inne problemy związane z danymi aktywującymi

Nie dotyczy.

6.5 Nadzorowanie bezpieczeństwa systemu komputerowego

Informacje związane z nadzorowaniem bezpieczeństwa systemów komputerowych w NBP objęte są tajemnicą i mogą być udostępniane jedynie osobom upoważnionym. Wszystkie elementy systemu PKI NBP chronione są zgodnie z wewnętrznymi regulacjami NBP, w tym zgodnie z zapisami polityki bezpieczeństwa w NBP. W szczególności wszystkie elementy systemu PKI NBP objęte są ochroną antywirusową.

6.5.1 Wymagania techniczne dotyczące specyficznych zabezpieczeń systemów komputerowych

Informacje związane z wymaganiami technicznymi dotyczącymi specyficznych zabezpieczeń systemów komputerowych w NBP objęte są tajemnicą i mogą być udostępniane jedynie osobom upoważnionym.

6.5.2 Ocena bezpieczeństwa systemów komputerowych

Informacje związane z oceną bezpieczeństwa systemów komputerowych w NBP objęte są tajemnicą i mogą być udostępniane jedynie osobom upoważnionym.

6.6 Cykl życia zabezpieczeń technicznych

Informacje związane z cyklem życia zabezpieczeń technicznych w NBP objęte są tajemnicą i mogą być udostępniane jedynie osobom upoważnionym.

6.6.1 Nadzorowanie rozwoju systemu

System PKI NBP jest na bieżąco monitorowany przez Inspektora Bezpieczeństwa Systemu. Przed wprowadzeniem jakichkolwiek zmian w tym systemie, są one konsultowane z IBS, a także przeprowadzane są testy (w tym testy bezpieczeństwa). Po wprowadzeniu zmian aktualizowana jest dokumentacja systemu.

6.6.2 Nadzorowanie zarządzania bezpieczeństwem

Zgodnie z wewnętrznymi regulacjami NBP.

6.6.3 Nadzorowanie cyklu życia zabezpieczeń

Niniejszy Kodeks nie określa żadnych wymagań w tym zakresie.

6.7 Nadzorowanie zabezpieczeń sieci komputerowej

Informacje związane z nadzorowaniem zabezpieczeń sieci komputerowej w NBP objęte są tajemnicą i mogą być udostępniane jedynie osobom upoważnionym.

6.8 Znakowanie czasem

Nie dotyczy.

7. Profile certyfikatów oraz list CRL

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

7.1 Profil certyfikatu

Certyfikat według normy X.509 v.3 jest sekwencją trzech pól, z których pierwsze zawiera treść certyfikatu (tbsCertificate), drugie – informację o typie algorytmu użytego do podpisania certyfikatu (signatureAlgorithm), zaś trzecie – podpis cyfrowy, składany na certyfikacie przez CCK (signatureValue). Na treść certyfikatu składają się wartości pól podstawowych oraz rozszerzeń (standardowych, określonych przez normę oraz prywatnych, definiowanych przez urząd certyfikacji).

Certyfikaty w systemie PKI NBP zawierają następujące pola podstawowe:

- Wersja: wersję trzecią (X.509 v3) formatu certyfikatu,
- Numer Seryjny: numer seryjny certyfikatu,
- Algorytm Podpisu : identyfikator algorytmu stosowanego przez CCK ,
- Wystawca: identyfikator wyróżniający CCK ,
- Okres ważności: data ważności certyfikatu określona przez początek (Ważny od) oraz koniec ważności (Ważny do),
- Podmiot: identyfikator wyróżniający subskrybenta,
- Klucz publiczny: wartość klucza publicznego wraz z identyfikatorem algorytmu,
- Podpis: podpis generowany i kodowany zgodnie z RFC 5280.

Zawartość pól podstawowych w certyfikatach wydanych w systemie PKI NBP

Nazwa Pola	Zawartość Pola	
Wersja	V3	
Numer Seryjny	Unikalny w ramach CCK numer seryjny certyfikatu	
Algorytm Podpisu	SHA1RSA[3]/Sha256RSA[4]	
Wystawca	Nazwa powszechna (CN)	NBP Root CA / NBP Enterprise CA
	Jednostka Organizacyjna (OU)	Centrum Certyfikacji Kluczy NBP
	Organizacja (O)	Narodowy Bank Polski
	Miejscowość (L)	Warszawa
	Kraj (C)	PL

[3] Dla certyfikatów wystawionych przed 10.10.2016
[4] Dla certyfikatów wystawionych po 10.10.2016

Ważny od	Podstawowy czas według UTC (Universal Time Coordinated)
Ważny do	Podstawowy czas według UTC (Universal Time Coordinated)
Podmiot	Identyfikator wyróżniający Subskrybenta zgodny z wymaganiami X.501. Dokładniejsze informacje dotyczące zawartości tego pola znajdują się w Politykach Certyfikacji
Klucz publiczny	Pole kodowane zgodnie z RFC 5280 i zawiera informacje o kluczu publicznym RSA (identyfikator klucza, jego długość i wartość)
Podpis	Podpis certyfikatu generowany i kodowany zgodnie z wymaganiami RFC 5280

7.1.1 Numer wersji

Wszystkie certyfikaty wydawane w systemie PKI NBP są zgodne z X.509 v3.

7.1.2 Rozszerzenia certyfikatów

Rozszerzenie znajdujące się w certyfikacie może być krytyczne, lub niekrytyczne. Jeśli rozszerzenie oznaczone jest jako krytyczne, to aplikacja bazująca na certyfikatach musi odrzucić każdy certyfikat, w którym nie jest w stanie rozpoznać tego rozszerzenia. Z kolei każde niekrytyczne rozszerzenie może być ignorowane. Certyfikaty wystawiane w systemie PKI NBP zawierają następujące rozszerzenia:

- Użycie klucza,
- Użycie klucza rozszerzonego,
- Identyfikator klucza podmiotu,
- Identyfikator klucza urzędu,
- Informacje o szablonie certyfikatu (ew. „Szablon certyfikatu”),
- Punkty dystrybucji list CRL,
- Dostęp do informacji o urzędach ,
- Zasady aplikacji,
- Alternatywna nazwa podmiotu,
- Możliwości edytora SMIME (tylko certyfikaty związane z szyfrowaniem),
- Podstawowe warunki ograniczające (tylko wybrane certyfikaty).

W zależności od szablonu certyfikatu rozszerzenia mogą być krytyczne. Szczegółowe informacje w odpowiedniej Polityce Certyfikacji.

7.1.3 Identyfikatory algorytmów

To pole zawiera identyfikator algorytmu kryptograficznego, opisującego algorytm stosowany do realizacji podpisu cyfrowego, składanego przez urząd certyfikacji na certyfikacie. W certyfikatach wydanych w systemie PKI NBP wartość tego pola to :

Dla certyfikatów wystawionych przed 10.10.2016

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

Dla certyfikatów wystawionych po 10.10.2016

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

7.1.4 Format nazw

Zgodnie z odpowiednią Polityką Certyfikacji.

7.1.5 Ograniczenia nakładane na nazwy

Zgodnie z odpowiednią Polityką Certyfikacji.

7.1.6 Identyfikatory polityk certyfikacji

Zgodnie z określoną Polityką Certyfikacji. Polityki certyfikacji w systemie PKI NBP posiadają identyfikatory zaczynające się od 1.3.6.1.4.1.31995.1.

7.1.7 Stosowanie rozszerzenia określającego ograniczenia nakładane na politykę

Nie dotyczy.

7.1.8 Składnia i semantyka kwalifikatorów polityki

Rozszerzenie „Zasady aplikacji" zawarte w certyfikacie zawiera adres URL wskazujący Kodeks oraz Politykę Certyfikacji związaną z danym certyfikatem.

7.1.9 Przetwarzanie semantyki krytycznych rozszerzeń polityki certyfikacji

By zapewnić maksymalną kompatybilność rozszerzenie „Zasady aplikacji" jest rozszerzeniem niekrytycznym.

7.2 Profil listy unieważnionych certyfikatów (CRL)

Lista certyfikatów unieważnionych (CRL) składa się z ciągu trzech pól. Pierwsze pole (tbsCertList) zawiera informacje o unieważnionych certyfikatach, drugie pole (signatureAlgorithm) informację o typie algorytmu

użytego do podpisania listy, a pole trzecie (signatureValue) - podpis cyfrowy, składany na liście CRL przez CCK.

Pole informacyjne tbsCertList jest sekwencją pól obowiązkowych i opcjonalnych. Pola obowiązkowe identyfikują wydawcę listy CRL, zaś opcjonalne zawierają unieważnione certyfikaty oraz rozszerzenia listy CRL. Opis podstawowych pól i rozszerzeń listy CRL znajduje się w poniższej tabeli:

Podstawowe pola i rozszerzenia listy CRL

Nazwa Pola	Zawartość Pola	
Wersja	V2	
Wystawca	Nazwa powszechna (CN)	NBP Root CA / NBP Enterprise CA
	Jednostka Organizacyjna (OU)	Centrum Certyfikacji Kluczy NBP
	Organizacja (O)	Narodowy Bank Polski
	Miejscowość (L)	Warszawa
	Kraj (C)	PL
Data wprowadzenia	Podstawowy czas według UTC (Universal Time Coordinated)	
Następna aktualizacja	Podstawowy czas według UTC (Universal Time Coordinated)	
Lista odwołania	Numer seryjny	Unikalny w ramach CCK numer seryjny certyfikatu
	Data odwołania	Podstawowy czas według UTC (Universal Coordinate Time)
	Kod przyczyny listy CRL – pole opcjonalne	Dodatkowe informacje o przyczynie unieważnienia (*)
Algorytm podpisu	Sha256RSA	
Identyfikator klucza urzędu	Pole kodowane zgodnie z RFC 5280 i zawierające identyfikator klucza RSA służącego do weryfikacji podpisu złożonego pod listą	
Wersja urzędu certyfikacji	Pole numeryczne. Jego wartość jest zwiększana za każdym razem gdy następuje zmiana klucza prywatnego CCK będącego wystawcą listy.	
Numer listy CRL	Kolejny numer listy CRL	
Publikowanie następnej listy CRL	Podstawowy czas według UTC (Universal Coordinate Time)	

Podpis	Podpis generowany i kodowany zgodnie z wymaganiami RFC 5280

(*) – W polu „Kod przyczyny listy CRL" mogą występować następujące wpisy:

- Złamanie klucza (1),
- Złamanie klucza urzędu (2),
- Zmiana przynależności (3),
- Zastąpienie nowszą wersją (4),
- Zaprzestanie działania (5),
- Wstrzymanie certyfikatu (6).

8. Audyt zgodności i inne oceny

8.1 Częstotliwość i okoliczności oceny

System PKI NBP jest objęty okresowym audytem wewnętrznym lub zewnętrznym, nie rzadziej niż raz na 3 lata. Dodatkowo, z częstotliwością określoną w przpisach odrębnych, Inspektor Bezpieczeństwa Systemu przeprowadza Analizę Ryzyka systemu PKI NBP. Celem przeprowadzenia Analizy Ryzyka jest ocena poziomu ryzyka bezpieczeństwa systemu. Analizę Ryzyka przeprowadza się zgodnie z obowiązującą w NBP metodyką.

8.2 Tożsamość i kwalifikacje audytora

Audytorzy wykonujący zadanie audytowe powinni posiadać wiedzę i kwalifikacje z zakresu infrastruktury klucza publicznego.

8.3 Związek audytora z audytowaną jednostką

Audytor z Departamentu Audytu Wewnętrznego jest pracownikiem NBP i audytuje system zarządzany w innym departamencie. Audytor zewnętrzny nie jest w żaden sposób związany z systemem PKI NBP.

8.4 Zagadnienia objęte audytem

Cel i zakres zadania audytowego są określane zgodnie z przepisami obowiązującymi w NBP i mogą obejmować w szczególności: funkcjonowanie systemu, zgodność świadczenia usług z kodeksem postępowania certyfikacyjnego i politykami certyfikacji oraz zgodność działań z obowiązującymi przepisami.

8.5 Działania podejmowane w celu usunięcia usterek wykrytych podczas audytu

Zgodnie z przepisami obowiązującymi w NBP.

8.6 Informowanie o wynikach audytu

Zgodnie z przepisami obowiązującymi w NBP.

9. Inne kwestie biznesowe i prawne

9.1 Opłaty

NBP nie pobiera opłat za wydanie kluczy kryptograficznych czy certyfikatów, za dostęp do repozytorium znajdującego się na stronach www.pki.nbp.pl/pki ani za korzystanie z usługi OCSP.

9.2 Odpowiedzialność finansowa

Świadczenie przez NBP usług zaufania w systemie PKI NBP nie wymaga zawarcia przez NBP umowy ubezpieczenia od odpowiedzialności cywilnej za szkody wyrządzone odbiorcom usług zaufania powstałe w okresie świadczenia usług zaufania, chyba że strony postanowią inaczej lub taki obowiązek wynikać będzie z przepisów powszechnie obowiązujących..

9.3 Poufność informacji biznesowej

NBP gwarantuje, że wszystkie informacje zbierane na potrzeby systemu PKI NBP są przechowywane i przetwarzane zgodnie z obowiązującymi w tym zakresie przepisami prawa.

Ochronie podlegają też informacje zastrzeżone jako tajemnica przedsiębiorstwa podmiotów, z którymi NBP zawarło umowę w ramach systemu PKI NBP.

9.3.1 Zakres poufności informacji

Wszystkie informacje związane ze świadczeniem przez NBP usług zaufania w systemie PKI NBP i nie oznaczone jako publiczne są traktowane jako tajemnica przedsiębiorstwa. Informacje związane bezpośrednio z działalnością CCK i PRU takie jak: klucze prywatne, dokumentacja techniczna oraz procedury systemowe i awaryjne podlegają ochronie zgodnie z ustawą o usługach zaufania.

9.3.2 Informacje znajdujące się poza zakresem poufności informacji

Do informacji związanych ze świadczeniem przez NBP usług zaufania w systemie PKI NBP można zaliczyć:

- Kodeks,
- Polityki Certyfikacji,
- Certyfikaty CCK,
- Dane teleadresowe PRU oraz CCK,
- Listy CRL publikowane w repozytorium.

9.3.3 Obowiązek ochrony poufności informacji

Wszyscy pracownicy NBP wykonujący zadania związane ze świadczeniem usług certyfikacyjnych są zobowiązani do zachowania poufności informacji opisanych w rozdziale 9.3.1. Obowiązek ochrony

poufności informacji przez pracowników firm zewnętrznych wykonujących zadania na rzecz NBP jest regulowany w umowach zawartych przez NBP z tymi firmami.

9.4 Zobowiązania i gwarancje

W tym rozdziale przedstawiono wszystkie zobowiązania nałożone na strony niniejszego Kodeksu tj. na CCK, PRU, Subskrybentów oraz strony ufające.

9.4.1 Zobowiązania CCK

W ramach świadczenia swoich usług w systemie PKI NBP Operator CCK ma obowiązek:

- Przestrzegać zapisów niniejszego Kodeksu oraz Polityk Certyfikacji,
- Chronić klucze prywatne CCK i zapewnić bezpieczeństwo procesu generowania kluczy kryptograficznych subskrybentów,
- Generować i zarządzać certyfikatami zgodnie ze standardem x.509 v3,
- Publikować, bez zbędnej zwłoki, wygenerowane certyfikaty CCK w repozytorium opisanym w rozdziale 2.1,
- Unieważniać certyfikaty zgodnie z zapisami rozdziału 4.9,
- Publikować, bez zbędnej zwłoki, listy CRL w repozytorium opisanym w rozdziale 2.1,
- Zapewnić dostępność najbardziej aktualnych list CRL, certyfikatów CCK Kodeksu Postępowania Certyfikacyjnego oraz Polityk Certyfikacji w repozytorium opisanym w rozdziale 2.1,
- Świadczyć usługi certyfikacyjne zgodnie z obowiązującym prawem oraz zgodnie z zatwierdzonymi procedurami systemu PKI NBP,
- Zapewnić by wszystkie czynności związane ze świadczeniem usług zaufania w systemie PKI NBP wykonywane były tylko przez osoby do tego upoważnione,
- Przechowywać i archiwizować dokumenty i dane w postaci elektronicznej bezpośrednio związane ze świadczeniem usług zaufania, w sposób zapewniający bezpieczeństwo tych danych i dokumentów.

9.4.2 Zobowiązania PRU

W ramach świadczenia swoich usług w systemie PKI NBP Operator PRU ma obowiązek:

- Przestrzegać zapisów niniejszego Kodeksu oraz Polityk Certyfikacji,
- Zapewnić by wnioski kierowane do CCK zawierały prawdziwe dane Subskrybenta i były wolne od błędów,
- Na bieżąco informować CCK o zauważonych problemach w systemie PKI NBP,
- Przechowywać i archiwizować dokumenty i dane w postaci elektronicznej bezpośrednio związane ze świadczeniem usług zaufania, w sposób zapewniający bezpieczeństwo tych danych i dokumentów,
- Dokonywać weryfikacji subskrybenta zgodnie z zapisami Polityki Certyfikacji oraz procedur systemu PKI NBP,
- Współpracować z Subskrybentem w procesie generowania kluczy kryptograficznymi tylko w przypadku poprawnego zweryfikowania Subskrybenta.

9.4.3 Zobowiązania subskrybenta

Subskrybent ma obowiązek:

- Dostarczyć wszystkie dane wymagane do wystawienia certyfikatu w systemie PKI NBP i zapewnić ich prawdziwość,
- Niezwłocznie informować PRU o wszelkich zmianach danych opisanych wyżej,
- Przestrzegać zapisów niniejszego Kodeksu oraz odpowiednich Polityk Certyfikacji,
- Zapewnić należytą ochronę klucza swojego klucza prywatnego oraz danych służących do jego aktywacji,
- Wykorzystywać klucze kryptograficzne i certyfikaty systemu PKI NBP tylko w zakresie określonym w certyfikacie (pola KeyUsage i ExtKeyUsage),
- Natychmiast żądać unieważnienia swojego certyfikatu w przypadku kompromitacji odpowiadającego mu klucza prywatnego.

9.4.4 Zobowiązania strony ufającej

Strona ufająca wykorzystująca certyfikaty systemu PKI NBP, ma obowiązek:

- Ufać certyfikatom tylko w zakresie opisanym w certyfikacie (pola KeyUsage i ExtKeyUsage),
- Dokonywać pełnej weryfikacji certyfikatu Subskrybenta przed jego wykorzystaniem,
- Informować PRU lub CCK o każdym użyciu certyfikatu przez osobę nieupoważnioną lub w sposób niezgodny z przeznaczeniem certyfikatu.

9.5 Wyłączenia odpowiedzialności z tytułu gwarancji

Wydanie certyfikatu w systemie PKI NBP nie czyni z Narodowego Banku Polskiego agenta, powiernika czy reprezentanta Subskrybenta, któremu wydany został certyfikat.

9.6 Ograniczenia odpowiedzialności

Narodowy Bank Polski nie ponosi odpowiedzialności za dokonanie przez Stronę ufającą poprawnej i rzetelnej weryfikacji każdego podpisu i /lub certyfikatu któremu zamierza zaufać. Zaufanie niekompletnie lub negatywnie zweryfikowanemu podpisowi lub certyfikatowi następuje na wyłączną odpowiedzialność Strony ufającej.

Narodowy Bank Polski nie ponosi odpowiedzialności za użycie przez Subskrybenta kluczy kryptograficznych i certyfikatów niezgodnie z ich przeznaczeniem określonym w niniejszym Kodeksie oraz w odpowiednich Politykach Certyfikacji.

Narodowy Bank Polski, jako właściciel systemu PKI NBP nie ponosi odpowiedzialności za zawartość dokumentów (lub innych danych) podpisanych lub zaszyfrowanych przy użyciu kluczy kryptograficznych i certyfikatów wygenerowanych w tym systemie.

10. Ochrona danych osobowych

Dane osobowe w systemie PKI NBP przetwarzane są zarówno w postaci papierowej, jak i elektronicznej i są chronione zgodnie z obowiązującymi przepisami prawa. Dane osobowe, wchodzące w skład identyfikatora wyróżniającego subskrybenta, pobierane są z usługi katalogowej Active Directory lub wprowadzane są do systemu ręcznie przez operatora punktu rejestracji użytkowników, na podstawie dostarczonego „Zamówienia na usługę kryptograficzną".

W systemie PKI NBP w dokumentacji w formie papierowej przetwarza się następujące dane osobowe subskrybenta:

- imię i nazwisko;
- seria i numer dokumentu tożsamości;
- miejsce zatrudnienia;
- adres e-mail;
- numer telefonu służbowego;
- podpis.

Dokumenty w formie papierowej i elektronicznej, zawierające dane osobowe związane z systemem PKI NBP, podlegają zabezpieczeniom zapobiegającym nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu zgodnie z przepisami prawa. Dane osobowe dotyczące PKI NBP są przechowywane przez okres ważności certyfikatu i przez lat 5 (w przypadku certyfikatów do podpisu elektronicznego lub uwierzytelniania) lub 10 lat (w przypadku certyfikatów do szyfrowania) po wygaśnięciu certyfikatu osoby, której dane dotyczą. Po tym okresie certyfikaty są usuwane z systemu PKI NBP, a kopie archiwalne zawierające te certyfikaty są niszczone.

Załącznik A – Autocertyfikaty CCK

Autocertyfikat NBP Root CA	
Data wystawienia	20 listopada 2008 roku
Data wygaśnięcia	20 listopada 2018 roku
Identyfikator klucza podmiotu	8b c9 e4 49 27 49 69 01 6e f0 38 3a 24 99 18 9d 3f e9 d8 81
Certyfikat w formacie base64	-----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/ MqEEXrzbyqPOqPAqdnCR3Qlkwc/V+mduHH1Iw9ffd538WYMXoqZEm0HprSz sd0ZyW1I8wP8cKnAl4b3GqmvdKmno8coXpSJIQdA== -----END CERTIFICATE-----

Autocertyfikat NBP Root CA	
Data wystawienia	2 czerwca 2014 roku
Data wygaśnięcia	2 czerwca 2034 roku
Identyfikator klucza podmiotu	7a 84 99 54 a5 27 11 4b 19 51 d5 a6 09 c2 e0 b4 0f 7e dc 7f
Certyfikat w formacie base64	-----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-----

Autocertyfikat NBP Root CA	
Data wystawienia	2 czerwca 2014 roku
Data wygaśnięcia	16 września 2036 roku
Identyfikator klucza podmiotu	7a 84 99 54 a5 27 11 4b 19 51 d5 a6 09 c2 e0 b4 0f 7e dc 7f
Certyfikat w formacie base64	-----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-----

Certyfikat NBP Enterprise CA	
Data wystawienia	2 czerwca 2014 roku
Data wygaśnięcia	2 czerwca 2021 roku
Identyfikator klucza podmiotu	d4 36 f2 2d d0 46 2c 20 33 13 84 6d 15 d7 4e 95 21 0b 0f 11
Certyfikat w formacie base64	-----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-----

Certyfikat NBP Enterprise CA	
Data wystawienia	10 października 2016 roku
Data wygaśnięcia	10 października 2026 roku
Identyfikator klucza podmiotu	d4 36 f2 2d d0 46 2c 20 33 13 84 6d 15 d7 4e 95 21 0b 0f 11
Certyfikat w formacie base64	-----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-----

Załącznik B – Historia zmian dokumentu

Lp.	Data	Wersja	Osoba	Opis wykonanych prac
1.	02.09.2011	0.1		Utworzenie dokumentu
2.	20.09.2011	0.2		Dodanie zapisów rozdziałów 2, 5.4, 5.5, 5.6, 5.7
3.	13.10.2011	0.3		Przegląd dokumentu
4.	04.11.2011	0.4		Dodanie zapisów rozdziałów 4.9.3, 4.9.15, 6.3.2, 6.4
5.	11.05.2012	0.5		Dodanie zapisów rozdziałów 8, 9, 10
6.	24.05.2012	0.6		Przegląd i korekta dokumentu
7.	22.08.2012	0.7		Przegląd i uzupełnienie dokumentu
8.	10.09.2012	0.8		Przegląd dokumentu
9.	12.09.2012	0.9		Przegląd dokumentu
10.	**18.09.2012**	**1.0**		**Zatwierdzenie dokumentu**
11.	11.10.2012	1.01		Uzupełnienie dokumentu – uwagi DAW
12.	29.10.2012	1.02		Przegląd i uzupełnienie dokumentu
13.	30.10.2012	1.03		Przegląd dokumentu
14.	30.10.2012	1.04		Przegląd dokumentu
15.	05.11 2012	1.05		Przegląd dokumentu
16.	**08.11.2012**	**1.1**		**Zatwierdzenie dokumentu**
17.	23.01.2013	1.11		Uzupełnienie dokumentu – uwagi audytorów ESBC
18.	31.01.2013	1.12		Przegląd dokumentu
19.	31.01.2013	1.13		Przegląd dokumentu
20.	31.01.2013	1.14		Przegląd dokumentu
21.	**19.02.2013**	**1.2**		**Zatwierdzenie dokumentu**
22.	05.09.2013	1.21		Dostosowanie dokumentu do Księgi Identyfikacji Wizualnej
23.	13.09.2013	1.22		Przegląd dokumentu
24.	20.09.2013	1.23		Przegląd dokumentu
25.	20.09.2013	1.24		Przegląd dokumentu
26.	**02.10.2013**	**1.3**		**Zatwierdzenie dokumentu**
27.	03.06.2014	1.31		Zmiany w rozdziale 2, 6.1.5, 6.3.2 oraz Załączniku 2 w związku z wymianą kluczy kryptograficznych urzędów w systemie
28.	03.06.2014	1.31		Przegląd dokumentu

29.	03.06.2014	1.31	Przegląd dokumentu
30.	06.06.2014	1.31	Przegląd dokumentu
31.	**10.06.2014**	**1.4**	**Zatwierdzenie dokumentu**
32.	05.02.2015	1.41	Dostosowanie dokumentu do zapisów Uchwały nr 1/2015 Zarządu NBP
33.	06.02.2015	1.42	Przegląd dokumentu
34.	20.10.2016	1.51	Zmiany w zmiązku z wymianą funkcji skrótu wykorzystywanej w systemie oraz dostosowanie do uchwały nr 53/2016 Zarządu NBP
35.	**16.12.2016**	**1.6**	**Zatwierdzenie dokumentu**
36.	20.02.2017	1.61	Zmiany związane z uwagami otrzymanymi z PKI Assessment Body (EBC)
37.	27.02.2017	1.61	Przegląd dokumentu
38.	02.03.2017	1.62	Przegląd dokumentu
39.	23.05.2018	2.01	Zmiany związane ze zmianą uchwały nr 53/2016 Zarządu NBP
40.	04.06.2018	2.02	Przegląd dokumentu

Uzgodnienie dokumentu

Data	Wersja	Osoba	Podpis
	2.1	Dyrektor Departamentu Informatyki i Telekomunikacji	

Zatwierdzenie dokumentu

Data	Wersja	Osoba	Podpis
	2.1	Dyrektor Departamentu Bezpieczeństwa	