
System DOCert - Polityka certyfikacji dla certyfikatów użytkowych

OID: 1.3.6.1.4.1.31995.2.1.2
wersja 1.2

Spis treści

1. Wstęp	1
1.1 Wprowadzenie	1
1.2 Nazwa dokumentu i jego identyfikacja	2
1.3 Definicje	2
1.4 Strony Polityki Certyfikacji	5
1.4.1 Narodowy Bank Polski	5
1.4.2 Centrum Certyfikacji Kluczy	6
1.4.3 Punkt Rejestracji Użytkowników	6
1.4.4 Uczestnicy	6
1.4.5 Użytkownicy	6
1.4.6 Strony ufające	7
1.5 Zakres stosowania certyfikatów	7
1.6 Administrowanie Polityką Certyfikacji	7
1.6.1 Organizacja odpowiedzialna za administrowanie dokumentem	7
1.6.2 Kontakt	7
1.6.3 Procedura zatwierdzania dokumentu	8
2. Odpowiedzialność za publikację i repozytorium	9
2.1 Repozytorium	9
2.2 Informacje publikowane w repozytorium	9
2.3 Częstotliwość publikacji	9
2.4 Kontrola dostępu do repozytorium	10
3. Identyfikacja i uwierzytelnianie	11
3.1 Nadawanie nazw	11
3.1.1 Typy nazw	11
3.1.2 Konieczność używania nazw znaczących	11
3.1.3 Zasady interpretacji różnych form nazw	11
3.1.4 Unikalność nazw	12
3.1.5 Rozpoznawanie, uwierzytelnianie oraz rola znaków towarowych	12
3.2 Początkowa walidacja tożsamości	12
3.2.1 Dowód posiadania klucza prywatnego	12
3.2.2 Uwierzytelnienie tożsamości osób prawnych	13
3.2.3 Uwierzytelnienie tożsamości osób fizycznych	13
3.2.4 Dane Uczestnika niepodlegające weryfikacji	13
3.2.5 Walidacja urzędów i organizacji	13
3.2.6 Kryteria interoperacyjności	13
3.3 Identyfikacja i uwierzytelnienie w przypadku żądania aktualizacji kluczy	13
3.3.1 Identyfikacja i uwierzytelnienie w przypadku normalnej aktualizacji kluczy	14
3.3.2 Identyfikacja i uwierzytelnienie w przypadku żądania aktualizacji kluczy po ich unieważnieniu	14
4. Wymagania funkcjonalne	15
4.1 Składanie wniosków	15

4.1.1 Kto może złożyć wniosek o wydanie certyfikatu ?	15
4.1.2 Proces składania wniosków i związane z tym obowiązki	16
4.2 Przetwarzanie wniosków	16
4.2.1 Realizacja funkcji identyfikacji i uwierzytelniania	16
4.2.2 Przyjęcie lub odrzucenie wniosku	17
4.2.3 Okres oczekiwania na przetworzenie wniosku	18
4.3 Wydanie certyfikatu	18
4.3.1 Czynności CCK wykonywane podczas wydawania certyfikatu	18
4.3.2 Informowanie Użytkownika o wydaniu certyfikatu	18
4.4 Akceptacja certyfikatu	19
4.4.1 Potwierdzenie akceptacji certyfikatu	19
4.4.2 Publikowanie certyfikatu przez CCK	19
4.4.3 Informowanie innych podmiotów o wydaniu certyfikatu	19
4.5 Stosowanie kluczy kryptograficznych oraz certyfikatów	20
4.5.1 Stosowanie kluczy i certyfikatów przez Uczestnika	20
4.5.2 Stosowanie kluczy i certyfikatu przez stronę ufającą	20
4.6 Recertyfikacja	20
4.7 Odnowienie certyfikatu	20
4.7.1 Okoliczności odnowienia certyfikatu	21
4.7.2 Kto może żądać odnowienia certyfikatu?	21
4.7.3 Przetwarzanie wniosku o odnowienie certyfikatu	22
4.7.4 Informowanie o wydaniu nowego certyfikatu	22
4.7.5 Potwierdzenie akceptacji nowego certyfikatu	22
4.7.6 Publikowanie nowego certyfikatu	22
4.7.7 Informowanie o wydaniu certyfikatu innych podmiotów	22
4.8 Modyfikacja certyfikatu	22
4.9 Unieważnienie i zawieszenie certyfikatu	22
4.9.1 Okoliczności unieważnienia certyfikatu	23
4.9.2 Kto może żądać unieważnienia certyfikatu	24
4.9.3 Procedura unieważniania certyfikatu	24
4.9.4 Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu	25
4.9.5 Maksymalny dopuszczalny czas przetwarzania wniosku o unieważnienie	25
4.9.6 Obowiązek sprawdzania list CRL przez stronę ufającą	25
4.9.7 Częstotliwość publikowania list CRL	25
4.9.8 Maksymalne opóźnienie w publikowaniu list CRL	26
4.9.9 Dostępność usługi OCSP	26
4.9.10 Obowiązek sprawdzania unieważnień w trybie on-line	26
4.9.11 Inne dostępne formy ogłaszania unieważnień certyfikatów	26
4.9.12 Specjalne obowiązki w przypadku naruszenia ochrony klucza	26
4.9.13 Okoliczności zawieszenia certyfikatu	26
4.9.14 Kto może żądać zawieszenia certyfikatu	27
4.9.15 Procedura zawieszenia i uchylecia zawieszenia certyfikatu	27
4.9.16 Ograniczenia okresu zawieszenia certyfikatu	27

4.10 Usługi weryfikacji statusu certyfikatu	27
4.10.1 Charakterystyki operacyjne	27
4.10.2 Dostępność usługi	28
4.10.3 Cechy opcjonalne	28
4.11 Zakończenie subskrypcji	28
4.12 Deponowanie i odtwarzanie klucza	28
5. Zabezpieczenia techniczne, organizacyjne i operacyjne	29
5.1 Zabezpieczenia fizyczne	29
5.1.1 Lokalizacja i budynki	29
5.1.2 Dostęp fizyczny	29
5.1.3 Zasilanie oraz klimatyzacja	29
5.1.4 Zagrożenie powodziowe	30
5.1.5 Ochrona przeciwpożarowa	30
5.1.6 Nośniki informacji	30
5.1.7 Niszczenie zbędnych nośników informacji	30
5.1.8 Przechowywanie kopii bezpieczeństwa	30
5.2 Zabezpieczenia organizacyjne	31
5.2.1 Zaufane role	31
5.2.2 Lista osób wymaganych podczas realizacji zadania	31
5.2.3 Identyfikacja oraz uwierzytelnianie każdej roli	31
5.2.4 Role, które nie mogą być łączone	32
5.3 Nadzorowanie personelu	32
5.3.1 Kwalifikacje, doświadczenie oraz upoważnienia	32
5.3.2 Procedury weryfikacji przygotowania	32
5.3.3 Szkolenie	32
5.3.4 Częstotliwość powtarzania szkoleń oraz wymagania	32
5.3.5 Częstotliwość rotacji stanowisk i jej kolejność	33
5.3.6 Sankcje z tytułu nieuprawnionych działań	33
5.3.7 Pracownicy kontraktowi	33
5.3.8 Dokumentacja przekazana pracownikom	33
5.4 Procedury rejestrowania zdarzeń oraz audytu	33
5.4.1 Typy rejestrowanych zdarzeń	33
5.4.2 Częstotliwość przetwarzania zapisów rejestrowanych zdarzeń	34
5.4.3 Okres przechowywania zapisów rejestrowanych zdarzeń	34
5.4.4 Ochrona zapisów rejestrowanych zdarzeń	34
5.4.5 Procedury tworzenia kopii zapisów rejestrowanych zdarzeń	34
5.4.6 System gromadzenia zapisów rejestrowanych zdarzeń (wewnętrzny a zewnętrzny)	34
5.4.7 Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenie	35
5.4.8 Oszacowanie podatności na zagrożenia	35
5.5 Zapisy archiwalne	35
5.5.1 Rodzaje archiwizowanych danych	35
5.5.2 Okres przechowywania archiwum	35
5.5.3 Ochrona archiwum	35

5.5.4	Procedury tworzenia kopii archiwalnych	36
5.5.5	Wymaganie znakowania czasem kopii archiwalnych	36
5.5.6	Kopie archiwalne rejestrów zdarzeń (system wewnętrzny i zewnętrzny)	36
5.5.7	Procedury dostępu oraz weryfikacji zarchiwizowanej informacji	36
5.6	Zmiana klucza	36
5.7	Naruszenie ochrony klucza i uruchamianie po awariach oraz klęskach żywiołowych	37
5.7.1	Procedury obsługi incydentów i reagowania na nie	37
5.7.2	Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych	37
5.7.3	Ujawnienie lub podejrzenie ujawnienia klucza prywatnego podmiotu (CCK lub PRU)	37
5.7.4	Zapewnienie ciągłości działania po katastrofach	38
5.8	Zakończenie działalności CCK lub PRU	39
5.8.1	CCK	39
5.8.2	PRU	39
6	Procedury bezpieczeństwa technicznego	41
6.1	Generowanie pary kluczy i jej instalowanie	41
6.1.1	Generowanie pary kluczy	41
6.1.2	Przekazywanie klucza prywatnego Użytkownikowi	41
6.1.3	Dostarczanie klucza publicznego do wystawcy	41
6.1.4	Przekazywanie klucza publicznego CCK	42
6.1.5	Długości kluczy	42
6.1.6	Parametry generowania klucza publicznego oraz weryfikacja jakości	42
6.1.7	Akceptowane zastosowanie kluczy (zgodnie z polem KeyUsage w X.509 v3)	42
6.2	Ochrona klucza prywatnego oraz nadzorowanie mechanizmów modułu kryptograficznego	42
6.2.1	Standardy modułów kryptograficznych	42
6.2.2	Podział klucza prywatnego na części	43
6.2.3	Deponowanie klucza prywatnego	43
6.2.4	Kopie zapasowe klucza prywatnego	43
6.2.5	Archiwizowanie klucza prywatnego	43
6.2.6	Wprowadzenie lub pobieranie klucza prywatnego do/z modułu kryptograficznego	43
6.2.7	Przechowywanie klucza prywatnego w module kryptograficznym	43
6.2.8	Metoda aktywacji klucza prywatnego	44
6.2.9	Metoda dezaktywacji klucza prywatnego	44
6.2.10	Metoda niszczenia klucza prywatnego	45
6.2.11	Ocena modułu kryptograficznego	45
6.3	Inne aspekty zarządzania kluczami	45
6.3.1	Archiwizowanie kluczy publicznych	45
6.3.2	Okresy stosowania klucza publicznego i prywatnego	45
6.4	Dane aktywujące	46
6.4.1	Generowanie danych aktywujących i ich instalowanie	46
6.4.2	Ochrona danych aktywujących	47
6.4.3	Inne problemy związane z danymi aktywującymi	47
6.5	Nadzorowanie bezpieczeństwa systemu komputerowego	47
6.5.1	Wymagania techniczne dotyczące specyficznych zabezpieczeń systemów komputerowych	48

6.5.2 Ocena bezpieczeństwa systemów komputerowych	48
6.6 Cykl życia zabezpieczeń technicznych	48
6.6.1 Nadzorowanie rozwoju systemu	48
6.6.2 Nadzorowanie zarządzania bezpieczeństwem	48
6.6.3 Nadzorowanie cyklu życia zabezpieczeń	49
6.7 Nadzorowanie zabezpieczeń sieci komputerowej	49
6.8 Znakowanie czasem	49
7. Profile certyfikatów oraz list CRL	50
7.1 Profil certyfikatu	50
7.1.1 Numer wersji	51
7.1.2 Rozszerzenia certyfikatów	51
7.1.3 Identyfikatory algorytmów	52
7.1.4 Format nazw	52
7.1.5 Ograniczenia nakładane na nazwy	52
7.1.6 Identyfikatory polityk certyfikacji	52
7.1.7 Stosowanie rozszerzenia określającego ograniczenia nakładane na politykę certyfikacji	52
7.1.8 Składnia i semantyka kwalifikatorów polityki certyfikacji	52
7.1.9 Przetwarzanie semantyki krytycznych rozszerzeń polityki certyfikacji	53
7.2 Profil listy unieważnionych certyfikatów (CRL)	53
7.2.1 Numer wersji	54
7.2.3 Rozszerzenia CRL oraz rozszerzenia dostępu do CRL	54
7.2.4 Rozszerzenia dostępu do CRL	54
8. Audyt zgodności i inne oceny	56
8.1 Częstotliwość i okoliczności oceny	56
8.2 Tożsamość i kwalifikacje audytora	56
8.3 Związek audytora z audytowaną jednostką	56
8.4 Zagadnienia objęte audytem	56
8.5 Działania podejmowane w celu usunięcia usterek wykrytych podczas audytu	56
8.6 Informowanie o wynikach audytu	56
9. Inne kwestie biznesowe i prawne	57
9.1 Opłaty	57
9.2 Odpowiedzialność finansowa	57
9.3 Poufność informacji biznesowej	57
9.3.1 Zakres poufności informacji	57
9.3.2 Informacje znajdujące się poza zakresem poufności informacji	58
9.3.3 Obowiązek ochrony poufności informacji	58
9.4 Zobowiązania i gwarancje	58
9.5 Wyłączenia odpowiedzialności z tytułu gwarancji	60
9.6 Ograniczenia odpowiedzialności	60
10. Ochrona danych osobowych	61
Załącznik A – Autocertyfikaty CCK	62
Załącznik B – Historia zmian dokumentu	63

1. Wstęp

1.1 Wprowadzenie

Narodowy Bank Polski, zwany dalej „NBP”, od marca 1996 roku stosuje technologię klucza publicznego do zapewnienia atrybutów ochrony informacji jakimi są integralność, poufność i niezaprzeczalność w systemach informatycznych obsługujących Klientów NBP. Do realizacji tego celu w NBP wykorzystywany jest system DOCert, służący do wystawiania, unieważniania i dystrybucji certyfikatów. W skład systemu DOCert wchodzi dwa Centra Certyfikacji Kluczy, zwane dalej „CCK” lub „urzędami”:

- NBP CCK 2 - wydające certyfikaty użytkowe,
- NBP CCK TEST 2 - wydające certyfikaty testowe,

a także 17 Punktów Rejestracji Użytkowników, zwanych dalej „PRU” i funkcjonujących: 1 – w Centrali NBP oraz 16 - w oddziałach okręgowych NBP. Każdy PRU posiada wydzielone stacje robocze, dedykowane do generowania kluczy kryptograficznych Uczestników.

Poza CCK i PRU w skład systemu DOCert wchodzi System Zdalnej Obsługi Certyfikatów, zwany dalej „SZOC” dostępny na stronie www.DOCert.nbp.pl i umożliwiający zdalne generowanie lub aktualizowanie kluczy kryptograficznych i certyfikatów na stacji roboczej Klienta, bez konieczności składania wizyty w siedzibie NBP.

Niniejszy dokument „**System DOCert - Polityka certyfikacji dla certyfikatów użytkowych**” zwany dalej „Polityką”, opisuje zasady funkcjonowania urzędu NBP CCK 2 w systemie DOCert i ma zastosowanie dla wszystkich użytkowników systemu DOCert tzn. CCK, PRU, podmiotów wnioskujących o certyfikat do NBP lub zdalnie generujących klucze i certyfikaty, posiadaczy certyfikatów oraz stron ufających. Polityka określa sposób świadczenia usług zaufania, począwszy od rejestracji Uczestników, certyfikacji kluczy publicznych, aktualizacji kluczy i certyfikatów, na unieważnianiu certyfikatów kończąc. Stanowi swego rodzaju „przewodnik” w relacjach pomiędzy systemem DOCert a jego użytkownikami. Z tego powodu wszyscy użytkownicy systemu DOCert powinni znać Politykę i stosować się do zapisów w niej zawartych.

Struktura i merytoryczna zawartość niniejszej Polityki są zgodne z dokumentem RFC 3647 *Certificate Policy and Certificate Practice Statement Framework*. W Polityce zostały zawarte wszystkie elementy opisane w RFC 3647. Zabieg ten ma na celu uczynienie dokumentu bardziej przejrzystym i bardziej przyjaznym dla odbiorców. W przypadku, gdy wymieniony element nie występuje w systemie DOCert - w odpowiednim rozdziale wpisano „Nie dotyczy”.

1.2 Nazwa dokumentu i jego identyfikacja

Nazwa dokumentu	Polityka Certyfikacji dla certyfikatów użytkowych
Wersja dokumentu	1.2
Status dokumentu	obowiązujący
Data wprowadzenia	25.05.2018
OID	1.3.6.1.4.1.31995.2.1.2
Lokalizacja	http://www.DOCert.nbp.pl/Certyfikaty/PC_DOCert.pdf

1.3 Definicje

Na użytek Polityki przyjmuje się następujące pojęcia:

- 1) **autocertyfikat** (certyfikat samopodpisany) - certyfikat klucza publicznego, w którym podpis da się zweryfikować przy pomocy klucza publicznego, zawartego w tym certyfikacie (w polu **subjectKeyInfo**), zawartości pól **issuer** oraz **subject** są takie same, zaś pole **cA** rozszerzenia **BasicConstraints** ustawione jest na **true**.
- 2) **centrum certyfikacji kluczy (CCK)** - moduł systemu DOCert, posługujący się własnym, wygenerowanym przez siebie kluczem prywatnym służącym do elektronicznego podpisywania certyfikatów, wystawiający, unieważniający i dystrybuujący certyfikaty zgodnie z zasadami określonymi w niniejszej Polityce.
- 3) **certyfikat (certyfikat klucza publicznego)** - elektroniczne zaświadczenie, za pomocą którego klucz publiczny jest przyporządkowany do Uczestnika, umożliwiającą jednoznaczną jego identyfikację.
- 4) **certyfikat zakładkowy** – samowystawiony certyfikat CCK, służący do zbudowania zaufania pomiędzy dwoma różnymi kluczami publicznymi jednego CCK; jest generowany podczas planowej wymiany kluczy CCK.
- 5) **Gestor** - jednostka NBP, która sprawuje merytoryczny nadzór nad systemem informatycznym, a w szczególności określa cel jego powstania.
- 6) **identyfikator wyróżniający** - informacja zamieszczona w certyfikacie, pozwalająca na jednoznaczną identyfikację Uczestnika w ramach zbioru Uczestników obsługiwanych przez CCK.
- 7) **infrastruktura klucza publicznego** - wzajemnie powiązane ze sobą elementy infrastruktury sprzętowej, programowej, baz danych, sieci, procedury bezpieczeństwa oraz zobowiązania prawne, które dzięki współpracy realizują oraz udostępniają usługi certyfikacyjne.
- 8) **integralność** - właściwość świadcząca o tym, że informacje nie zostały zmienione od momentu podpisania do momentu zweryfikowania podpisania.
- 9) **jednostka organizacyjna NBP** - departament Centrali i oddział okręgowy NBP.

- 10) **Klient** - osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która na podstawie umowy lub przepisów powszechnie obowiązujących korzysta z certyfikatów systemu DOCert.
- 11) **klucz kryptograficzny** - parametr, który steruje operacjami szyfrowania lub deszyfrowania informacji albo operacjami podpisywania i weryfikacji podpisu.
- 12) **klucz prywatny** - klucz kryptograficzny do wyłącznego użytku Uczestnika podpisującego lub deszyfrującego adresowaną do niego informację.
- 13) **klucz publiczny** - klucz kryptograficzny publicznie znany, powiązany z kluczem prywatnym, który jest stosowany do szyfrowania wysyłanej do adresata informacji lub weryfikowania podpisania.
- 14) **kod jednorazowy** – wygenerowany przez CCK lub PRU ciąg znaków, przypisany do Uczestnika i pozwalający na wygenerowanie dla niego, za pomocą systemu zdalnej obsługi certyfikatów, kluczy kryptograficznych i certyfikatów.
- 15) **lista CRL** - lista unieważnionych lub zawieszonych certyfikatów, których okres ważności jeszcze nie upłynął.
- 16) **niezaprzeczalność** - właściwość polegająca na tym, że nadawca informacji nie może zanegować faktu jej nadania.
- 17) **OCSP** – usługa weryfikacji statusu certyfikatu w trybie on-line,
- 18) **Operator Punktu Rejestracji Użytkowników (Operator PRU)** – pracownik NBP realizujący zadania Punktu Rejestracji Użytkowników.
- 19) **pakiet ochrony kryptograficznej** - zestaw narzędzi informatycznych przekazywany przez NBP Uczestnikowi, służący do zapewnienia poufności, integralności i niezaprzeczalności informacji.
- 20) **PIN** - osobisty numer identyfikacyjny, kod zabezpieczający kartę elektroniczną przed możliwością użycia jej przez osoby niepowołane.
- 21) **podpis cyfrowy** - przekształcenie kryptograficzne danych, umożliwiające odbiorcy sprawdzenie pochodzenia i integralności tych danych oraz zapewniających ochronę nadawcy i odbiorcy jednostki danych przed sfałszowaniem przez odbiorcę.
- 22) **podpis elektroniczny** - dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny.
- 23) **podpisanie** – czynność polegająca na:
 - złożeniu podpisu elektronicznego zgodnie z Ustawą z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. 2016 poz. 1579) lub
 - dołączeniu danych umożliwiających sprawdzenie autentyczności i integralności podpisanych informacji oraz uwierzytelnienie Uczestnika.

- 24) **polityka certyfikacji** - dokument określający ogólne zasady stosowane przez CCK podczas procesu certyfikacji kluczy publicznych, definiujący osoby biorące udział w tym procesie, ich obowiązki i odpowiedzialność, typy certyfikatów, procedury weryfikacji tożsamości używane przy ich wydawaniu oraz obszary zastosowań.
- 25) **poufność** - właściwość polegająca na tym, że informacje są niedostępne dla nieupoważnionych osób.
- 26) **PUK** (lub PIN Administratora) – kod służący do zarządzania kartą elektroniczną, w szczególności do jej odblokowania.
- 27) **Punkt Rejestracji Użytkowników (PRU)** – moduł systemu DOCert, służący w szczególności do weryfikacji Użytkowników i do rejestracji Uczestników, a także do generowania i certyfikacji kluczy kryptograficznych Uczestników.
- 28) **schemat podziału sekretu „n z m”** - podział klucza kryptograficznego na „m” części w taki sposób, by do jego odtworzenia konieczne było użycie przynajmniej „n” tych części (przy założeniu, że „n” nie jest większe od „m”).
- 29) **System DOCert** - system informatyczny NBP służący do centralnego, elektronicznego wystawiania i dystrybucji certyfikatów, oparty o infrastrukturę klucza publicznego (ang. Public Key Infrastructure).
- 30) **System Zdalnej Obsługi Certyfikatów** – umieszczona na stronie www.docert.nbp.pl aplikacja pozwalająca na generowanie i certyfikację kluczy kryptograficznych Uczestnika bezpośrednio na stacji roboczej Klienta, bez konieczności składania wizyty w siedzibie NBP.
- 31) **Uczestnik** - Klient, przedstawiciel Klienta, jednostka organizacyjna NBP lub obiekt (np. serwer) posiadający certyfikat wydany w systemie DOCert.
- 32) **umowa** - umowa zawarta pomiędzy Klientem i NBP lub akt prawny (np. rozporządzenie), na podstawie którego NBP świadczy dla Klienta usługi zaufania.
- 33) **uwierzytelnienie** - właściwość umożliwiająca potwierdzenie deklarowanej tożsamości nadawcy informacji.
- 34) **Użytkownik** – Uczestnik, przedstawiciel Uczestnika lub osoba odpowiedzialna za realizację zadań związanych z generowaniem, odbiorem oraz późniejszym wykorzystywaniem certyfikatów.

Usługi certyfikacyjne w systemie DOCert nie są usługami publicznymi. Jedynie podmioty, które podpisały umowę z NBP lub które na mocy obowiązującego prawa są zobowiązane do użytkowania jednego z systemów informatycznych NBP, mogą otrzymać certyfikaty systemu DOCert. **Klientem** nazywamy podmiot, który na mocy umowy lub obowiązującego prawa wykorzystuje przynajmniej jeden z systemów NBP, a co za tym idzie - wykorzystuje certyfikaty systemu DOCert.

Wszyscy posiadacze certyfikatów systemu DOCert określani są jako **Uczestnicy**. Oznacza to, iż Uczestnikiem może być zarówno instytucja, np. bank komercyjny, jak i pracownik tej instytucji, może to być także osoba fizyczna niezwiązana z żadną instytucją, a także komponent infrastruktury teleinformatycznej NBP, taki jak serwer czy stacja robocza. W pierwszym przypadku w certyfikacie zawarte będą tylko dane instytucji, np. nazwa i numer rozliczeniowy banku, w drugim przypadku - zarówno dane instytucji jak i dane właściciela certyfikatu (np. imię i nazwisko), w trzecim przypadku w certyfikacie zawarte będą tylko dane identyfikujące konkretną osobę fizyczną (np. imię i nazwisko), a w czwartym przypadku - dane identyfikujące konkretny sprzęt komputerowy.

W przypadku certyfikatów wydawanych dla osób fizycznych - zarówno dla pracowników, Klientów, jak i dla osób działających we własnym imieniu, wszystkie operacje związane z generowaniem i odbiorem kluczy kryptograficznych i certyfikatów muszą być przeprowadzane osobiście przez osobę, której dane zawarte są w certyfikacie lub przez jej pełnomocnika posiadającego notarialne upoważnienie.

W przypadku certyfikatów wystawianych Uczestnikom niebędącym osobami fizycznymi, generowanie i odbiór kluczy kryptograficznych, a także wszelki kontakt z PRU, realizowany jest przez osobę fizyczną upoważnioną przez Klienta lub odpowiedzialną za Uczestnika (w przypadku, gdy Uczestnikiem jest komponent infrastruktury teleinformatycznej). W celu uproszczenia dalszych zapisów Polityki osobę fizyczną będącą Uczestnikiem, upoważnioną przez Klienta lub odpowiedzialną za Uczestnika i wykonującą czynności związane z generowaniem kluczy kryptograficznych Uczestnika, będziemy nazywać Użytkownikiem.

W większości przypadków Użytkownicy otrzymują i wykorzystują certyfikaty systemu DOCert na podstawie umowy zawartej pomiędzy Klientem a NBP. W niektórych przypadkach taka umowa nie jest zawierana a zasady współpracy pomiędzy Klientem a NBP określone są w regulaminach lub w aktach prawnych. W celu uproszczenia nazewnictwa, na potrzeby niniejszej Polityki przyjmuje się, iż termin „Umowa” oznacza dokument, na podstawie którego NBP wydaje dla Klienta certyfikaty.

1.4 Strony Polityki Certyfikacji

1.4.1 Narodowy Bank Polski

NBP jest właścicielem systemu DOCert i odpowiada za funkcjonowanie całości systemu DOCert. Wszystkie osoby pełniące role wymienione w punkcie 5.2.1 są pracownikami NBP. Wybrane elementy systemu DOCert mogą być objęte umowami serwisowymi i wsparcia, zawartymi pomiędzy NBP a firmami zewnętrznymi, z zastrzeżeniem, że usługi zaufania w

tym systemie świadczone są jedynie przez pracowników NBP. Zakres obowiązków i odpowiedzialności firm zewnętrznych regulują umowy serwisowe i wsparcia.

1.4.2 Centrum Certyfikacji Kluczy

Centrum Certyfikacji Kluczy odpowiada za:

- ustalanie parametrów początkowych systemu,
- zarządzanie kluczami kryptograficznymi i certyfikatami CCK,
- zarządzanie certyfikatami Operatorów PRU,
- generowanie, publikację i unieważnianie certyfikatów Uczestników,
- generowanie i publikację list unieważnionych certyfikatów,
- generowanie kodów jednorazowych dla Uczestników,
- prowadzenie bazy certyfikatów,
- dystrybucję pakietów ochrony kryptograficznej do PRU.

W systemie DOCert za funkcjonowanie Centrum Certyfikacji Kluczy odpowiada Departament Bezpieczeństwa NBP, zwany dalej „DB”.

1.4.3 Punkt Rejestracji Użytkowników

Punkty Rejestracji Użytkowników odpowiadają za:

- weryfikację tożsamości Użytkowników,
- rejestrację i modyfikację danych Uczestników,
- przesyłanie do CCK, w imieniu Uczestników żądań certyfikacji ich kluczy kryptograficznych,
- wystawianie, w imieniu Uczestników żądań unieważnienia lub zawieszenia ich certyfikatów,
- dystrybucję pakietów ochrony kryptograficznej,
- udzielanie konsultacji oraz szkoleń z zakresu obsługi pakietów ochrony kryptograficznej,
- generowanie kodów jednorazowych.

W systemie DOCert za funkcjonowanie Punktów Rejestracji Użytkowników odpowiadają oddziały okręgowe NBP.

1.4.4 Uczestnicy

Podmiot, osoba lub obiekt, o którym mowa w rozdziale 1.3 punkt 31.

1.4.5 Użytkownicy

Użytkownik to osoba fizyczna, o której mowa w rozdziale 1.3 punkt 35, odpowiedzialna za wykonywanie czynności związanych z certyfikatami Uczestnika w systemie DOCert, takich

jak np. generowanie kluczy kryptograficznych, wykorzystywanie wygenerowanych lub otrzymanych kluczy kryptograficznych i certyfikatów, a także za zapewnienie bezpieczeństwa klucza prywatnego oraz hasła chroniącego ten klucz.

1.4.6 Strony ufające

Stroną ufającą jest osoba lub podmiot, inna niż Uczestnik, która akceptuje i ufa certyfikatowi wydanemu w systemie DOCert.

1.5 Zakres stosowania certyfikatów

Certyfikaty wydawane w systemie DOCert nie są certyfikatami kwalifikowanymi w rozumieniu ustawy o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. 2016 poz 1579, z późn. zm.) zwanej dalej „ustawą o usługach zaufania”.

Certyfikaty wydawane w systemie DOCert mogą być stosowane:

- tylko zgodnie z informacją zawartą w certyfikacie (pole KeyUsage),
- w systemach informatycznych NBP do wymiany informacji wewnątrz NBP oraz pomiędzy NBP a Klientami,
- do zapewnienia integralności, poufności i niezaprzeczalności w systemach informatycznych NBP,
- w należącym do Ministerstwa Finansów systemie obsługi budżetu państwa TREZOR, do zapewnienia integralności oraz niezaprzeczalności.

Szczegółowy zakres stosowania certyfikatów systemu DOCert zależy od systemu, na potrzeby którego zostały wygenerowane i jest każdorazowo określony w odpowiednich dokumentach.

1.6 Administrowanie Polityką Certyfikacji

1.6.1 Organizacja odpowiedzialna za administrowanie dokumentem

Autorem i administratorem niniejszej Polityki jest:

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

1.6.2 Kontakt

Za zarządzanie Polityką odpowiedzialny jest:

Departament Bezpieczeństwa

Narodowego Banku Polskiego

ul. Świętokrzyska 11/21

00-919 Warszawa

tel. +48221851414 fax: +48221852336

mail: cck@nbp.pl

1.6.3 Procedura zatwierdzania dokumentu

Ogólne zasady świadczenia usług zaufania w systemie DOCert określone są w Uchwale nr 53/2016 Zarządu NBP z dnia 21 października 2016 r. w sprawie wprowadzenia dokumentów określających zasady świadczenia usług zaufania przez Narodowy Bank Polski zwanej dalej „U53/2016”. W treści uchwały zawarte są m.in. informacje związane z odpowiedzialnością NBP jako dostawcy usług zaufania, informacje dotyczące podziału zadań pomiędzy poszczególnymi departamentami i oddziałami okręgowymi NBP, czy informacje dotyczące kontroli i audytu. Niniejsza Polityka powstała na bazie załącznika nr 2 do U53/2016 i jest zatwierdzana przez Dyrektora DB.

Każda z wersji Polityki obowiązuje (posiada aktualny status) do czasu zatwierdzenia i opublikowania nowej wersji. Nowa wersja opracowywana jest przez pracowników DB i ze statusem „do uzgodnienia” jest przekazywana do oddziałów okręgowych NBP oraz Gestorów systemów informatycznych NBP wykorzystujących certyfikaty systemu DOCert. Po uzgodnieniu, nowa wersja Polityki zatwierdzana jest przez Dyrektora DB.

W przypadku zmiany zapisów znajdujących się w U53/2016 - przed opracowaniem nowej wersji Polityki - konieczne jest dokonanie niezbędnej zmiany w U53/2016. Zmiana odbywa się na zasadach obowiązujących w NBP.

Pracownicy DB, nie rzadziej niż raz w roku, oraz w przypadku wprowadzania jakichkolwiek zmian w systemie DOCert, dokonują przeglądu Polityki pod względem aktualności jej zapisów.

2. Odpowiedzialność za publikację i repozytorium

2.1 Repozytorium

W systemie DOCert wyróżnić można dwa oddzielne repozytoria:

- repozytorium wewnętrzne - składające się z dwóch serwerów dystrybucji certyfikatów i list CRL. Serwery te znajdują się w sieci wewnętrznej NBP i nie istnieje techniczna możliwość dostępu do nich z zewnątrz,
- repozytorium zewnętrzne - znajdujące się na stronie internetowej www.docert.nbp.pl.

2.2 Informacje publikowane w repozytorium

W repozytorium wewnętrznym publikowane są certyfikaty CCK, certyfikaty Uczestników oraz listy CRL. W repozytorium zewnętrznym publikowane są następujące informacje:

- autocertyfikat NBP CCK 2 pod adresem:
<http://www.docert.nbp.pl/certyfikaty/pliki/nbpccck2.crt>
- autocertyfikat NBP TEST CCK 2 pod adresem:
http://www.docert.nbp.pl/certyfikaty/pliki/ccknbp_test_2014.crt
- lista CRL wydana przez NBP CCK 2, pod adresem:
<http://www.docert.nbp.pl/Certyfikaty/CRLcck2.crl>
- lista CRL wydana przez NBP TEST CCK 2, pod adresem:
<http://www.docert.nbp.pl/Certyfikaty/CRLccktest2.crl>
- Polityka Certyfikacji dla certyfikatów użytkowych, pod adresem:
http://www.docert.nbp.pl/certyfikaty/PC_DOCert.pdf
- Informacja o zasadach świadczenia usług zaufania w systemie DOCert, pod adresem:
http://www.docert.nbp.pl/certyfikaty/PDS_DOCert.pdf

2.3 Częstotliwość publikacji

Publikacja certyfikatów Uczestników oraz list CRL na serwery dystrybucji certyfikatów oraz na stronę internetową www.docert.nbp.pl (tylko lista CRL) jest automatyczna i następuje w ciągu 60 minut od wygenerowania lub unieważnienia/zawieszenia certyfikatu. Dodatkowo, Operator CCK może w dowolnym momencie ręcznie opublikować listę CRL.

Pozostałe informacje publikowane na stronie www.docert.nbp.pl, np. autocertyfikaty CCK oraz Polityki publikowane są ręcznie przez pracowników NBP tylko w przypadku konieczności ich aktualizacji.

2.4 Kontrola dostępu do repozytorium

Dostęp do serwerów dystrybucji certyfikatów możliwy jest jedynie ze stacji roboczych i serwerów znajdujących się wewnątrz sieci NBP. Zmiany na serwerach dystrybucji certyfikatów mogą być dokonywane jedynie za pośrednictwem CCK.

Strona www.docert.nbp.pl jest publicznie dostępna, jednak nie umożliwia nieautoryzowanego zapisu lub modyfikacji danych.

3. Identyfikacja i uwierzytelnianie

Poniżej przedstawiono ogólne zasady weryfikacji tożsamości Użytkowników, którymi kieruje się PRU i CCK podczas wydawania certyfikatów. Zasady te, oparte na określonych typach informacji, definiują środki, które są niezbędne do uzyskania pewności, iż informacje te są dokładne i wiarygodne w momencie wydawania certyfikatu. Procedura weryfikacji tożsamości Użytkownika jest przeprowadzana przez Operatora PRU za każdym razem przed generowaniem certyfikatu w siedzibie NBP. Natomiast w przypadku korzystania z SZOC identyfikacja i uwierzytelnianie dotyczy Uczestnika i odbywa się na podstawie posiadanego certyfikatu lub kodu jednorazowego.

3.1 Nadawanie nazw

Certyfikaty wydawane przez CCK w systemie DOCert są zgodne z normą X.509 v3. Oznacza to, że zarówno wydawca certyfikatu, jak też działający w jego imieniu PRU, akceptują tylko takie nazwy Uczestników, które są zgodne ze standardem X.509 (z powołaniem się na zalecenia serii X.500).

Dane, które zostają umieszczane w certyfikacie generowanym w systemie DOCert, dostarczane są do PRU we wniosku „Zamówienie na usługę kryptograficzną” zwanym dalej „Zamówieniem”, podpisanym przez Gestora lub osobę przez niego upoważnioną. Możliwe jest także pobranie danych z katalogu LDAP (w takim przypadku, w Zamówieniu znajduje się jedynie identyfikator Uczestnika).

3.1.1 Typy nazw

Dokładna struktura identyfikatora wyróżniającego w certyfikacie zależy od systemu informatycznego, w którym wykorzystywany jest certyfikat i jest ustalana z Gestorem tego systemu.

3.1.2 Konieczność używania nazw znaczących

W systemie DOCert wszystkie nazwy wchodzące w skład identyfikatora wyróżniającego Uczestnika muszą posiadać swoje znaczenie w języku polskim lub angielskim.

3.1.3 Zasady interpretacji różnych form nazw

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

3.1.4 Unikalność nazw

W systemie DOCert istnieją 3 wyróżniki certyfikatu, które mogą pozwolić na jednoznaczną identyfikację Uczestnika. Są to następujące pola w identyfikatorze wyróżniającym:

- Nazwa powszechna – dla certyfikatów wystawianych dla serwerów;
- Tytuł – dla Uczestników, korzystających z systemów zintegrowanych z systemem ZSZT;
- Email – w pozostałych przypadkach.

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

Na wniosek Klienta, w identyfikatorze wyróżniającym może zostać umieszczona nazwa handlowa lub znak handlowy. Zabrania się jednak używania we wnioskach nazw, które nie są własnością Klienta. W przypadku, gdy we wniosku o wystawienie certyfikatu występują informacje o takim charakterze, wnioskodawca jest zobowiązany do dołączenia dokumentów potwierdzających posiadane prawa własności.

PRU działa na podstawie Zamówienia podpisanego przez Gestora i nie dokonuje dodatkowej weryfikacji, czy Klient ma prawo do posługiwania się nazwą umieszczoną w tym Zamówieniu.

3.2 Początkowa walidacja tożsamości

3.2.1 Dowód posiadania klucza prywatnego

Klucze kryptograficzne w systemie DOCert generowane mogą być na dwa sposoby:

- osobiście przez Użytkownika, na wydzielonym stanowisku w PRU, w obecności Operatora PRU,
- za pomocą SZOC, dostępnego na stronie www.docert.nbp.pl, z zastrzeżeniem, że Użytkownik generujący klucze kryptograficzne posiada ważny certyfikat systemu DOCert lub ważny kod jednorazowy otrzymany z NBP.

W obu przypadkach klucz publiczny w postaci żądania certyfikacyjnego, podpisanego odpowiadającym mu kluczem prywatnym, jest przekazywany do CCK. Aplikacje służące do

generowania kluczy kryptograficznych automatycznie tworzą i podpisują żądania certyfikacyjne.

3.2.2 Uwierzytelnienie tożsamości osób prawnych

Uwierzytelnianie tożsamości osób prawnych przeprowadzane jest przez Gestora systemu informatycznego, na potrzeby którego generowany jest certyfikat, lub przez osobę przez niego upoważnioną. Podstawą wykonywania działań przez PRU jest Zamówienie podpisane przez Gestora lub przez osobę przez niego upoważnioną. Otrzymując podpisane Zamówienie Operator PRU zakłada, iż osoba, która je wypełniła lub akceptowała, dokonała wcześniej uwierzytelnienia.

3.2.3 Uwierzytelnienie tożsamości osób fizycznych

W uzgodnionym terminie Użytkownicy wskazani w Zamówieniu, zgłaszają się do NBP z dokumentem tożsamości. Przed przystąpieniem do generowania kluczy kryptograficznych i certyfikatów Operator PRU dokonuje weryfikacji tożsamości Użytkownika. Weryfikacja ta polega na porównaniu numeru PESEL lub serii i numeru dokumentu tożsamości, wskazanego w Zamówieniu, z informacją zawartą w dokumencie tożsamości, który Użytkownik powinien posiadać podczas wizyty w PRU i okazać na żądanie Operatora PRU.

3.2.4 Dane Uczestnika niepodlegające weryfikacji

Nie dotyczy. Wszystkie dane Uczestnika umieszczane w certyfikacie podlegają weryfikacji w NBP.

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

Aktualizacja kluczy kryptograficznych Uczestnika może być przeprowadzona zarówno w PRU - wtedy proces przebiega identycznie jak w przypadku generowania pierwszych kluczy kryptograficznych, jak i za pomocą SZOC - wtedy Użytkownik nie musi składać wizyty w siedzibie NBP. Wykorzystanie SZOC możliwe jest jednak tylko w okresie ważności aktualnego certyfikatu.

3.3.1 Identyfikacja i uwierzytelnienie w przypadku normalnej aktualizacji kluczy

W przypadku generowania kolejnych kluczy kryptograficznych i certyfikatów w PRU identyfikacja i uwierzytelnianie przebiega identycznie jak w przypadku generowania pierwszych kluczy kryptograficznych. Patrz rozdziały 3.2.1 – 3.2.4.

W przypadku generowania nowych kluczy kryptograficznych i certyfikatów za pomocą SZOC, do identyfikacji i uwierzytelnienia Uczestnika wykorzystywane są aktualne klucze kryptograficzne i certyfikat tego Uczestnika lub kod jednorazowy (dotyczy niektórych systemów).

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

Po unieważnieniu certyfikatów nie ma możliwości skorzystania z SZOC i w celu wygenerowania nowych kluczy kryptograficznych i certyfikatów Użytkownik musi udać się do PRU i powtórzyć procedurę stosowaną w przypadku generowania pierwszych kluczy kryptograficznych i certyfikatów Uczestnika. Patrz rozdziały 3.2.1 – 3.2.4.

4. Wymagania funkcjonalne

4.1 Składanie wniosków

Ze względu na to, iż certyfikaty systemu DOCert wydawane są na potrzeby systemów informatycznych NBP, w systemie DOCert można wyróżnić dwa rodzaje wniosków – wnioski składane przez Klienta do PRU za pośrednictwem Gestora wybranego systemu informatycznego (lub osoby przez niego upoważnionej), oraz wnioski składane przez Klienta bezpośrednio do CCK lub PRU.

W przypadku wniosków składanych za pośrednictwem Gestora, procedura przebiega dwuetapowo. W pierwszym etapie Klient składa do NBP wypełniony i podpisany wniosek, którego wzór, różny dla różnych systemów informatycznych, jest udostępniany Klientowi przez NBP. W drugim etapie, osoba upoważniona przez Gestora, na podstawie otrzymanego od Klienta wniosku, przygotowuje i przekazuje do PRU Zamówienie będące dokumentem stanowiącym podstawę działań PRU.

Niniejsza Polityka opisuje tylko zasady regulujące drugi etap wymienionego wyżej procesu. Zasady regulujące składanie wniosku przez Klienta do NBP określone są w odrębnych dokumentach związanych z poszczególnymi systemami informatycznymi NBP.

Dodatkowo, w systemie DOCert dwa rodzaje wniosków mogą być składane przez Klienta bezpośrednio do CCK lub PRU. Są to wnioski związane z unieważnieniem lub zawieszeniem certyfikatów oraz wnioski o wydanie kluczy kryptograficznych i certyfikatów składane za pomocą SZOC.

4.1.1 Kto może złożyć wniosek o wydanie certyfikatu ?

Podstawą wydania certyfikatu przez PRU jest Zamówienie, przygotowane i podpisane przez Gestora danego systemu lub osobę przez niego upoważnioną. Zamówienie, niepodpisane przez Gestora lub osobę przez niego upoważnioną, jest nieważne i nie będzie akceptowane przez PRU. Zasady dotyczące składania przez Klientów wniosków do NBP określone są w Umowach i nie są regulowane przez niniejszą Politykę.

Wniosek o wydanie nowego certyfikatu za pomocą SZOC może złożyć Użytkownik posiadający dostęp do klucza prywatnego powiązanego z certyfikatem Uczestnika, znający hasło chroniące klucz prywatny lub posiadając ważny kod jednorazowy, otrzymany z NBP.

4.1.2 Proces składania wniosków i związane z tym obowiązki

Wnioski składane za pośrednictwem Gestora

Po otrzymaniu prawidłowo wypełnionego wniosku od Klienta, Gestor lub osoba przez niego upoważniona wypełnia Zamówienie i przekazuje je do PRU. Zamówienie powinno zawierać dane pozwalające na weryfikację tożsamości Użytkowników, którzy zgłoszą się po odbiór kluczy kryptograficznych i certyfikatów: imię, nazwisko, PESEL lub numer dokumentu tożsamości.

W uzgodnionym terminie Użytkownicy wskazani w Zamówieniu, zgłaszają się do NBP z dokumentem tożsamości.

W przypadku poprawnej weryfikacji tożsamości Użytkownika, Operator PRU udostępnia Użytkownikowi stanowisko do generowania kluczy kryptograficznych. Użytkownik osobiście generuje klucze kryptograficzne, ustala hasła dostępu do nich a następnie przekazuje wygenerowane klucze publiczne Operatorowi PRU w celu ich certyfikacji. Operator PRU tworzy żądanie certyfikacyjne, zawierające klucze publiczne Uczestnika, podpisując je swoim kluczem prywatnym i przekazuje do CCK w celu wygenerowania odpowiednich certyfikatów.

Wnioski składane bezpośrednio do PRU lub CCK

Procedura postępowania w przypadku wniosków o unieważnienie lub zawieszenie certyfikatów opisana jest w rozdziale 4.9.3.

W przypadku składania wniosków za pomocą SZOC, procedura generowania kluczy kryptograficznych i certyfikatów realizowana jest na stacji Klienta. Do jej przeprowadzenia konieczne jest posiadanie kluczy kryptograficznych i ważnego certyfikatu (oraz znajomość hasła chroniącego klucz prywatny), lub posiadanie ważnego kodu jednorazowego, otrzymanego z NBP. Na podstawie tych danych dokonywane jest uwierzytelnienie Użytkownika dokonującego generowania kluczy kryptograficznych i certyfikatów za pomocą SZOC. Instrukcje obsługi SZOC dostępne są na stronie www.docert.nbp.pl.

4.2 Przetwarzanie wniosków

4.2.1 Realizacja funkcji identyfikacji i uwierzytelniania

Wnioski składane za pośrednictwem Gestora

Ze względu na fakt, iż PRU nie posiada dokumentów pozwalających na weryfikację podpisów osób upoważnionych ze strony Klienta, funkcje identyfikacji i uwierzytelnienia są podzielone pomiędzy PRU oraz Gestora, lub osobę przez niego upoważnioną.

Osoba wskazana przez Gestora dokonuje weryfikacji podpisów złożonych przez osoby mające prawo reprezentowania Klienta, na dokumentach dostarczonych przez Klienta, np. na wnioskach o wydanie certyfikatu, i na ich podstawie przygotowuje Zamówienie. W Zamówieniu należy jasno wskazać dane osoby/osób, które generować będą klucze kryptograficzne. Dane te obejmować powinny imię i nazwisko oraz numer PESEL lub numer dokumentu tożsamości.

Operator PRU dokonuje weryfikacji tożsamości Użytkownika porównując informacje zawarte w Zamówieniu z dokumentem tożsamości Użytkownika, który wykonywać będzie czynności wskazane w Zamówieniu podpisanym przez Gestora Systemu, lub osobę przez niego upoważnioną. Dopiero po weryfikacji tożsamości, Operator PRU udostępnia Użytkownikowi stanowisko oraz materiały niezbędne do wygenerowania kluczy kryptograficznych.

Wnioski składane bezpośrednio do PRU lub CCK

Procedurę postępowania w przypadku wniosków o unieważnienie lub zawieszenie certyfikatów określa rozdział 4.9.3.

W przypadku wykorzystywania SZOC, funkcje identyfikacji i uwierzytelniania są realizowane na podstawie kodu jednorazowego, otrzymanego z NBP, albo na podstawie posiadanego klucza prywatnego i ważnego certyfikatu.

4.2.2 Przyjęcie lub odrzucenie wniosku

Wnioski składane za pośrednictwem Gestora

Wniosek złożony przez Klienta w NBP zostanie przyjęty i zrealizowany przez CCK, gdy zostaną spełnione łącznie następujące warunki:

- PRU otrzyma poprawne Zamówienie,
- PRU pozytywnie zweryfikuje tożsamość Użytkownika,
- Operator PRU zatwierdzi (za pomocą swojego klucza prywatnego) żądanie certyfikacyjne wysłane do CCK,
- CCK poprawnie zweryfikuje podpis złożony przez Operatora PRU pod żądaniem certyfikacyjnym.

Wnioski składane bezpośrednio do PRU lub CCK

Procedurę postępowania w przypadku wniosków o awaryjne unieważnienie lub zawieszenie certyfikatów określa rozdział 4.9.3.

Wniosek złożony za pomocą SZOC zostanie przyjęty i zrealizowany przez CCK, po spełnieniu jednego z warunków:

1. Użytkownik wprowadzi do systemu poprawny i niewykorzystany wcześniej kod jednorazowy,
2. Użytkownik posiada klucz prywatny, zna hasło chroniące ten klucz a certyfikat powiązany z tym kluczem prywatnym znajduje się w okresie ważności.

4.2.3 Okres oczekiwania na przetworzenie wniosku

Zarówno CCK jak i PRU, dokładają wszelkich starań, by wnioski składane przez Klientów były realizowane w możliwie jak najkrótszym czasie, bez zbędnej zwłoki.

Maksymalny czas przetwarzania wniosku o awaryjne unieważnienie lub zawieszenie certyfikatu ustalany jest dla każdego systemu informatycznego NBP osobno i określony w Umowie zawartej pomiędzy Klientem a NBP.

4.3 Wydanie certyfikatu

4.3.1 Czynności CCK wykonywane podczas wydawania certyfikatu

Procedura wydawania certyfikatu przebiega następująco:

- po otrzymaniu z PRU lub z SZOC potwierdzonego żądania certyfikacyjnego, CCK wystawia certyfikat i zleca jego podpisanie sprzętowemu modułowi bezpieczeństwa,
- podpisany certyfikat jest zapisywany w bazie danych CCK,
- certyfikat jest przesyłany do modułu wykorzystywanego przez PRU lub do SZOC,
- certyfikat jest instalowany na nośniku kluczy kryptograficznych Uczestnika,
- certyfikat jest publikowany w repozytorium.

4.3.2 Informowanie Użytkownika o wydaniu certyfikatu

W przypadku generowania certyfikatów w PRU, Operator PRU informuje Uczestnika o wydaniu certyfikatu, przekazując mu „Protokół przekazania kluczy kryptograficznych”, zawierający informacje dotyczące wydanego certyfikatu wraz z datą jego ważności.

W przypadku wykorzystania SZOC Użytkownik, o wydaniu certyfikatu informowany jest przez system odpowiednim komunikatem.

4.4 Akceptacja certyfikatu

4.4.1 Potwierdzenie akceptacji certyfikatu

W przypadku generowania certyfikatów w PRU, Użytkownik potwierdza akceptację odbieranego certyfikatu poprzez złożenie podpisu na „Protokole przekazania kluczy kryptograficznych”.

W przypadku, gdy Użytkownik nie akceptuje certyfikatu wygenerowanego za pomocą SZOC, zobowiązany jest do niezwłocznego przekazania do PRU żądania unieważnienia tego certyfikatu zgodnie z procedurą, o której mowa w rozdziale 4.9.

W przypadku kluczy kryptograficznych i certyfikatów wykorzystywanych do komunikacji z NBP - w szczególności dotyczy to certyfikatów dla serwerów aplikacyjnych NBP - pracownik NBP odpowiedzialny za zarządzanie tymi kluczami kryptograficznymi, ma obowiązek dokonać ich sprawdzenia a następnie przekazać informację o wyniku tego sprawdzenia do DB.

4.4.2 Publikowanie certyfikatu przez CCK

W repozytorium na stronie www.docert.nbp.pl publikowane są jedynie certyfikaty CCK. Są one publikowane ręcznie przez Operatorów CCK niezwłocznie po ich wygenerowaniu.

Na serwerach dystrybucji certyfikatów publikowane są tylko certyfikaty wykorzystywane w wybranych systemach informatycznych NBP. Publikowane są automatycznie, w ciągu 1 godziny od momentu wygenerowania.

4.4.3 Informowanie innych podmiotów o wydaniu certyfikatu

Uczestnicy nieposiadający dostępu do serwerów dystrybucji certyfikatów opisanych w rozdziale 2 otrzymują w PRU wszystkie certyfikaty, konieczne do zapewnienia prawidłowej pracy systemu informatycznego, właściwego dla Uczestnika.

W przypadku, gdy za dystrybucję wymienionych certyfikatów odpowiedzialny jest DB, certyfikaty mogą zostać rozesłane dopiero po otrzymaniu przez DB informacji, o której mowa w punkcie 4.4.1.

4.5 Stosowanie kluczy kryptograficznych oraz certyfikatów

Ogólne zasady stosowania kluczy kryptograficznych i certyfikatów wydawanych w systemie DOCert opisano poniżej. Dokładne informacje dotyczące dozwolonego zastosowania wydawanych certyfikatów, zawarte są w Umowach pomiędzy Klientem a NBP.

4.5.1 Stosowanie kluczy i certyfikatów przez Uczestnika

Uczestnicy, w tym Operatorzy PRU, zobowiązani są stosować klucze prywatne i certyfikaty:

- zgodnie z treścią certyfikatu (pola keyUsage oraz extendedKeyUsage),
- zgodnie z treścią Umowy zawartej pomiędzy Klientem a NBP,
- tylko w okresie ważności certyfikatu (nie dotyczy certyfikatów do szyfrowania),
- tylko do momentu unieważnienia lub zawieszenia certyfikatu (nie dotyczy certyfikatów do szyfrowania).

4.5.2 Stosowanie kluczy i certyfikatu przez stronę ufającą

Strona ufająca zobowiązana jest stosować certyfikaty:

- zgodnie z treścią certyfikatu (pola keyUsage oraz extendedKeyUsage),
- tylko po zweryfikowaniu ich statusu (patrz rozdział 4.9) oraz wiarygodności podpisu CCK, które wystawiło certyfikat,
- tylko w okresie ich ważności (nie dotyczy certyfikatów do weryfikacji podpisu cyfrowego),
- tylko do momentu unieważnienia lub zawieszenia certyfikatu (nie dotyczy certyfikatów do weryfikacji podpisu cyfrowego).

4.6 Recertyfikacja

W systemie DOCert nie wykonuje się recertyfikacji kluczy kryptograficznych. Przed każdym generowaniem certyfikatu, konieczne jest wygenerowanie nowej pary kluczy kryptograficznych. Zapis ten dotyczy także kluczy kryptograficznych CCK oraz kluczy Operatorów PRU.

4.7 Odnowienie certyfikatu

Odnowienie certyfikatu ma miejsce zawsze wtedy, gdy Uczestnik zażąda wystawienia nowego certyfikatu dla **nowej pary kluczy**. W systemie DOCert nie jest możliwa recertyfikacja posiadanych kluczy kryptograficznych, patrz pkt 4.6.

Odnowienie certyfikatu dotyczy zawsze ściśle określonego, wskazanego we wniosku certyfikatu. Nowy certyfikat posiada prawie identyczną treść jak związany z nim certyfikat. Różnice to:

- nowa para kluczy,
- nowy numer seryjny certyfikatu,
- nowy okres ważności certyfikatu,
- nowy podpis CCK.

Dodatkowo dopuszczalne są zmiany w identyfikatorze wyróżniającym certyfikatu, jednak zmiany te nie mogą dotyczyć pola w którym zawarty jest unikalny identyfikator Uczestnika.

Odnowienie certyfikatu z użyciem SZOC, połączone ze zmianami w identyfikatorze wyróżniającym certyfikatu jest możliwe tylko w przypadku, gdy dane Uczestnika pobierane są z katalogu LDAP. W innym przypadku, odnowienie certyfikatu musi odbyć się w PRU.

Procedurze odnowienia certyfikatu podlegają również certyfikaty CCK. Nowe klucze kryptograficzne i certyfikat CCK generowane są najpóźniej na pięć lat przed końcem okresu ważności aktualnie wykorzystywanego certyfikatu. Operacja ta wykonywana jest przez Operatorów CCK pod nadzorem Inspektora Bezpieczeństwa Systemu systemu DOCert.

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?

W przypadku wykorzystania SZOC, odnowienia certyfikatu żądać może Uczestnik wskazany w danym certyfikacie. Warunkiem przeprowadzenia tej procedury jest posiadanie ważnego certyfikatu oraz klucza prywatnego związanego z tym certyfikatem, wraz hasłem go chroniącym.

W przypadku odnawiania certyfikatu w PRU w siedzibie NBP, procedura odnowienia certyfikatu jest identyczna jak procedura stosowana w przypadku generowania pierwszego certyfikatu w NBP; w tym przypadku stosuje się przepisy rozdziału 4.1.1.

4.7.3 Przetwarzanie wniosku o odnowienie certyfikatu

Odnowienie certyfikatu Uczestnika może się odbyć na dwa sposoby:

- na komputerze w siedzibie Klienta, za pomocą SZOC. W takim przypadku w procesie identyfikacji i uwierzytelnienia wykorzystywane są aktualne klucze kryptograficzne i certyfikaty Uczestnika. Z tego względu operacja ta jest możliwa tylko w przypadku posiadania przez Uczestnika ważnego certyfikatu. SZOC dokonuje identyfikacji i uwierzytelnienia Uczestnika, a następnie generuje klucze kryptograficzne i żądanie certyfikacyjne, które przesyła bezpośrednio do CCK. Po wygenerowaniu przez CCK nowego certyfikatu, jest on przesyłany na stację roboczą Klienta, gdzie jest instalowany przez SZOC,
- w PRU w siedzibie NBP. W takim przypadku proces przebiega zgodnie z opisem zawartym w rozdziale 4.2.

4.7.4 Informowanie o wydaniu nowego certyfikatu

Identycznie jak w przypadku generowania pierwszego certyfikatu – patrz rozdział 4.3.2

4.7.5 Potwierdzenie akceptacji nowego certyfikatu

Identycznie jak w przypadku generowania pierwszego certyfikatu – patrz rozdział 4.4.1

4.7.6 Publikowanie nowego certyfikatu

Identycznie jak w przypadku generowania pierwszego certyfikatu – patrz rozdział 4.4.2

4.7.7 Informowanie o wydaniu certyfikatu innych podmiotów

Identycznie jak w przypadku generowania pierwszego certyfikatu – patrz rozdział 4.4.3

4.8 Modyfikacja certyfikatu

Każda modyfikacja certyfikatu wymaga jego odnowienia; w tym przypadku zastosowanie mają przepisy rozdziału 4.7, z zastrzeżeniem, iż odnowienie z modyfikacją certyfikatu może się odbyć za pomocą SZOC tylko w przypadku, gdy dane Uczestnika pobierane są z katalogu LDAP. W innym przypadku, odnowienie certyfikatu musi odbyć się w PRU.

4.9 Unieważnienie i zawieszenie certyfikatu

Niniejszy rozdział określa warunki, które muszą być spełnione, aby CCK miało podstawy do unieważnienia lub zawieszenia certyfikatu. Mimo, że zawieszenie certyfikatu jest szczególną formą unieważnienia, w dalszej części rozróżnić się będzie te dwa pojęcia dla podkreślenia

istotnej różnicy między nimi: **zawieszenie certyfikatu może być cofnięte, a unieważnienie certyfikatu jest ostateczne i nieodwołalne.**

Unieważnienie lub zawieszenie certyfikatu ma ściśle określony wpływ na certyfikaty oraz obowiązki posługującego się nim Użytkownika. W trakcie trwania zawieszenia lub natychmiast po unieważnieniu certyfikatu należy uznać, że stracił on ważność. Unieważnienie lub zawieszenie certyfikatu nie ma wpływu na wcześniej zaciągnięte zobowiązania lub obowiązki wynikające z przestrzegania niniejszej Polityki. Zawieszenie certyfikatu jest czasowe i trwa zwykle do czasu wyjaśnienia wątpliwości, które były podstawą do zawieszenia. Na przykład, jeśli Użytkownik straci kontrolę nad nośnikiem kluczy prywatnych, powinien natychmiast zgłosić to do PRU lub CCK, z żądaniem zawieszenia certyfikatu powiązanego z tym kluczem. W przypadku odnalezienia nośnika oraz uzyskaniu pewności, że nie zostało naruszone bezpieczeństwo klucza prywatnego, certyfikat może być, na wniosek Klienta, odwieszony, co przywróci mu stan aktywności. W przypadku unieważnienia lub zawieszenia certyfikatu, klucz prywatny powiązany z tym certyfikatem pozostający pod kontrolą Użytkownika, powinien być przez niego nadal chroniony w sposób, który gwarantuje jego wiarygodność przez cały okres zawieszenia certyfikatu oraz przechowywania go po unieważnieniu, aż do momentu fizycznego zniszczenia.

4.9.1 Okoliczności unieważnienia certyfikatu

Podstawowymi przyczynami unieważnienia certyfikatu są:

- utrata kontroli nad kluczem prywatnym powiązany z danym certyfikatem,
- naruszenie bezpieczeństwa klucza prywatnego¹,
- rażące naruszenie przez Klienta zasad Polityki,
- wymiana certyfikatu (np. w przypadku zmiany danych w nim zawartych),
- rozwiązanie Umowy pomiędzy NBP a Klientem,
- każde żądanie Uczestnika wskazanego w certyfikacie,
- każde żądanie osoby upoważnionej przez Klienta,
- każde żądanie Gestora systemu właściwego dla danego certyfikatu,
- zakończenie działalności CCK - w takim przypadku unieważnia się wszystkie certyfikaty wydane przez to CCK przed upływem deklarowanego terminu zakończenia działalności,
- kompromitacja klucza prywatnego CCK - w takim przypadku unieważnia się wszystkie certyfikaty wydane przez to CCK,
- kompromitacja algorytmu kryptograficznego lub parametrów z nim związanych, powiązanego z danym certyfikatem.

¹ Naruszenie bezpieczeństwa klucza prywatnego oznacza: (1) nieuprawniony dostęp do klucza prywatnego, (2) zagubienie klucza prywatnego, (3) kradzież klucza prywatnego, (4) przypadkowe zniszczenie klucza prywatnego.

4.9.2 Kto może żądać unieważnienia certyfikatu

Unieważnienia certyfikatu Uczestnika mogą żądać jedynie:

- Uczestnik – właściciel unieważnianego certyfikatu, lub osoba przez niego upoważniona,
- Klient lub osoba przez niego upoważniona,
- Dyrektor jednostki organizacyjnej NBP, w której zatrudniony jest Użytkownik – w przypadku gdy jest on pracownikiem NBP,
- Dyrektor jednostki organizacyjnej NBP, która podpisała umowę z firmą zatrudniającą Użytkownika,
- Gestor systemu informatycznego, na potrzeby którego wygenerowano certyfikat Uczestnika,
- Operator PRU występujący z wnioskiem w imieniu Klienta lub z własnej inicjatywy, jeśli jest w posiadaniu informacji uzasadniającej unieważnienie certyfikatu.

4.9.3 Procedura unieważniania certyfikatu

W systemie DOCert funkcjonują dwie procedury unieważniania certyfikatów.

- **Procedura standardowa** stosowana jest w przypadkach, gdy nie zachodzi potrzeba natychmiastowego unieważnienia certyfikatów Uczestnika. Procedura ta może dodatkowo obejmować generowanie nowych certyfikatów, które zastąpią certyfikaty unieważniane. W przypadku procedury standardowej Klient lub osoba przez niego upoważniona przekazuje do NBP odpowiedni wniosek, na podstawie którego Gestor lub osoba przez niego upoważniona wypełnia i przekazuje do PRU Zamówienie. W przypadku procedury standardowej we wniosku o unieważnienie certyfikatu Klient może zażądać jednocześnie wygenerowania nowych certyfikatów. Konieczne jest również, by przedstawiciel Gestora zaznaczył w Zamówieniu, iż wniosek ten dotyczy zarówno unieważnienia starych certyfikatów Uczestnika, jak i wygenerowania nowych. Dodatkowo, Klient wypełniając wniosek wskazuje termin realizacji unieważnienia. **Unieważnianie certyfikatów w ramach procedury standardowej realizowane jest jedynie w godzinach pracy PRU.**
- **Procedura awaryjna** realizowana jest w sytuacjach wymagających natychmiastowego unieważnienia wskazanego certyfikatu, np. kradzież nośnika z kluczem prywatnym Uczestnika i jest dostępna tylko dla certyfikatów wydanych dla wybranych systemów informatycznych NBP. W takim przypadku, odpowiednie zapisy zawarte są w umowie zawartej pomiędzy NBP a Klientami korzystającymi z tych systemów. Podczas wydawania certyfikatów objętych *awaryjną procedurą unieważniania* Klient otrzymuje z PRU hasło do unieważnienia certyfikatu. Hasło to ma charakter losowy i przypisane jest do konkretnego Uczestnika.

W celu dokonania awaryjnego unieważnienia certyfikatu Klient przesyła drogą mailową zgłoszenie zawierające dane certyfikatu, tzn. dane Uczestnika wskazanego w certyfikacie, a także, jeżeli jest to wymagane, rodzaj certyfikatu oraz jednorazowe hasło na adres mailowy wskazany przez PRU. Po otrzymaniu i zweryfikowaniu otrzymanego zgłoszenia, Operator PRU unieważnia certyfikaty wskazane w zgłoszeniu, publikuje nową listę CRL oraz potwierdza te zdarzenia datą i własnoręcznym podpisem złożonym na wydrukowanym zgłoszeniu. Czas realizacji zgłoszenia otrzymanego w ramach procedury awaryjnej jest każdorazowo określany w Umowach.

4.9.4 Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu

Unieważnienie certyfikatu wykonywane jest bez zbędnej zwłoki, natychmiast po przetworzeniu wniosku o unieważnienie. Nowa lista CRL publikowana jest w ciągu 1 godziny od unieważnienia certyfikatu.

4.9.5 Maksymalny dopuszczalny czas przetwarzania wniosku o unieważnienie

Wniosek o unieważnienie certyfikatu zgłoszony za pomocą procedury standardowej przetwarzany jest bez zbędnej zwłoki w dni robocze w godzinach 7.30 – 15.30. Czasy przetwarzania wniosków zgłoszonych za pomocą procedury awaryjnej określone są w Umowach.

4.9.6 Obowiązek sprawdzania list CRL przez stronę ufającą

Strona ufająca przed wykorzystaniem certyfikatu Uczestnika zobowiązana jest do sprawdzenia czy nie znajduje się on na liście certyfikatów unieważnionych. Strona ufająca powinna zawsze posiadać najbardziej aktualną listę CRL.

4.9.7 Częstotliwość publikowania list CRL

W systemie DOCert publikowane są dwa rodzaje list CRL – bieżące listy CRL i planowe listy CRL. Bieżąca lista CRL generowana jest automatycznie, najpóźniej w ciągu 1 godziny od unieważnienia certyfikatu. Planowe listy CRL generowane są raz na miesiąc.

Zarówno bieżące, jak i planowe listy CRL w polu „Następna aktualizacja” (patrz rozdział 7.2), zawierają datę publikacji następnej planowej listy CRL.

Wszystkie listy CRL systemu DOCert publikowane są automatycznie na serwerach dystrybucji certyfikatów oraz na stronie www.docert.nbp.pl.

4.9.8 Maksymalne opóźnienie w publikowaniu list CRL

Listy CRL są publikowane na serwerach dystrybucji certyfikatów oraz na stronie www.docert.nbp.pl, bezpośrednio po ich wygenerowaniu.

4.9.9 Dostępność usługi OCSP

Usługa OCSP systemu DOCert 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 DOCert 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, DB stosuje wszelkie dostępne środki w celu niezwłocznego poinformowania o tym stron ufających, odwołujących się do informacji zgromadzonej w repozytorium systemu DOCert.

W przypadku, gdy Operator PRU stwierdzi lub podejrzewa ujawnienie swojego klucza prywatnego, jest on zobowiązany do natychmiastowego zgłoszenia tych okoliczności do CCK.

W przypadku ujawnienia lub podejrzenia ujawnienia klucza prywatnego należącego do Uczestnika, jest on zobowiązany do natychmiastowego zgłoszenia okoliczności do PRU lub CCK.

4.9.13 Okoliczności zawieszenia certyfikatu

Certyfikat Uczestnika może być zawieszony w przypadku:

- podejrzenia ujawnienia klucza prywatnego,
- żądania Uczestnika wskazanego w certyfikacie,
- żądania osoby upoważnionej przez Klienta,
- żądania Gestora systemu właściwego dla danego certyfikatu,

- gdy Operator PRU otrzyma żądanie unieważnienia certyfikatu lecz nie jest w stanie zweryfikować uprawnień osoby składającej to żądanie.

4.9.14 Kto może żądać zawieszenia certyfikatu

Zawieszenia certyfikatu Uczestnika mogą żądać jedynie:

- Klient lub osoba przez niego upoważniona,
- Użytkownik – w przypadku certyfikatu wystawionego na osobę fizyczną,
- Dyrektor jednostki organizacyjnej NBP, w której zatrudniony jest Użytkownik (w przypadku Użytkowników będących pracownikami NBP),
- Dyrektor jednostki organizacyjnej NBP, która podpisała umowę z firmą zatrudniającą Użytkownika,
- Operator PRU, występujący z wnioskiem w imieniu Klienta lub z własnej inicjatywy, jeśli jest w posiadaniu informacji uzasadniającej zawieszenie certyfikatu.

4.9.15 Procedura zawieszenia i uchylecia zawieszenia certyfikatu

Procedura zawieszenia certyfikatu jest identyczna jak procedura unieważnienia i zastosowanie mają tutaj przepisy punktu 4.9.3, z tą różnicą, że we wniosku należy jasno wskazać, iż dotyczy on zawieszenia, a nie unieważnienia certyfikatu.

Uchylenie zawieszenia certyfikatu każdorazowo wymaga złożenia przez Klienta wniosku do NBP, na podstawie którego Gestor lub osoba przez niego upoważniona wypełnia i przekazuje odpowiednie Zamówienie.

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 DOCert można uzyskać w oparciu o listy CRL publikowane na serwerach dystrybucji certyfikatów (dostęp ograniczony zgodnie z zapisami rozdziału 2.4), na stronie internetowej www.docert.nbp.pl, lub usługę OCSP dostępną na stronie <http://ocsp.nbp.pl/ocsp>.

Lista CRL dostępna jest pod adresem:

- <http://www.nbp.pl/Certyfikaty/CRLcck2.crl>

4.10.2 Dostępność usługi

Usługi weryfikacji statusu certyfikatu są dostępne 24 godziny na dobę przez 7 dni w tygodniu.

4.10.3 Cechy opcjonalne

Nie dotyczy.

4.11 Zakończenie subskrypcji

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

- gdy minął okres ważności wszystkich certyfikatów Uczestnika, zaś Klient nie podjął działań mających na celu uzyskanie nowego certyfikatu,
- unieważniono certyfikaty Uczestnika i nie zostały one zastąpione przez inne certyfikaty lub certyfikat.

Po zakończeniu subskrypcji Klient zobowiązany jest do zwrotu następujących, **otrzymanych z NBP**, elementów pakietu ochrony kryptograficznej:

- kart elektronicznych wraz z oprogramowaniem do nich,
- czytników kart elektronicznych wraz z oprogramowaniem do nich,
- oprogramowania kryptograficznego (nośnik i licencja).

W przypadku niezwrócenia tych elementów lub zwrócenia uszkodzonych, Klient może być zobowiązany do uiszczenia opłaty za te elementy. Dane Uczestnika pozostają w bazie CCK przez okres ustalony z Gestorem systemu, w którym wykorzystywane były certyfikaty tego Uczestnika. Po tym okresie dane o Uczestniku i jego certyfikatach są usuwane z systemu.

4.12 Deponowanie i odtwarzanie klucza

W systemie DOCert żadne klucze prywatne nie podlegają operacji deponowania (ang. key escrow).

5. Zabezpieczenia techniczne, organizacyjne i operacyjne

W niniejszym rozdziale zawarto najważniejsze informacje dotyczące zabezpieczeń fizycznych, organizacyjnych oraz operacyjnych stosowanych w systemie DOCert, m. in. podczas generowania kluczy kryptograficznych, uwierzytelniania Użytkowników, publikacji i unieważnianiu certyfikatów, w trakcie przeprowadzania audytu, a także wykonywania kopii zapasowych i archiwalnych danych systemu.

5.1 Zabezpieczenia fizyczne

5.1.1 Lokalizacja i budynki

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

5.1.2 Dostęp fizyczny

Pomieszczenia, w których zlokalizowane są elementy systemu DOCert, objęte są systemem kontroli dostępu oraz są monitorowane 24 godziny na dobę. Dostęp do elementów systemu DOCert mają wyłącznie uprawnione osoby pełniące funkcje w systemie DOCert.

W związku z realizacją zadań określonych w umowach zawartych przez NBP, dopuszcza się pracę w systemie osób niebędących pracownikami 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 DOCert.

5.1.3 Zasilanie oraz klimatyzacja

W celu przeciwdziałania przerwaniu działalności na skutek braku energii elektrycznej lub zakłóceń w jej dopływie, system DOCert posiada dedykowany system zasilania oraz system awaryjny wyposażony w generatory prądotwórcze. Odpowiednia temperatura oraz wilgotność powietrza w pomieszczeniach obu ośrodków zapewnione są przez systemy klimatyzacji.

5.1.4 Zagrożenie powodziowe

Krytyczne elementy systemu wykorzystywanego przez system DOCert 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 DOCert, są chronione przez automatyczną instalację przeciwpożarową. W przypadku wystąpienia zagrożenia pożarowego postępuje się zgodnie z procedurami obowiązującymi w NBP.

5.1.6 Nośniki informacji

Szczegółnej kontroli, w tym ograniczeniu ruchu pomiędzy strefami bezpieczeństwa w centrach komputerowych, podlegają wszelkie urządzenia umożliwiające utwalenie 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 i archiwalnych.

5.1.7 Niszczenie zbędnych nośników informacji

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

5.1.8 Przechowywanie kopii bezpieczeństwa

Kopie bezpieczeństwa są przechowywane w zamkniętych pomieszczeniach w różnych lokalizacjach. Ośrodek zapasowy, zapewniający możliwość pełnego odtworzenia funkcjonalności systemu ośrodka podstawowego, jest dostępny dla upoważnionych osób pełniących funkcje w systemie DOCert 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 DOCert wyróżnia się następujące role:

- 1) **Administratorzy Systemu** – odpowiedzialni za administrowanie systemem operacyjnym serwerów i stacji roboczych w systemie DOCert oraz za administrowanie sprzętem,
- 2) **Operatorzy CCK** – odpowiedzialni za administrowanie oprogramowaniem CCK, za obsługę sprzętowych modułów bezpieczeństwa oraz za wykonywanie kopii zapasowych i archiwalnych,
- 3) **Operatorzy PRU** – odpowiedzialni za rejestrację i modyfikację danych Uczestników oraz za generowanie i unieważnianie certyfikatów, a także za generowanie kodów jednorazowych,
- 4) **Inspektorzy Bezpieczeństwa Systemu** – odpowiedzialni za nadzór nad przestrzeganiem procedur systemu, bieżącą kontrolę stanu i niezawodności zabezpieczeń technicznych, przegląd logów oraz za przechowywanie kart z danymi służącymi do odtworzenia klucza prywatnego CCK,
- 5) **Weryfikatorzy** – odpowiedzialni za weryfikację autentyczności przesyłek elektronicznych, zabezpieczonych z użyciem certyfikatów wydanych w systemie DOCert.

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 z częściami klucza prywatnego CCK.

Dodatkowo, wszelkie zmiany konfiguracyjne w systemie mogą być przeprowadzane jedynie pod nadzorem Inspektora Bezpieczeństwa Systemu.

5.2.3 Identyfikacja oraz uwierzytelnianie każdej roli

Osoby funkcyjne w systemie DOCert wyznaczone są decyzją Dyrektora DB - Gestora Systemu DOCert, Dyrektora DIT lub Dyrektora oddziału okręgowego NBP.

Administratorzy Systemu oraz Inspektorzy Bezpieczeństwa Systemu identyfikowani i uwierzytelniani są na podstawie loginu i hasła.

Operatorzy CCK oraz Operatorzy PRU identyfikowani i uwierzytelniani są na podstawie loginu i hasła oraz kluczy kryptograficznych i certyfikatów, znajdujących się na karcie elektronicznej zabezpieczonej PINem.

Weryfikatorzy identyfikowani są za pomocą loginu i hasła, a także za pomocą podpisu elektronicznego (stosowanego do autoryzacji ekspertyz).

5.2.4 Role, które nie mogą być łączone

Rola Administratora Systemu nie może być łączona z żadną inną. Rola Inspektora Bezpieczeństwa Systemu nie może być łączona z żadną inną. Rola Operatora CCK może być łączona tylko z rolą Operatora PRU.

5.3 Nadzorowanie personelu

5.3.1 Kwalifikacje, doświadczenie oraz upoważnienia

Osoby pełniące zaufane role w systemie DOCert są pracownikami NBP posiadającymi niezbędną wiedzę i umiejętności w zakresie: świadczenia usług związanych z podpisem elektronicznym, obsługi sprzętu i oprogramowania stosowanego do elektronicznego przetwarzania danych, automatycznego przetwarzania danych w sieciach i systemach teleinformatycznych. Osoby pełniące zaufane role w systemie DOCert są wyznaczone decyzjami Dyrektora DIT, Dyrektora DB lub Dyrektora oddziału okręgowego NBP. Wszystkie osoby pełniące zaufane role w systemie DOCert posiadają upoważnienia do przetwarzania danych osobowych.

5.3.2 Procedury weryfikacji przygotowania

Zgodnie z zasadami zatrudniania pracowników w NBP.

5.3.3 Szkolenie

Zgodnie z odrębnymi przepisami, osoby pełniące zaufane role w systemie DOCert odbywają szkolenia związane z obsługą tego systemu, a w szczególności:

- zapoznają się z polityką certyfikacji oraz z dokumentacją i procedurami systemu;
- uczestniczą w szkoleniach z zakresu administrowania systemami operacyjnymi zainstalowanymi na serwerach i stacjach roboczych systemu DOCert;
- uczestniczą w szkoleniach z zakresu administrowania i obsługi aplikacji wykorzystywanych przez CCK i PRU;
- uczestniczą w szkoleniach dotyczących kryptografii, infrastruktury klucza publicznego oraz podpisu elektronicznego.

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 DOCert są dokumentowane i nadzorowane. Umożliwia to w szczególności wykrycie ewentualnych nieuprawnionych działań osób pełniących zaufane role w systemie DOCert.

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

5.3.7 Pracownicy kontraktowi

Zgodnie z ogólnymi zasadami dotyczącymi pracowników kontraktowych, obowiązującymi w NBP.

5.3.8 Dokumentacja przekazana pracownikom

Osoby funkcyjne w systemie DOCert muszą mieć dostęp do następujących dokumentów:

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

5.4 Procedury rejestrowania zdarzeń oraz audytu

W systemie DOCert rejestrowane są wszystkie istotne zdarzenia, które mogą mieć wpływ na bezpieczeństwo i funkcjonowanie systemu. Zarejestrowane zdarzenia są archiwizowane.

5.4.1 Typy rejestrowanych zdarzeń

W systemie DOCert rejestrowane są zdarzenia:

- związane z użyciem klucza prywatnego CCK (zapisywane w wewnętrznym rejestrze sprzętowego modułu bezpieczeństwa),
- związane z aplikacjami wykorzystywanymi przez CCK, PRU oraz serwery dystrybucji certyfikatów (zapisywane w logach tych aplikacji),
- związane z systemem operacyjnym (zapisywane w dziennikach zdarzeń systemu operacyjnego oraz w zewnętrznym systemie informatycznym),
- związane z przetwarzaniem danych osobowych.

Dodatkowo, zewnętrzny system na bieżąco monitoruje stan serwerów dystrybucji certyfikatów. W przypadku gdy którykolwiek z serwerów przestaje być dostępny, system powiadamia (drogą mailową) Operatorów CCK.

5.4.2 Częstotliwość przetwarzania zapisów rejestrowanych zdarzeń

Na serwerach DOCert zainstalowane jest oprogramowanie monitorujące, które na bieżąco sprawdza stan systemu operacyjnego oraz usług związanych z pracą CCK i w razie wystąpienia incydentu generuje raporty i powiadomienia dla Administratorów Systemu oraz Operatorów CCK.

Administratorzy Systemu oraz Operatorzy CCK na bieżąco analizują otrzymywane raporty i w razie potrzeby przeglądają logi bezpośrednio na serwerze.

5.4.3 Okres przechowywania zapisów rejestrowanych zdarzeń

Kopie archiwalne zawierające zapisy rejestrowanych zdarzeń przechowywane są przez okres 5 lat.

5.4.4 Ochrona zapisów rejestrowanych zdarzeń

Tylko Administratorzy Systemu oraz Operatorzy CCK posiadają dostęp do zapisów rejestrowanych zdarzeń. Kopie archiwalne zawierające zapisy rejestrowanych zdarzeń przechowywane są w pomieszczeniach objętych systemem kontroli dostępu i znajdują się w szafie metalowej zamykanej na klucz.

5.4.5 Procedury tworzenia kopii zapisów rejestrowanych zdarzeń

Kopie archiwalne zapisów rejestrowanych zdarzeń wykonywane są przez Operatorów CCK zgodnie z procedurami systemu DOCert raz w miesiącu, a kopie zapasowe, zawierające zapisy zdarzeń związanych z aplikacją CCK, wykonywane są codziennie.

5.4.6 System gromadzenia zapisów rejestrowanych zdarzeń (wewnętrzny a zewnętrzny)

Zapisy rejestrowanych zdarzeń są gromadzone lokalnie przez system operacyjny serwerów CCK oraz przez aplikacje wykorzystywane przez CCK, PRU oraz serwery dystrybucji certyfikatów.

5.4.7 Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenie

System monitorujący prawidłowe działanie serwerów dystrybucji certyfikatów automatycznie, za pomocą poczty elektronicznej, powiadamia Operatorów CCK w przypadku wykrycia błędów w działaniu tych serwerów.

5.4.8 Oszacowanie podatności na zagrożenia

System DOCert podlega bieżącej kontroli Inspektora Bezpieczeństwa Systemu. Dodatkowo, Inspektor Bezpieczeństwa Systemu wykonuje okresowe analizy ryzyka, nie rzadziej niż raz na 24 miesiące, oraz w przypadku dokonywania znaczących zmian w systemie, które pozwalają na określenie podatności na zagrożenia. System DOCert podlega także okresowym audytom wykonywanym przez pracowników Departament Audytu Wewnętrznego lub przez audytorów zewnętrznych.

5.5 Zapisy archiwalne

5.5.1 Rodzaje archiwizowanych danych

W systemie DOCert raz w miesiącu tworzone są kopie archiwalne zawierające:

- Bazę certyfikatów i list CRL,
- Zapisy logów aplikacji CCK,
- Zapisy logów systemu operacyjnego serwera CCK.

Dodatkowo, archiwizacji podlegają także dokumenty papierowe związane z pracą PRU, dotyczące rejestracji i wydawania certyfikatów Uczestników, tj.:

- „Zamówienie na usługę kryptograficzną”,
- „Protokół przekazania kluczy kryptograficznych”,
- „Protokół przekazania elementów pakietu ochrony kryptograficznej”.

5.5.2 Okres przechowywania archiwum

Kopie archiwalne przechowywane są co najmniej przez okres 5 lat.

5.5.3 Ochrona archiwum

Nośniki elektroniczne zawierające kopie archiwalne przechowywane są w pomieszczeniach chronionych systemem kontroli dostępu. Dodatkowo umieszczone są w szafie pancerniej zamykanej na klucz i o odporności ogniowej 120 min.

5.5.4 Procedury tworzenia kopii archiwalnych

Kopie archiwalne wykonywane są przez Operatorów CCK zgodnie z wewnętrznymi procedurami obowiązującymi w NBP. Procedury systemu DOCert podlegają okresowemu przeglądowi i w razie potrzeby są aktualizowane.

5.5.5 Wymaganie znakowania czasem kopii archiwalnych

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

5.5.6 Kopie archiwalne rejestrów zdarzeń (system wewnętrzny i zewnętrzny)

Kopie archiwalne są wykonywane ręcznie przez Operatorów CCK i zapisywane na zewnętrznych nośnikach danych.

5.5.7 Procedury dostępu oraz weryfikacji zarchiwizowanej informacji

Dostęp do zarchiwizowanych danych mają tylko osoby upoważnione. Nośniki zawierające kopie archiwalne podlegają okresowej weryfikacji wykonywanej przez Operatorów CCK.

5.6 Zmiana klucza

W systemie DOCert wymiana klucza CCK odbywa się najpóźniej na pięć lat przed wygaśnięciem autocertyfikatu CCK. Najpóźniej 6 miesięcy przed wymianą kluczy CCK, DB jest zobowiązany do poinformowania o tym DIT oraz Gestorów systemów informatycznych NBP, wykorzystujących certyfikaty systemu DOCert. DIT wspólnie z DB, przeprowadza konieczne testy w wymienionych systemach oraz informuje Gestorów o ich wyniku.

Po wygenerowaniu nowych kluczy kryptograficznych CCK, generowany jest nowy autocertyfikat z identycznym identyfikatorem wyróżniającym oraz certyfikaty zakładkowe, dzięki którym możliwe jest zbudowanie relacji zaufania pomiędzy kluczami kryptograficznymi CCK.

Nowy autocertyfikat CCK oraz certyfikaty zakładkowe, niezwłocznie po ich wygenerowaniu, publikowane są w repozytorium oraz przekazywane są do Klientów.

W przypadku dokonywania znaczących zmian w konfiguracji CCK, takich jak np. zmiana algorytmów kryptograficznych, może zostać podjęta decyzja o zmianie kluczy

kryptograficznych, połączonej ze zmianą identyfikatora wyróżniającego CCK. W takim przypadku w systemie DOCert zostaje uruchomione drugie, niezależne CCK i do czasu wygaśnięcia autocertyfikatu „starego” CCK funkcjonują dwa CCK, posługujące się różnymi kluczami kryptograficznymi i różnymi nazwami.

Przed wprowadzeniem nowych algorytmów kryptograficznych w systemie DOCert, DB jest zobowiązany do poinformowania o tym DIT oraz Gestorów, a także do przeprowadzenia, wspólnie z DIT, testów pozwalających na określenie, czy wszystkie systemy informatyczne NBP, korzystające z certyfikatów systemu DOCert, będą prawidłowo obsługiwać nowe algorytmy kryptograficzne. Dopiero po uzyskaniu pewności, iż nowe algorytmy będą prawidłowo obsługiwane, możliwe jest wprowadzenie zmian w systemie DOCert.

5.7 Naruszenie ochrony klucza i uruchamianie po awariach oraz kłękach żywiołowych

5.7.1 Procedury obsługi incydentów i reagowania na nie

Realizowane są zgodnie z obowiązującymi w NBP wewnętrznymi przepisami dotyczącymi obsługi incydentów oraz z odpowiednimi zapisami w umowach zawartych przez NBP z firmami zewnętrznymi, świadczącymi usługi wsparcia i serwisu oprogramowania oraz sprzętu wykorzystywanego w systemie DOCert.

5.7.2 Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych

Elementy systemu DOCert znajdują się w dwóch, odległych od siebie lokalizacjach. Dane systemu są na bieżąco kopiowane (replikowane) z ośrodka podstawowego do ośrodka zapasowego. Dodatkowo, w ośrodku podstawowym istnieje możliwość uruchomienia serwera rezerwowego w przypadku uszkodzenia serwera podstawowego.

W przypadku uszkodzenia urządzeń HSM, dostarczenie zapasowych urządzeń jest zapewnione przez odpowiednie zapisy w umowach serwisowych/wsparcia, zawartych przez NBP z firmami zewnętrznymi.

Kopie zapasowe danych oraz karty potrzebne do wczytania klucza prywatnego CCK przechowywane są w obu lokalizacjach.

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

Na wypadek sytuacji ujawnienia klucza prywatnego Operatora PRU przyjęto następującą procedurę:

- CCK unieważnia certyfikat powiązany z ujawnionym kluczem prywatnym,
- dokonywana jest analiza zapisów CCK w celu ustalenia, czy ujawniony klucz prywatny Operatora PRU był wykorzystany w okresie pomiędzy momentem jego ujawnienia a unieważnieniem,
- w przypadku, gdy został on w tym okresie bezprawnie użyty do wystawienia certyfikatów – certyfikaty te także zostają unieważnione.

Na wypadek sytuacji ujawnienia klucza prywatnego CCK przyjęto następującą procedurę:

- CCK unieważnia wszystkie certyfikaty podpisane ujawnionym kluczem prywatnym, a następnie publikuje nową listę CRL,
- informacja o unieważnieniu zostaje niezwłocznie przekazana wszystkim Klientom, stronom ufającym oraz Gestorom systemów informatycznych NBP, korzystających z certyfikatów systemu DOCert. Odpowiednie informacje zostają także opublikowane w repozytorium opisanym w rozdziale 2.
- zostają wygenerowane nowe klucze kryptograficzne CCK oraz nowy autocertyfikat, przy czym identyfikator wyróżniający może, lecz nie musi, pozostać bez zmian, oraz przystępuje się do wymiany kluczy kryptograficznych i certyfikatów Uczestników,
- tryb wymiany kluczy kryptograficznych i certyfikatów Uczestników jest określany osobno dla każdego systemu informatycznego NBP, wykorzystującego certyfikaty systemu DOCert. Decyzję dotyczącą trybu podejmuje Dyrektor DB wspólnie z Gestorem danego systemu informatycznego oraz Dyrektorem DIT.

Ze względu na to, iż ujawnienie klucza prywatnego CCK, skutkujące koniecznością unieważnienia wszystkich certyfikatów w systemie DOCert, może uniemożliwić funkcjonowanie systemów informatycznych NBP, wykorzystujących te certyfikaty, NBP stosuje zabezpieczenia techniczne, informatyczne oraz proceduralne, które mają na celu zapewnienie maksymalnej ochrony klucza prywatnego CCK i minimalizację ewentualnych strat.

5.7.4 Zapewnienie ciągłości działania po katastrofach

Elementy systemu DOCert znajdują się w dwóch, odległych od siebie ośrodkach obliczeniowych. Dane z ośrodka podstawowego są na bieżąco replikowane do ośrodka zapasowego. Każdy z ośrodków obliczeniowych systemu DOCert obsługiwany jest przez innych pracowników, co sprawia, iż w przypadku katastrofy przywrócenie pracy systemu DOCert nie wymaga przejazdu pracowników NBP do ośrodka zapasowego.

Dodatkowo, system DOCert objęty jest Planem Ciągłości Działania PCD-NBP, określającym procedury mające na celu zapewnienie działania systemu po katastrofach oraz minimalizującym czas potrzebny na przywrócenie prawidłowego działania.

5.8 Zakończenie działalności CCK lub PRU

5.8.1 CCK

Certyfikaty systemu DOCert wydawane są na potrzeby systemów informatycznych NBP. Zakończenie działalności Centrum Certyfikacji Kluczy możliwe jest dopiero po ustaleniu przez Dyrektora DB, z departamentami odpowiedzialnymi merytorycznie za funkcjonowanie tych systemów, sposobu przeprowadzenia tej procedury. W przypadku planowania zakończenia działalności Centrum Certyfikacji Kluczy możliwe są trzy rozwiązania:

- 1) uruchomienie nowego Centrum Certyfikacji Kluczy w ramach systemu DOCert, które przejmie zadania Centrum Certyfikacji Kluczy kończącego działalność;
- 2) podpisanie umowy z zewnętrznym Centrum Certyfikacji Kluczy, które zapewni obsługę kryptograficzną Uczestników;
- 3) rezygnacja ze stosowania kryptograficznej ochrony informacji w systemach informatycznych NBP.

W momencie zakończenia działalności Centrum Certyfikacji Kluczy zobowiązane jest do:

- 1) unieważnienia wszystkich certyfikatów, które pozostały aktywne, niezależnie od tego, czy Klient złożył wniosek o unieważnienie czy nie;
- 2) powiadomienia wszystkich Klientów, Punktów Rejestracji Użytkowników oraz departamentów odpowiedzialnych merytorycznie za funkcjonowanie systemów informatycznych NBP, wykorzystujących certyfikaty systemu DOCert, o zakończeniu swojej działalności.

Po podjęciu decyzji dotyczącej wyboru rozwiązania, Centrum Certyfikacji Kluczy zobowiązane jest do powiadomienia, co najmniej na 90 dni przed zakończeniem działalności, wszystkich Uczestników, którzy posiadają jeszcze ważny certyfikat wydany przez Centrum Certyfikacji Kluczy, o zamiarze zakończenia działalności oraz o dalszych czynnościach, które Klienci powinni w związku z tym podjąć.

5.8.2 PRU

Najpóźniej na 90 dni przed planowanym zakończeniem działalności, Punkt Rejestracji Użytkowników ma obowiązek poinformowania o tym Centrum Certyfikacji Kluczy.

Następnie podejmowana jest decyzja o przeniesieniu obowiązków likwidowanego Punktu Rejestracji Użytkowników do innego Punktu Rejestracji Użytkowników.

Po podjęciu decyzji o zmianie Punktu Rejestracji Użytkowników, Dyrektor DB informuje o tym departamenty odpowiedzialne merytorycznie za funkcjonowanie systemów informatycznych obsługiwanych przez kończący działalność Punkt Rejestracji Użytkowników.

Niezwłocznie po zakończeniu działalności, likwidowany Punkt Rejestracji Użytkowników ma obowiązek przekazania dokumentacji, dotyczącej Uczestników, do Punktu Rejestracji Użytkowników przejmującego jego zdania.

6 Procedury bezpieczeństwa technicznego

6.1 Generowanie pary kluczy i jej instalowanie

6.1.1 Generowanie pary kluczy

Klucze kryptograficzne urzędu CCK NBP generowane są przez Operatorów CCK w sprzętowych modułach bezpieczeństwa.

Operatorzy PRU generują osobiście swoje klucze kryptograficzne, a następnie przekazują klucze publiczne Operatorom CCK w celu ich certyfikacji.

Klucze kryptograficzne Uczestników generowane są w PRU, na wydzielonej do tego celu stacji, przez Użytkownika, na nośniku elektronicznym przekazanym przez PRU lub dostarczonym przez Użytkownika.

Podczas generowania kluczy kryptograficznych Użytkownik sam ustala hasła zabezpieczające klucz prywatny, znajdujący się na nośniku. Od momentu wygenerowania, za bezpieczeństwo klucza prywatnego oraz chroniącego go hasła odpowiada Użytkownik. Operator PRU nigdy nie ma bezpośredniej styczności z kluczem prywatnym Uczestnika.

W przypadku wykorzystania SZOC, dostępnego na stronie www.docert.nbp.pl, klucze kryptograficzne generowane są bezpośrednio na stacji roboczej Klienta. Klucz publiczny za pomocą SZOC przesyłany jest automatycznie do CCK w celu jego certyfikacji.

6.1.2 Przekazywanie klucza prywatnego Użytkownikowi

Nie dotyczy, gdyż klucze kryptograficzne generowane są przez Użytkownika w PRU na wydzielonej do tego celu stacji roboczej lub bezpośrednio na stacji roboczej Klienta.

6.1.3 Dostarczanie klucza publicznego do wystawcy

W przypadku generowania kluczy kryptograficznych w PRU, klucze publiczne przenoszone są pomiędzy stacją do generowania kluczy a stanowiskiem PRU za pomocą zewnętrznego nośnika elektronicznego. Na stanowisku PRU Operator wczytuje żądanie certyfikacyjne z nośnika, a następnie podpisuje je swoim kluczem prywatnym i przesyła do CCK.

W przypadku wykorzystania SZOC klucze publiczne przekazywane są do CCK automatycznie, z wykorzystaniem kluczy kryptograficznych i certyfikatów przypisanych do SZOC.

6.1.4 Przekazywanie klucza publicznego CCK

Klucze publiczne CCK przekazywane są Użytkownikowi na nośniku elektronicznym wraz z wygenerowanymi dla niego certyfikatami. Dodatkowo klucze publiczne CCK dostępne są w repozytorium (patrz rozdział 2.1), a w szczególnych przypadkach mogą być dostarczone do Klienta drogą mailową.

W trakcie generowania kluczy kryptograficznych i certyfikatów za pomocą SZOC, klucze publiczne CCK są automatycznie instalowane na stacji roboczej Klienta.

6.1.5 Długości kluczy

Klucze kryptograficzne CCK mają długość 4096 bitów. Minimalna długość kluczy kryptograficznych Uczestników to 2048 bitów.

6.1.6 Parametry generowania klucza publicznego oraz weryfikacja jakości

Klucze publiczne są kodowane zgodnie z RFC 3280 i PKCS#1. Wszystkie generowane klucze są kluczami algorytmu RSA. Podczas generowania w PRU kluczy kryptograficznych Uczestników, do uzyskania ziarna losowego używany jest mechanizm wykorzystujący zjawiska fizyczne.

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

Akceptowane zastosowanie kluczy Uczestników opisane jest w odpowiednich Umowach. Klucze kryptograficzne CCK 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

Wszystkie operacje związane z zarządzaniem modułami kryptograficznymi, w tym operacje związane z kluczami kryptograficznymi zapisanymi na nich, wymagają użycia kart procesorowych będących w posiadaniu Operatorów CCK. Klucze prywatne CCK w formie jawnej występują jedynie wewnątrz sprzętowych modułów bezpieczeństwa; wszystkie

operacje wymagające użycia klucza prywatnego CCK, w szczególności podpisywanie certyfikatów, następują wewnątrz tych modułów.

6.2.2 Podział klucza prywatnego na części

Klucze prywatne CCK podlegają ochronie za pomocą tzw. pośredniego schematu podziału klucza na części. W schemacie tym podziałowi podlega klucz symetryczny użyty do zaszyfrowania klucza prywatnego CCK. Klucz symetryczny podzielony jest na 9 części zapisanych na kartach elektronicznych zabezpieczonych PINami i przekazanych Operatorom CCK. Do odtworzenia klucza konieczne jest użycie przynajmniej dwóch takich kart i możliwe jest to jedynie wewnątrz urządzenia HSM.

6.2.3 Deponowanie klucza prywatnego

Żadne klucze prywatne w systemie DOCert nie podlegają operacji deponowania.

6.2.4 Kopie zapasowe klucza prywatnego

Nie dotyczy.

6.2.5 Archiwizowanie klucza prywatnego

Klucze prywatne CCK ani klucze prywatne Uczestników nie są archiwizowane. Karty z częściami klucza prywatnego CCK są niszczone po wygaśnięciu autocertyfikatu CCK, powiązanego z tym kluczem.

6.2.6 Wprowadzenie lub pobieranie klucza prywatnego do/z modułu kryptograficznego

Klucze prywatne CCK poza modułem kryptograficznym 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 CCK 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 CCK 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 CCK 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).

Klucze prywatne Operatorów PRU są aktywowane po uwierzytelnieniu operatora poprzez podanie PINu i tylko na czas wykonania pojedynczej operacji kryptograficznej z użyciem tego klucza. Po zakończeniu wykonywania operacji klucz prywatny jest automatycznie dezaktywowany i musi być ponownie uaktywniony przed wykonaniem kolejnej operacji.

Aktywacja kluczy prywatnych Uczestników zależy od zastosowanego nośnika kluczy kryptograficznych. W przypadku zastosowania kart elektronicznych, klucz prywatny jest aktywowany po uwierzytelnieniu Użytkownika poprzez podanie PINu. Klucz prywatny może być aktywny tylko na czas wykonania pojedynczej operacji bądź przez ustalony okres czasu.

W przypadku gdy klucze kryptograficzne zapisywane są w postaci plików PKCS#12 - pliki z rozszerzeniem .pfx, lub .p12 - metoda aktywacji klucza prywatnego zależy od konfiguracji systemu operacyjnego i stosowanego oprogramowania. W szczególności możliwa jest automatyczna aktywacja klucza prywatnego przez system operacyjny lub np. przez przeglądarkę internetową. W takim przypadku hasło chroniące plik PKCS#12 wykorzystywane jest jedynie przy instalacji kluczy kryptograficznych i certyfikatów Uczestnika w systemie operacyjnym.

6.2.9 Metoda dezaktywacji klucza prywatnego

Dezaktywacja klucza prywatnego CCK możliwa jest poprzez wyłączenie modułu kryptograficznego.

Metoda dezaktywacji klucza prywatnego Uczestnika zależy od nośnika tego klucza oraz od konfiguracji aplikacji wykorzystującej ten klucz.

6.2.10 Metoda niszczenia klucza prywatnego

Niszczenie kluczy prywatnych Uczestników lub operatorów PRU polega na ich bezpiecznym usunięciu z nośnika kluczy lub zniszczeniu tego nośnika.

Niszczenie klucza prywatnego CCK wykonuje się poprzez oprogramowanie dołączone do modułu kryptograficznego. W przypadku bezpośredniego zagrożenia bezpieczeństwa klucza prywatnego CCK możliwe jest zastosowanie „przycisku samobójcy”, znajdującego się na przednim panelu modułu. „Przycisk samobójcy” służy do natychmiastowego wyczyszczenia pamięci modułu kryptograficznego.

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 Uczestników przechowywane są w bazie CCK przez cały okres subskrypcji, a także przez ustaloną liczbę lat po jego zakończeniu, przy czym okres ten zależy od systemu informatycznego, na potrzeby którego wygenerowano klucze Uczestnika i jest każdorazowo ustalany z Gestorem danego systemu.

Dodatkowo klucze publiczne Uczestników przechowywane są na nośnikach zawierających kopie archiwalne, z których usuwane są po 5 latach od zakończenia subskrypcji. Klucze publiczne CCK nie są usuwane ani z systemu, ani z kopii archiwalnych.

6.3.2 Okresy stosowania klucza publicznego i prywatnego

Okres życia klucza publicznego określony jest przez pole *validity* każdego certyfikatu klucza publicznego (patrz rozdział 7.1). Okres ważności klucza prywatnego może być krótszy niż okres ważności certyfikatu. Wynika to z możliwości zaprzestania używania klucza w dowolnym momencie (np. w przypadku wymiany autocertyfikatu CCK). Okresy stosowania kluczy kryptograficznych Uczestników zależą od systemu, na potrzeby którego te klucze zostały wygenerowane.

Okresy stosowania kluczy CCK przedstawione są w poniższej tabeli:

Okresy stosowania kluczy CCK

Nazwa CCK	Typ klucza	Okres stosowania
NBP CCK 2	Publiczny	20 lat
NBP CCK 2	Prywatny	15 lat

6.4 Dane aktywujące

Dane aktywujące stosowane są do uaktywniania kluczy prywatnych Uczestników, Operatorów PRU oraz Operatorów CCK. Najczęściej używane są na etapie uwierzytelnienia podmiotu i kontroli dostępu do klucza prywatnego.

W przypadku części kart elektronicznych, stosowanych w systemie DOCert, występują dwa rodzaje danych aktywujących – kody PIN służące do uwierzytelniania i pozwalające na użycie klucza prywatnego oraz kody PUK pozwalające na zarządzanie kartą w szczególności na zmianę kodów PIN oraz na odblokowanie karty elektronicznej. Opisane poniżej zasady są stosowane dla obu rodzajów danych aktywujących.

6.4.1 Generowanie danych aktywujących i ich instalowanie

Dane aktywujące używane są w dwóch podstawowych przypadkach:

- jako element jedno - lub dwuczynnikowej procedury uwierzytelniania (hasła, PINy),
- jako część sekretu współdzielonego, który po zainstalowaniu w systemie umożliwia odtworzenie klucza prywatnego CCK.

Dane aktywujące klucz prywatny Uczestnika (kody PIN) ustalane są przez Użytkownika w trakcie generowania kluczy kryptograficznych. W przypadku, gdy nośnik kluczy kryptograficznych umożliwia zmianę danych aktywujących, Użytkownik, CCK ani PRU nie przechowują kopii tych danych, aktywujących klucze prywatne Uczestników.

Kod PUK ustalany jest przez PRU i przekazywany Użytkownikowi, który nie powinien go zmieniać. Operator PRU zna algorytm wyliczania kodu PUK i dzięki temu może on odblokować kartę w przypadku, gdy Użytkownik zapomni kodu PUK.

W przypadku, gdy Użytkownik zmieni kod PUK, musi go podać Operatorowi PRU w momencie dokonywania zwrotu karty elektronicznej. W przeciwnym przypadku Klient uiszcza opłatę zgodnie z taryfą opłat i prowizji, obowiązującą w NBP.

Sekrety współdzielone używane do ochrony kluczy prywatnych CCK generowane są zgodnie z wymaganiami określonymi w rozdziale 6.2 i zapisywane na specjalnych kartach elektronicznych. Karty te chronione są numerem PIN, ustalonym przez Operatora CCK. Sekrety współdzielone stają się danymi aktywacyjnymi dopiero po ich uaktywnieniu, tj. po umieszczeniu ich w module kryptograficznym i prawidłowym podaniu numeru PIN, chroniącego daną kartę.

6.4.2 Ochrona danych aktywujących

Uczestnik, podczas generowania kluczy kryptograficznych, otrzymuje materiały do zapisania danych aktywujących. Dodatkowo otrzymuje od PRU informację o konieczności bezpiecznego przechowywania zapisanych danych aktywujących.

Karty elektroniczne wykorzystywane jako nośnik kluczy kryptograficznych w systemie DOCert ulegają zablokowaniu po kilkukrotnym wprowadzeniu błędnych danych aktywujących (liczba możliwych prób jest zależna od typu karty).

Kody PUK, znane Operatorom PRU, nie są zapisywane w PRU. Każdy Operator PRU posiada aplikację służącą do wyliczania kodu PUK dla konkretnej karty. Kod PUK zależy od numeru karty, a także od hasła danego PRU.

6.4.3 Inne problemy związane z danymi aktywującymi

Dane aktywujące powinny być przechowywane tylko w jednej kopii i nigdy razem z nośnikiem kluczy kryptograficznych, chronionym tymi danymi.

6.5 Nadzorowanie bezpieczeństwa systemu komputerowego

Wszystkie elementy systemu DOCert chronione są zgodnie z przepisami prawa powszechnie obowiązującego, wewnętrznymi regulacjami NBP, w szczególności zgodnie z przepisami dotyczącymi polityki bezpieczeństwa w NBP oraz zarządzania bezpieczeństwem systemów informatycznych w NBP. Wszystkie elementy systemu DOCert objęte są ochroną antywirusową.

6.5.1 Wymagania techniczne dotyczące specyficznych zabezpieczeń systemów komputerowych

Zgodnie z przepisami prawa powszechnie obowiązującego i wewnętrznymi regulacjami NBP, w tym dotyczącymi polityki bezpieczeństwa w NBP oraz zarządzania bezpieczeństwem systemów informatycznych w NBP.

6.5.2 Ocena bezpieczeństwa systemów komputerowych

Zgodnie z przepisami prawa powszechnie obowiązującego i wewnętrznymi regulacjami NBP, w tym dotyczącymi polityki bezpieczeństwa w NBP oraz zarządzania bezpieczeństwem systemów informatycznych w NBP.

6.6 Cykl życia zabezpieczeń technicznych

Zgodnie z przepisami prawa powszechnie obowiązującego i wewnętrznymi regulacjami NBP, w tym dotyczącymi polityki bezpieczeństwa w NBP oraz zarządzania bezpieczeństwem systemów informatycznych w NBP.

6.6.1 Nadzorowanie rozwoju systemu

Zgodnie z wewnętrznymi regulacjami NBP dotyczącymi zarządzania bezpieczeństwem systemów informatycznych w NBP.

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

Oprogramowanie systemu DOCert jest systematycznie aktualizowane i w razie potrzeby podnoszone do najnowszych wersji. Przed dokonaniem zmian w systemie przeprowadzane są testy mające na celu potwierdzenie prawidłowej współpracy nowej wersji oprogramowania z innymi elementami systemu DOCert oraz z innymi systemami wykorzystującymi klucze kryptograficzne i certyfikaty.

6.6.2 Nadzorowanie zarządzania bezpieczeństwem

Zgodnie z przepisami prawa powszechnie obowiązującego i wewnętrznymi regulacjami NBP, w tym dotyczącymi polityki bezpieczeństwa w NBP oraz zarządzania bezpieczeństwem systemów informatycznych w NBP.

6.6.3 Nadzorowanie cyklu życia zabezpieczeń

Niniejsza Polityka nie określa żadnych wymagań w tym zakresie.

6.7 Nadzorowanie zabezpieczeń sieci komputerowej

Zgodnie z przepisami prawa powszechnie obowiązującego i wewnętrznymi regulacjami NBP, w tym dotyczącymi polityki bezpieczeństwa w NBP oraz zarządzania bezpieczeństwem systemów informatycznych w NBP.

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 DOCert 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 Uczestnika,
- 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 DOCert

Nazwa Pola		Zawartość Pola
Wersja	V3	
Numer Seryjny	Unikalny w ramach CCK numer seryjny certyfikatu	
Algorytm Podpisu	sha256RSA	
Wystawca	Nazwa powszechna (CN)	NBP CCK 2

Jednostka Organizacyjna (OU)	Centrum Certyfikacji Kluczy NBP
Organizacja (O)	Narodowy Bank Polski
Miejscowość (L)	Warszawa
Kraj (C)	PL

Ważny od Podstawowy czas według UTC (Universal Time Coordinated)

Ważny do Podstawowy czas według UTC (Universal Time Coordinated)

Podmiot Identyfikator wyróżniający Uczestnika zgodny z wymaganiami X.501. Zawartość tego pola jest ustalana osobno dla każdego systemu informatycznego

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 DOCert są zgodne z X.509 v3.

7.1.2 Rozszerzenia certyfikatów

Certyfikaty systemu DOCert zawierają dwa rodzaje rozszerzeń. Rozszerzenie krytyczne jest rozszerzeniem, które nie może być zignorowane przez aplikację wykorzystującą dany certyfikat. Jeżeli aplikacja nie jest w stanie rozpoznać jakiegokolwiek rozszerzenia krytycznego, zawartego w certyfikacie, odrzuca ten certyfikat. Rozszerzenie niekrytyczne ma bardziej charakter „informacyjny” i może być zignorowane.

Certyfikaty wystawiane w systemie DOCert zawierają następujące rozszerzenia:

- Użycie klucza
- Identyfikator klucza urzędu
- Punkty dystrybucji list CRL
- Podstawowe warunki ograniczające (**rozszerzenie krytyczne**)

Powyższa lista nie jest listą zamkniętą i na prośbę Gestorów systemów informatycznych NBP, wykorzystujących klucze kryptograficzne i certyfikaty systemu DOCert, może być rozszerzona. Każda zmiana profilu certyfikatu (w tym dodanie rozszerzeń) musi być poprzedzona testami i uzyskać akceptację Dyrektora DB, jako Gestora Systemu DOCert.

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 DOCert:

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

7.1.4 Format nazw

Zawartość identyfikatora wyróżniającego Uczestnika jest ustalana z Gestorem systemu informatycznego, na potrzeby którego generowany jest certyfikat.

7.1.5 Ograniczenia nakładane na nazwy

Zawartość identyfikatora wyróżniającego Uczestnika jest ustalana z Gestorem systemu informatycznego, na potrzeby którego generowany jest certyfikat.

7.1.6 Identyfikatory polityk certyfikacji

Certyfikaty wydane w systemie DOCert posiadają następujący identyfikator polityki certyfikacji: od 1.3.6.1.4.1.31995.2.1.x gdzie x oznacza wersję polityki certyfikacji.

7.1.7 Stosowanie rozszerzenia określającego ograniczenia nakładane na politykę certyfikacji

Nie dotyczy.

7.1.8 Składnia i semantyka kwalifikatorów polityki certyfikacji

Rozszerzenie „Zasady aplikacji” zawarte w certyfikacie zawiera adres URL, wskazujący politykę certyfikacji związaną z danym certyfikatem.

7.1.9 Przetwarzanie semantyki krytycznych rozszerzeń polityki certyfikacji

Dla zapewnienia maksymalnej kompatybilności 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 CCK 2
	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 odwołań	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

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

7.2.1 Numer wersji

Listy CRL wydawane w systemie DOCert są zgodne z X.509 v2.

7.2.3 Rozszerzenia CRL oraz rozszerzenia dostępu do CRL

W systemie DOCert występują dwa rozszerzenia listy CRL.

- Pierwsze z nich to pole „Identyfikator klucza urzędu”, które umożliwia identyfikację klucza publicznego, odpowiadającego kluczowi prywatnemu, zastosowanemu do podpisania danej listy CRL,
- Drugie rozszerzenie to „numer listy CRL”, zawierające monotonicznie zwiększany numer listy CRL, wydawanej przez dane CCK. Rozszerzenie „numer listy CRL” pozwala określić, kiedy jakiś CRL zastąpił inny CRL.

7.2.4 Rozszerzenia dostępu do CRL

Oprócz rozszerzeń CRL w systemie DOCert mogą być stosowane trzy rozszerzenia dostępu do CRL.

7.2.4.1 Kod przyczyny listy CRL

Rozszerzenie „Kod przyczyny listy CRL” pozwala na umieszczenie dodatkowych informacji dotyczących przyczyny unieważnienia danego certyfikatu. W systemie DOCert dopuszcza się następujące przyczyny unieważnienia:

- Nieokreślona (0)
- Złamanie klucza (1)
- Złamanie klucza urzędu (2)
- Zmiana przynależności (3)
- Zastąpienie nowszą wersją (4)
- Zaprzestanie działania (5)
- Wstrzymanie² certyfikatu (6)
- Anulowanie uprawnień zawartych w certyfikacie (9)³

7.2.4.2 Data złamania klucza

Rozszerzenie „Data złamania klucza” pojawia się jedynie w przypadku, gdy w rozszerzeniu „Kod przyczyny listy CRL” wpisano „1” lub „2”, czyli „Złamanie klucza” lub „Złamanie klucza urzędu”. Rozszerzenie to pozwala na umieszczenie informacji o dacie złamania klucza prywatnego Uczestnika lub CCK.

7.2.4.3 Postępowanie po napotkaniu zawieszenia certyfikatu

Ostatnie rozszerzenie „Postępowanie po napotkaniu zawieszenia certyfikatu” określa czynności, które powinny zostać wykonane po napotkaniu na liście CRL certyfikatu z adnotacją o przyczynie unieważnienia „wstrzymanie³ certyfikatu”.

W polu tym mogą pojawić się następujące wartości:

- Brak (06 07 2a 86 48 ce 38 02 01)
- Powiadomienie wystawcy certyfikatu (06 07 2a 86 48 ce 38 02 02)
- Odrzucenie certyfikatu (06 07 2a 86 48 ce 38 02 03)

² Pojęcie „wstrzymanie certyfikatu” występuje w systemach Microsoft Windows, jest ono równoważne pojęciu „zawieszenie certyfikatu”.

³ W systemach Microsoft Windows wyświetlone zostaje „Nieznana przyczyna CRL”.
System DOCert - Polityka certyfikacji dla certyfikatów użytkowych

8. Audyt zgodności i inne oceny

8.1 Częstotliwość i okoliczności oceny

System DOCert może być objęty kontrolą wewnętrzną lub zadaniem audytowym zgodnie z przepisami odrębnymi. Dodatkowo, z częstotliwością określoną w przepisach odrębnych, Inspektor Bezpieczeństwa Systemu przeprowadza Analizę Ryzyka systemu DOCert. Celem przeprowadzenia Analizy Ryzyka systemu DOCert 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

Audytorzy wykonujący zadanie audytowe nie są w żaden sposób związani z systemem DOCert.

8.4 Zagadnienia objęte audytem

Cel i zakres zadania audytowego są określane zgodnie z przepisami odrębnymi i mogą obejmować w szczególności funkcjonowanie systemu, zgodność świadczenia usług z politykami certyfikacji oraz zgodność działań z powszechnie obowiązującymi przepisami.

8.5 Działania podejmowane w celu usunięcia usterek wykrytych podczas audytu

Zgodnie z przepisami odrębnymi.

8.6 Informowanie o wynikach audytu

Zgodnie z przepisami odrębnymi.

9. Inne kwestie biznesowe i prawne

9.1 Opłaty

NBP nie pobiera opłat za wydanie pakietu ochrony kryptograficznej, kluczy kryptograficznych czy certyfikatów, ani za dostęp do repozytorium, znajdującego się na stronie www.docert.nbp.pl.

NBP **pobiera opłaty** w przypadku :

- Zniszczenia⁴ lub zagubienia karty elektronicznej wydanej przez NBP,
- Zagubienia licencji oprogramowania kryptograficznego, przekazanego przez NBP,
- Zagubienia lub zniszczenia czytnika kart elektronicznych, przekazanego przez NBP.

9.2 Odpowiedzialność finansowa

Zasady odpowiedzialności finansowej NBP i Klientów określają Umowy.

9.3 Poufność informacji biznesowej

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

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

9.3.1 Zakres poufności informacji

Zgodnie z art. 15 ustawy o usługach zaufania, tajemnicą objęte są wszystkie informacje związane ze świadczeniem usług zaufania, których nieuprawnione ujawnienie mogłoby narazić na szkodę dostawcę usług zaufania lub odbiorcę tych usług. W szczególności tajemnicą objęte są klucze prywatne CCK oraz wszelkie dane mogące służyć ich odtworzeniu.

Zgodnie z ustawą o ochronie danych osobowych szczególnej ochronie podlegają dane osobowe przetwarzane w systemie DOCert. Szczegółowe informacje dotyczące ochrony danych osobowych opisane są w rozdziale 10.

⁴ Za zniszczenie uważa się także trwałe zablokowanie karty elektronicznej.

Dodatkowo, ochronie podlegają informacje zastrzeżone jako tajemnica przedsiębiorstwa podmiotów, z którymi NBP zawarł umowę w ramach systemu DOCert.

9.3.2 Informacje znajdujące się poza zakresem poufności informacji

Wszystkie informacje objęte tajemnicą wymienione zostały w rozdziale 9.3.1.

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 obowiązki nałożone na strony niniejszej Polityki, tj. na CCK, PRU, Uczestników oraz strony ufające.

W ramach świadczenia swoich usług w systemie DOCert, Operator CCK ma obowiązek:

- 1) przestrzegać przepisów polityk certyfikacji oraz umów zawartych pomiędzy NBP a Klientami;
- 2) chronić klucze prywatne Centrum Certyfikacji Kluczy i zapewnić bezpieczeństwo procesu generowania kluczy kryptograficznych Uczestników;
- 3) generować i zarządzać certyfikatami zgodnie ze standardem x.509 v3;
- 4) unieważniać certyfikaty zgodnie z obowiązującymi procedurami;
- 5) publikować, bez zbędnej zwłoki, listy unieważnionych certyfikatów;
- 6) zapewnić dostępność najbardziej aktualnych list unieważnionych certyfikatów, certyfikatów Centrum Certyfikacji Kluczy oraz polityk certyfikacji;
- 7) świadczyć usługi zaufania zgodnie z obowiązującymi przepisami prawa oraz zgodnie z zatwierdzonymi procedurami systemu DOCert;
- 8) zapewnić, by wszystkie czynności związane ze świadczeniem usług zaufania w systemie DOCert wykonywane były tylko przez osoby do tego upoważnione;
- 9) przechowywać i archiwizować dokumenty i dane w postaci elektronicznej, bezpośrednio związane ze świadczeniem usług zaufania, w sposób zapewniający bezpieczeństwo tych danych i dokumentów.

W ramach świadczenia swoich usług w systemie DOCert, Operator CCK ma zakaz:

- 1) przechowywania kluczy prywatnych Uczestników oraz danych mogących służyć do ich odtworzenia,

- 2) kopiowania kluczy prywatnych Uczestników oraz danych mogących służyć do ich odtworzenia.

W ramach świadczenia swoich usług w systemie DOCert, Operator PRU ma obowiązek:

- 1) przestrzegać przepisów polityk certyfikacji oraz umów zawartych pomiędzy NBP a Klientami;
- 2) świadczyć usługi zaufania zgodnie z obowiązującymi przepisami prawa oraz zgodnie z zatwierdzonymi procedurami systemu DOCert;
- 3) zapewnić, by wnioski kierowane do Centrum Certyfikacji Kluczy zawierały prawdziwe dane Uczestnika i były wolne od błędów;
- 4) na bieżąco informować Centrum Certyfikacji Kluczy o zauważonych problemach w systemie DOCert;
- 5) przechowywać i archiwizować dokumenty i dane w postaci elektronicznej, bezpośrednio związane ze świadczeniem usług zaufania, w sposób zapewniający bezpieczeństwo tych danych i dokumentów;
- 6) dokonywać weryfikacji tożsamości Użytkowników zgodnie z warunkami polityk certyfikacji, procedur systemu DOCert oraz umów zawartych między NBP a Klientami;
- 7) umożliwić generowanie kluczy kryptograficznych tylko zweryfikowanym poprawnie osobom;
- 8) udzielać pomocy osobom generującym klucze kryptograficzne.

Uczestnik oraz Użytkownik systemu DOCert mają obowiązek:

- 1) dostarczyć wszystkie dane wymagane do wystawienia certyfikatu w systemie DOCert i zapewnić ich prawdziwość;
- 2) niezwłocznie informować Punkt Rejestracji Użytkowników o wszelkich zmianach danych, o których mowa w pkt 1;
- 3) przestrzegać przepisów polityk certyfikacji oraz umów zawartych pomiędzy NBP a Klientami;
- 4) zapewnić należytą ochronę klucza prywatnego oraz hasła do niego;
- 5) wykorzystywać klucze kryptograficzne i certyfikaty systemu DOCert tylko w zakresie określonym w certyfikacie oraz opisanym w umowach zawartych pomiędzy NBP a Klientami;
- 6) natychmiast żądać unieważnienia certyfikatu w przypadku kompromitacji odpowiadającego mu klucza prywatnego;
- 7) terminowo wymieniać klucze kryptograficzne;
- 8) zapewnić aktualność posiadanego pakietu ochrony kryptograficznej;
- 9) w przypadku zakończenia uczestnictwa – zwrócić do Punktu Rejestracji Użytkowników wszystkie otrzymane z NBP elementy pakietu ochrony kryptograficznej, z wyłączeniem kluczy kryptograficznych zapisanych na płycie CD.

Strona ufająca wykorzystująca certyfikaty systemu DOCert, ma obowiązek:

- 1) korzystać z certyfikatów tylko w zakresie w nich opisanym;
- 2) dokonywać pełnej weryfikacji certyfikatu Uczestnika przed jego wykorzystaniem;
- 3) informować Punkt Rejestracji Użytkowników lub Centrum Certyfikacji Kluczy 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 DOCert nie czyni z NBP agenta, powiernika czy reprezentanta Uczestnika, któremu wydany został certyfikat.

9.6 Ograniczenia odpowiedzialności

NBP nie ponosi odpowiedzialności za niedokonanie 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.

NBP nie ponosi odpowiedzialności za użycie przez Użytkownika kluczy kryptograficznych i certyfikatów niezgodnie z ich przeznaczeniem określonym w Umowach oraz w odpowiednich politykach certyfikacji.

NBP, jako właściciel systemu DOCert, 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

NBP jest administratorem danych osobowych przetwarzanych w ramach systemu DOCert z wyłączeniem danych osobowych powierzonych NBP przez Ministerstwo Finansów w ramach porozumienia o współpracy w zakresie świadczenia usług certyfikacyjnych dla Systemu TREZOR. Dane osobowe w systemie DOCert przetwarzane są zarówno w postaci papierowej, jak i elektronicznej i nie są publicznie dostępne.

Zakres danych osobowych Użytkownika, przetwarzanych w systemie DOCert, to:

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

Dokumenty w formie papierowej i elektronicznej, zawierające dane osobowe związane z systemem DOCert, podlegają zabezpieczeniom zapobiegającym nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu, zgodnie z przepisami prawa. Dane osobowe przechowywane są przez okres ważności certyfikatów i przez 5 lat po wygaśnięciu ostatniego certyfikatu osoby, której dane dotyczą. Po tym okresie certyfikaty są usuwane z bazy systemu DOCert, a kopie archiwalne zawierające te certyfikaty są niszczone.

Załącznik A – Autocertyfikaty CCK

Autocertyfikat NBP CCK 2

Data wystawienia 28 stycznia 2015 roku

Data wygaśnięcia 28 stycznia 2035 roku

Identyfikator klucza podmiotu 3f 8b e5 8d b6 b6 86 92 bd 45 03 9c 17 a0 eb 2d 62 e1 ac a7

Autocertyfikat w formacie base64

```

-----BEGIN CERTIFICATE-----
MIIF2DCCA8CgAwIBAgIBATANBgkqhkiG9w0BAQsFADB9MQswCQYDVQQGEwJQTDER
MA8GA1UEBwwIV2Fyc3phd2ExHTAbBgNVBAoMFE5hcm9kb3d5IEJhbmsgUG9sc2tp
MSgwJgYDVQQQLDB9DZW50cnVtIENlcnR5ZmlrYWwqSBLbHVjenkgTkjQMRiWEAYD
VQDDA1OQ1AgQONLIDIwHhcNMTUwMTI4MTAzMjQxWWhcNMzUwMTI4MjMlOTU5WjB9
MQswCQYDVQQGEwJQTDERMA8GA1UEBwwIV2Fyc3phd2ExHTAbBgNVBAoMFE5hcm9k
b3d5IEJhbmsgUG9sc2tpMSgwJgYDVQQQLDB9DZW50cnVtIENlcnR5ZmlrYWwqSBL
bHVjenkgTkjQMRiWEAYDVQDDA1OQ1AgQONLIDIwggIiMA0GCSqGSIb3DQEBAQUA
A4ICDwAwggIKAoICAQDmLzqak9N6xD8AAPFzQLqVvNxnWjVPM2pK0iHbg4x78Lxx
9xEKeDtMTQumUgB6Se4+lMz3zEcDfEFx1zoEWrKVqg+IJB859V8G9C+ILMG4CrP
5kH2JqkSLsUT4LbC5VFcjXCjJUdRUXjarzn34CjAimvPdQ5MsP0Li6OWTldkZvmw
L7Lil/Obtbn9Fu2gOx91bzBawChrzyTyP2ziW9QYYfsmIRY7pb7ONEaYVCPst9s
hyToFDdjbB45yxfvGgEg5e583HqoUXTk9R/sP+TpEp0RR++UJHGnEuFsu6FbT5/
GLZ7EHniwHLgI/V0TPOZR7K5HAQsoZx94hROIi8SKfg+DvOeC+UA54FUSfHUA8y1
w8ULN1SoWaAydU+jYE2mVmU3KCi81xP50xeUdzcNj262LrupZBj1L4F5BL0pzhWg
5jIXVWxsxsrpArT/JFSrP5+9PmPQZoRmo1BIjWn3GwhfoobFZmYtva4k3wQKp+E6r
zn20daSV5ZapMvmU6fOaL1dXn4IiZzP80GzCuwGNFq+srHEjdnqhrQ/kU+fmSZWU
/l4szy+0LEDrgySKdrX86U8Ww19x9Zw0QPc/jWcZ52+Os0wAU8WZ4mZ+qFcoFMXz
TYwJnHU5mEENppf+7RYIEf1YqGK0SZ4EdhRxbF3/dr7F5ov2OGC3mbh8/QmkVwID
B1U3o2MwYTAOBgNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/BAUwAwEB/zAfBgNVHSME
GDAWgBQ/i+WNtraGkr1FA5wXoOstYuGspzAdBgNVHQ4EFgQUP4v1jba2hpK9RQOc
F6DrLWLhrKcwDQYJKoZIhvcNAQELBQADggIBAGQuFc2nXInG3rZ/7jSNOJ8ZWLdF
8y801uxjUT3tBEQuK6g2w/zPFGea7fkTkz/TDOZE889TxYLqr5M0b6QZVksu7qQ3
rWkGND/gkdOaAGjV32pTRYgp2PboGPWJrAXVyxv5EqmNjcpZPvyccLZX1CLY59Za
jRwTCEwC1NAZ2gbfjnel7VuEjyb+ECyZaTz2tuEydZ0poEztKdei1zS13gG1PMc
APYh6hUAogn/+UfX4cUU4DUyPRCnhkUd9a1XkhYeUqa+Jzmc0s04noyBG9imJlev
k41mr1UnUpIpmj7Ir+saAIBG7RJMIBUxO/YJ1H8MTLhbH7aJJxCXwsxzHgiJkzco
Uet27grdNOTFu0MtkfGg7Hr0eElv36LxYoSpat1C40xEeNCoeReSWkoKJzHfOkCM
0p04m7QJBFdHgIOu+kXRdXG7PcSXbxEQLGykUFFjdBOKii2SIL1IJPzxEQInwIe
p6JE6MuouHrFzyaEauFJLNRKT4T5rluzXiQCCRCEg6UGeO+vXx1106yDBqMJGL3C
DbNRbe8yoDYCFEGMhGCqr03JYScvno5Zvd+1I7qQn7y8ESIA36nXbsawZfLucQZ6
ZzDhccwd/pVoqNs5ALDgrkxgeK7SIuOeg5yY25KNi7ZbcaU/3K65g8Mm2w4pg3Ru
FIeZMgCIubc/PY4O -----END CERTIFICATE-----

```

Załącznik B – Historia zmian dokumentu

Lp.	Data	Wersja	Osoba	Opis wykonanych prac
1.	20.06.2014	0.1		Utworzenie dokumentu
2.	27.06.2014	0.1		Przegląd dokumentu, głównie pod kątem zgodności z przepisami obowiązującymi w NBP, zgłoszenie uwag do rozdziału 9.3 i 10 oraz drobnych uwag o charakterze redakcyjnym.
3.	30.06.2014	0.1		Przegląd dokumentu i zgłoszenie uwag w zakresie zgodności zapisów o zabezpieczeniu danych osobowych (rozdział 10) zgodnie z powszechnie obowiązującymi przepisami.
4.	01.07.2014	0.2		Zmiany w związku z uwagami otrzymanymi z Wydziału Ochrony Informacji DB
5.	01.07.2014	0.2		Przegląd wprowadzonych zmian, zgłoszenie drobnych uwag redakcyjnych.
6.	13.08.2014	0.3		Wprowadzenie zmian zgłoszonych przez oddziały okręgowe NBP.
7.	20.08.2014	0.4		Przegląd dokumentu
8.	21.08.2014	0.4		Przegląd dokumentu
9.	06.02.2015	0.5		Wprowadzenie zmian związanych z wprowadzeniem Uchwały Zarządu NBP nr 1/2015 oraz uruchomieniem urzędu NBP CCK 2
10.	Styczeń 2017	1.01		Wprowadzenie zmian związanych z wprowadzeniem Uchwały Zarządu NBP nr 53/2016 oraz zakończeniem pracy urzędów CCK-TEST i CCK NBP
11.	Luty 2017	1.02		Przegląd i korekta dokumentu
12.	Kwiecień 2017	1.03		Przegląd i korekta dokumentu
13.	Kwiecień 2017	1.04		Przegląd i korekta dokumentu
14.	Maj 2018	1.11		Wprowadzenie zmian związanych ze zmianą Uchwały Zarządu NBP nr 53/2016 (zmiany związane z RODO)

Zatwierdzenie dokumentu

Data	Wersja	Osoba	Podpis
	1.2	Dyrektor Departamentu Bezpieczeństwa	

www.nbp.pl