Polityka certyfikacji

Narodowego Centrum Certyfikacji

wersja 2.0

Metryka dokumentu

1.	**Źródło dokumentu**	Narodowy Bank Polski
2.	**Tytuł**	Polityka certyfikacji Narodowego Centrum Certyfikacji
3.	**Rodzaj dokumentu**	polityka certyfikacji
4.	**Status dokumentu**	zatwierdzony
5.	**Wersja**	2.0
6.	**Odpowiedzialny**	Renata Łukowska
7.	**Liczba stron**	117

Historia dokumentu

Lp	Data	Wersja	Osoba	Opis wykonanych prac
1.	kwiecień 2005	1.0		Opracowanie dokumentu
2.	kwiecień 2005	1.0		Przegląd dokumentu
3.	maj 2005	1.0		Ocena dokumentu pod kątem zgodności z wymaganiami prawnymi w ramach audytu
4.	czerwiec 2005	1.0		Uzupełnienie dokumentu zgodnie z wnioskami firmy audytorskiej
5.	03.06.2005	1.0		Przegląd dokumentu
6.	06.06.2005	1.0		Zatwierdzenie dokumentu
7.	07.09.2005	1.1		Uzupełnienie dokumentu o zapisy dotyczące prowadzenia rejestru podmiotów kwalifikowanych
8.	08.09.2005	1.1		Przegląd dokumentu
9.	30.09.2005	1.1		Zatwierdzenie dokumentu
10.	25.07.2006 04.08.2006	1.11 1.11		Zmiany w rozdziałach 2.2, 6.2 i 6.3.7 Załącznik nr 4 - Dodanie nowych profili zaświadczeń certyfikacyjnych
11.	10.08.2006	1.11		Przegląd dokumentu
12.	11.08.2006	1.11		Wysłanie dokumentu do Ministerstwa Gospodarki oraz do podmiotów kwalifikowanych, do konsultacji
13.	21.08.2006	1.11		Propozycja zmian
14.	21.08.2006	1.11		Propozycja zmian
15.	21.08.2006	1.11		Akceptacja dokumentu
16.	25.08.2006	1.11		Akceptacja dokumentu
17.	04.09.2006	1.11		Potwierdzenie uzgodnienia stanowisk KIR S.A. i UNIZETO TECHNOLOGIES S.A. w kwestii jaki bit keyUsage zostanie wykorzystany w zaświadczeniach certyfikacyjnych. Ustalono, że zostaną użyte bity nonRepudiation i digitalSignature.
18.	06.09.2006	1.12		Zmiany w Załączniku nr 4, w punktach: 1, 2, 2.2, 2.2.1, 3, 3.2,

Lp	Data	Wersja	Osoba	Opis wykonanych prac
				3.2.1, 3.2.2, 3.2.3, 4, 4.2, 4.2.1, 4.2.2, 5, 5.2, 5.2.1, 5.2.2, 5.2.3, dodany pkt 4.2.4.
19.	08.09.2006	1.12		Wysłanie dokumentu do Ministerstwa Gospodarki oraz do podmiotów kwalifikowanych, do konsultacji
20.	14.09.2006	1.12		Akceptacja dokumentu
21.	15.09.2006	1.12		Uwaga do rozdz.2.2.2. w Załączniku 4
22.	18.09.2006	1.13		Zmiana w rozdz.2.2.2. w Załączniku 4 - uwzględnienie uwagi UNIZETO TECHNOLOGIES S.A.
23.	18.09.2006	1.13		Konsultacja zmiany w rozdziale 2.2.2 w Załączniku 4 z Ministerstwem Gospodarki oraz podmiotami kwalifikowanymi
24.	11.10.2006	1.2		Zatwierdzenie dokumentu
25.	12.01.2007	1.21		Zmiana w rozdz. 2.2 Zmiany w Załączniku 4 - Dodanie nowych profili zaświadczeń certyfikacyjnych
26.	15.01.2007	1.21		Przegląd dokumentu
27.	15.01.2007	1.21		Konsultacja projektu zmian z Ministerstwem Gospodarki oraz podmiotami kwalifikowanymi
28.	05.02.2007	1.3		Zatwierdzenie dokumentu
29.	26.07.2007	1.31		Zmiany w rozdz. 1 i 2.2. Dodanie rozdz. 8 Zaświadczenie certyfikacyjne dla podmiotu kwalifikowanego świadczącego usługi w zakresie wydawania certyfikatów atrybutów
30.	07.08.2007	1.31		Konsultacja projektu zmian
31.	08.08.2007	1.31		Przegląd dokumentu
32.	09.08.2007	1.31		Wysłanie dokumentu do Ministerstwa Gospodarki oraz do podmiotów kwalifikowanych do konsultacji
33.	10.08.2007	1.31		Akceptacja dokumentu
34.	16.08.2007	1.31		Akceptacja dokumentu
35.	17.08.2007	1.31		Akceptacja dokumentu

Lp	Data	Wersja	Osoba	Opis wykonanych prac
36.	21.08.2007	1.31		Akceptacja dokumentu
37.	03.09.2007	1.4		Zatwierdzenie dokumentu
38.	26.11.2007	1.41		Zmiana definicji *Narodowego Centrum Certyfikacji* oraz *Punktu rejestracji* w rozdz. 1 oraz zmiana skrótu NCC na NCCert w całym dokumencie. Zmiany w rozdz. 2.2
39.	30.11.2007	1.41		Przegląd dokumentu
40.	14.12.2007	1.41		Opinia prawna – propozycja modyfikacji zaproponowanych definicji w rozdz. 1
41.	18.12.2007	1.42		Modyfikacji definicji *Narodowego Centrum Certyfikacji* oraz *Punktu rejestracji* w rozdz. 1 zgodnie z propozycją Departamentu Prawnego NBP
42.	18.12.2007	1.42		Wysłanie dokumentu do Ministerstwa Gospodarki do konsultacji
43.	21.12.2007	1.42		Wniosek o doprecyzowanie właściwej jednostki organizacyjnej w definicji Narodowego Centrum Certyfikacji
44.	12.03.2008	1.43		Modyfikacja definicji *Narodowego Centrum Certyfikacji* oraz *Punktu rejestracji* w rozdz. 1 po roboczych ustaleniach z Ministerstwem Gospodarki
45.	19.03.2008	1.43		Wysłanie dokumentu do Ministerstwa Gospodarki oraz do podmiotów kwalifikowanych do konsultacji oraz nie zgłoszenie uwag w wyznaczonym terminie
46.	25.04.2008	1.5		Zatwierdzenie dokumentu
47.	25.02.2009	1.51		Zmiany w dokumencie związane z wymianą zaświadczenia certyfikacyjnego ministra właściwego ds. gospodarki, rezygnacją z identyfikatora wyróżniającego wskazującego na Centrast SA, utworzeniem urzędu ***nowy Root*** Zmiany w rozdziałach: 2.1.1, 2.1.4, 2.1.5, 2.2, 2.3.1, 3.1.1, 3.1.3, 3.2.1, 3.6.1, 3.6.2, 3.6.4, 3.8.2, 3.9, 4.1.2, 5.4.3, 5.4.9,

Lp	Data	Wersja	Osoba	Opis wykonanych prac
				5.4.10, 5.6.1, 5.7.1.1, 5.7.1.2, 5.7.2, 9.2, załączniku nr 1, załączniku nr 2, załączniku nr 4
48.	02.03.2009	1.52		Przegląd dokumentu, zmiany w rozdziałach: 2.1.1 i 2.3.1
49.	23.03.2009	1.53		Przegląd dokumentu, zmiany w rozdziałach: 2.1.1, 2.1.4, 2.1.5 (OID polityki certyfikacji), 2.2, 2.3.1, 5.4.3, 5.4.10, 7.2.3, 7.2.8, 7.2.9,
50.	24.03.2009	1.54		Przegląd dokumentu – poprawki redakcyjne w rozdziałach: 5.2.1, 5.5.2, 5.5.3, 5.5.4, 5.5.5, 5.5.6.
51.	25.03.2009	1.55		Ostateczna redakcja dokumentu
52.	25.03.2009	1.55		Przegląd dokumentu
53.	26.03.2009	1.55		Wysłanie dokumentu do Ministerstwa Gospodarki oraz do podmiotów kwalifikowanych do konsultacji
54.	07.04.2009	1.55		Uwagi do: Pkt 2.1.5 – propozycja dodania do przypisu dotyczącego KRIO informacji dotyczącej prowadzenia KRIO z upoważnienia Polskiego Komitetu Normalizacyjnego Pkt 5.6.2 – propozycja dodania odwołania do pkt 5.6.1 Pkt 7.1.5 – komentarz z propozycją zmiany funkcji skrótu SHA-1 na jedną z funkcji rodziny SHA-2
55.	07.04.2009	1.55		Mail z informacją o akceptacji wersji 1.55 dokumentu
56.	21.04.2009	1.56		Uwzględnienie uwag UNIZETO S.A., zmiany w pkt 2.1.5 i 5.6.2
57.	24.04.2009	1.56		Zgłoszenie uwagi dotyczącej pomyłki pisarskiej w pkt 2.1.1 oraz wniosku o usunięcie z identyfikatora wyróżniającego polskich znaków diakrytycznych
58.	30.04.2009	1.57		Uwzględnienie uwag Ministerstwa Gospodarki, zmiany w pkt. 2.1.1, 5.7.1, załącznik nr 1, załącznik nr 2, załącznik nr 4 pkt 1.1.4 i 9.2.3
59.	19.05.2009	1.57		Przegląd i akceptacja dokumentu

Lp	Data	Wersja	Osoba	Opis wykonanych prac
60.	01.09.2009	1.57		Przegląd dokumentu w ramach audytu
61.	07.09.2009	1.58		Zmiany w pkt 3.7.6, pkt 5.4.3, pkt 6.1.2, pkt 7.1.5, pkt 7.1.9, pkt 7.2.6 oraz poprawki językowe w pkt 2.1.4 i pkt 5.5.3 – uwzględnienie uwag audytora.
62.	07.09.2009	1.58		Przegląd dokumentu
63.	17.09.2009	1.58		Akceptacja dokumentu
64.		1.58		Akceptacja dokumentu
65.		2.0		Zatwierdzenie dokumentu
66.				

Data obowiązywania dokumentu

Lp	Data	Wersja
1.	22.08.2005	1.0
2.	01.10.2005	1.1
3.	16.10.2006	1.2
4.	12.02.2007	1.3
5.	10.09.2007	1.4
6.	28.04.2008	1.5
7.	26.10.2009	2.0

Copyright

Spis treści

Uwaga dla Strony ufającej

Przed zaufaniem podpisowi lub poświadczeniu elektronicznemu weryfikowanemu z wykorzystaniem zaświadczenia certyfikacyjnego wydanego zgodnie z Polityką Certyfikacji należy dokładnie zapoznać się z warunkami opisanymi w niniejszym dokumencie.

W szczególności należy upewnić się, że zostały zrozumiane zarówno ograniczenia odpowiedzialności Narodowego Banku Polskiego jak i wymagania stawiane Subskrybentowi oraz Stronie ufającej.

1 Słownik pojęć

Certyfikat – według art. 2 pkt 10 *Ustawy o podpisie elektronicznym*: elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis elektroniczny.

Dane aktywujące – dane, których znajomość konieczna jest do użycia komponentu technicznego, w szczególności dane uwierzytelniające operatorów oraz PIN-y kart elektronicznych.

Dane służące do składania podpisu elektronicznego – zgodnie z art. 3 pkt 4 *Ustawy o podpisie elektronicznym* niepowtarzalne i przyporządkowane osobie fizycznej dane, które są wykorzystywane przez tę osobę do składania podpisu elektronicznego.

Dane służące do składania poświadczenia elektronicznego – zgodnie z art. 3 pkt 20 *Ustawy o podpisie elektronicznym* niepowtarzalne i przyporządkowane do podmiotu świadczącego usługi certyfikacyjne lub organu wydającego zaświadczenia certyfikacyjne dane, które są wykorzystywane przez ten podmiot lub organ do składania poświadczenia elektronicznego.

Dane służące do weryfikacji podpisu elektronicznego – zgodnie z art. 3 pkt 5 *Ustawy o podpisie elektronicznym*: niepowtarzalne i przyporządkowane osobie fizycznej dane, które są wykorzystywane do identyfikacji osoby składającej podpis elektroniczny.

Dane służące do weryfikacji poświadczenia elektronicznego – zgodnie z art. 3 pkt 21 *Ustawy o podpisie elektronicznym* niepowtarzalne i przyporządkowane do podmiotu świadczącego usługi certyfikacyjne lub organu wydającego zaświadczenia certyfikacyjne dane, które są wykorzystywane do identyfikacji podmiotu lub organu składającego poświadczenie elektroniczne.

Klucze infrastruktury (ang. Infrastructure Keys) – klucze infrastruktury w rozumieniu § 2 pkt 10 Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. Nr 128, poz. 1094).

Komponent techniczny – komponent techniczny w rozumieniu § 2 pkt 6 Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. Nr 128, poz. 1094).

Kwalifikowany podmiot świadczący usługi certyfikacyjne – według art. 3 pkt 15 *Ustawy o podpisie elektronicznym*: podmiot świadczący usługi certyfikacyjne, wpisany do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne.

Lista unieważnionych zaświadczeń certyfikacyjnych (ang. Authority Revocation List) – lista unieważnionych zaświadczeń certyfikacyjnych, wydawana przez podmiot wydający zaświadczenia certyfikacyjne, zawierająca numer kolejny listy, datę publikacji listy, przewidywany czas publikacji kolejnej listy, określenie podmiotu wydającego listę, numer unieważnionego zaświadczenia certyfikacyjnego, przyczynę i datę unieważnienia oraz poświadczenie elektroniczne listy.

Krajowa infrastruktura klucza publicznego – infrastruktura obejmująca sprzęt, oprogramowanie, ludzi, procesy i polityki, działająca zgodnie z postanowieniami *Ustawy o podpisie elektronicznym* oraz odpowiednimi aktami wykonawczymi, umożliwiająca wykorzystanie w Polsce bezpiecznego podpisu elektronicznego weryfikowanego przy pomocy kwalifikowanego certyfikatu.

Narodowe Centrum Certyfikacji (NCCert) – Narodowy Bank Polski, który na mocy decyzji Ministra Gospodarki i Pracy z dnia 27 lipca 2005 r., na podstawie art. 23 ust. 5 i art. 30 ust. 3 *Ustawy o podpisie elektronicznym*, został upoważniony do wykonywania następujących czynności:

1. wytwarzanie i wydawanie zaświadczeń certyfikacyjnych, o których mowa w art. 23 *Ustawy o podpisie elektronicznym,*
2. publikacja listy wydawanych zaświadczeń certyfikacyjnych, o których mowa w pkt 1,
3. publikacja danych służących do weryfikacji wydanych zaświadczeń certyfikacyjnych, o których mowa w pkt 1,
4. publikacja listy unieważnionych zaświadczeń certyfikacyjnych

oraz któremu powierzono prowadzenie rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, wskazanego w art. 30 ust. 2 pkt 1 *Ustawy o podpisie elektronicznym*.

Podmiot świadczący usługi certyfikacyjne – według art. 3 pkt 14 *Ustawy o podpisie elektronicznym*: przedsiębiorca w rozumieniu przepisów ustawy z dnia 19 listopada 1999 r. – Prawo działalności gospodarczej (Dz. U. Nr 101, poz. 1178, z 2000 r. Nr 86, poz. 958 i Nr 114, poz. 1193 oraz z 2001 r. Nr 49, poz. 509 i Nr 67, poz. 679), Narodowy Bank Polski albo organ władzy publicznej, świadczący co najmniej jedną z usług certyfikacyjnych.

Podmiot upoważniony – podmiot upoważniony, o którym mowa w art. 23 ust. 5 *Ustawy o podpisie elektronicznym*.

Podpis elektroniczny – według art. 3 pkt 1 *Ustawy o podpisie elektronicznym*: dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub logicznie z nimi powiązane, służą do identyfikacji osoby składającej podpis elektroniczny.

Polityka certyfikacji (ang. Certification Policy) – szczegółowe rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób, zakres oraz warunki bezpieczeństwa tworzenia i stosowania certyfikatów.

Poświadczenie elektroniczne – według art. 3 pkt 18 *Ustawy o podpisie elektronicznym*: dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub logicznie z nimi powiązane, umożliwiają identyfikację podmiotu świadczącego usługi certyfikacyjne lub organu wydającego zaświadczenia certyfikacyjne oraz spełniają następujące wymagania:

a. są sporządzane za pomocą podlegających wyłącznej kontroli podmiotu świadczącego usługi certyfikacyjne lub organu wydającego zaświadczenie certyfikacyjne bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania poświadczenia elektronicznego,
b. jakakolwiek zmiana danych poświadczonych jest rozpoznawalna.

Punkt rejestracji – Departament Ochrony w Narodowym Banku Polskim, do obowiązków którego należy:

a. odbiór poleceń ministra właściwego do spraw gospodarki,
b. wymiana dokumentów oraz informacji pomiędzy Subskrybentem a Narodowym Centrum Certyfikacji.

Repozytorium - ogólnodostępna baza danych, w której publikowane są m.in. zaświadczenia certyfikacyjne Subskrybenta, Polityka Certyfikacji oraz listy unieważnionych zaświadczeń certyfikacyjnych. Publikacja, o której mowa odbywa się na stronie internetowej http://www.nccert.pl.

Subskrybent – kwalifikowany podmiot świadczący usługi certyfikacyjne.

Strona ufająca (ang. Relying Party) – osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która:

a. zawarła z podmiotem świadczącym usługi certyfikacyjne umowę o świadczenie usług certyfikacyjnych, lub
b. w granicach określonych w polityce certyfikacji może działać w oparciu o certyfikat lub inne dane elektroniczne poświadczone przez podmiot świadczący usługi certyfikacyjne.

Ścieżka certyfikacji – ścieżka certyfikacji w rozumieniu § 2 pkt 16 Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. Nr 128, poz. 1094).

Usługi certyfikacyjne - według art. 3 pkt 13 *Ustawy o podpisie elektronicznym*: wydawanie certyfikatów, znakowanie czasem lub inne usługi związane z podpisem elektronicznym.

Ustawa o podpisie elektronicznym – Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130. poz. 1450) ze zm.

UTC (ang. Coordinated Universal Time) – czas, który jest obliczany przez Bureau International des Poids et Measures (BIPM) w Sevres we Francji. BIPM uśrednia dane pobierane z ponad 200 zegarów atomowych i wzorców częstotliwości utrzymywanych w około 50 laboratoriach na świecie.

Użytkownik końcowy – Subskrybent i Strona ufająca.

Zaświadczenie certyfikacyjne – według art. 3 pkt 11 *Ustawy o podpisie elektronicznym*: elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji poświadczenia elektronicznego są przyporządkowane do podmiotu świadczącego usługi certyfikacyjne lub organu wydającego zaświadczenia w imieniu ministra właściwego do spraw gospodarki, które umożliwiają identyfikację tego podmiotu lub organu.

Zaświadczenie certyfikacyjne ministra właściwego do spraw gospodarki - zaświadczenie certyfikacyjne, o którym mowa w § 1 pkt 1 Rozporządzenia Ministra Gospodarki z dnia 9 sierpnia 2002 r. w sprawie określenia szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem elektronicznym (Dz. U. Nr 128, poz. 1101).

Żądanie certyfikacji – plik w formacie PKCS#10 zawierający między innymi nazwę wyróżniającą Subskrybenta oraz dane służące do weryfikacji poświadczeń elektronicznych.

2 Wstęp

Polityka certyfikacji jest podstawowym dokumentem określającym warunki świadczenia usług certyfikacyjnych. Według *Ustawy z dnia 18 września 2001 roku o podpisie elektronicznym* (zwanej dalej *Ustawą o podpisie elektronicznym*) polityka certyfikacji jest dokumentem określającym „szczegółowe *rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób, zakres oraz warunki bezpieczeństwa tworzenia i stosowania certyfikatów".* W podobny sposób pojęcie „polityka certyfikacji" definiują standardy dotyczące świadczenia usług certyfikacyjnych. Na przykład standard *IETF RFC2527 X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, S. Chokhani, W. Ford, march 1999* (zwany dalej [RFC2527]) opisuje politykę certyfikacji jako:

„Spisany zbiór zasad, który określa zakres stosowania certyfikatów w obrębie określonego kręgu użytkowników i/lub klas aplikacji o podobnych wymaganiach w zakresie bezpieczeństwa".

Polityka certyfikacji, jako dokument opisujący zasady świadczenia usług certyfikacyjnych, znajduje zastosowanie w działalności wszystkich podmiotów świadczących usługi certyfikacyjne w obrębie określonego kręgu użytkowników.

Dokument „Polityka certyfikacji Narodowego Centrum Certyfikacji", zwany dalej Polityką Certyfikacji, przedstawia zasady pełnienia przez Narodowe Centrum Certyfikacji funkcji podmiotu upoważnionego, o którym mowa w art. 23 ust. 5 *Ustawy o podpisie elektronicznym*, powierzonej mu, na wniosek Prezesa Narodowego Banku Polskiego, przez ministra właściwego do spraw gospodarki.

Polityka Certyfikacji dostępna jest nieodpłatnie w wersji elektronicznej w Repozytorium.

2.1 Wprowadzenie

Na podstawie art. 23 ust. 5 *Ustawy o podpisie elektronicznym,* minister właściwy do spraw gospodarki, na wniosek Prezesa Narodowego Banku Polskiego, powierzył z dniem 14 listopada 2002 r. Centrum Zaufania i Certyfikacji CENTRAST S.A. funkcję podmiotu upoważnionego. W związku z postawieniem spółki CENTRAST w stan likwidacji, na wniosek Prezesa Narodowego Banku Polskiego, minister właściwy do spraw gospodarki powierzył Narodowemu Bankowi Polskiemu funkcję podmiotu upoważnionego, realizowaną przez Narodowe Centrum Certyfikacji, od dnia 22 sierpnia 2005 r..

Działalność Narodowego Centrum Certyfikacji stanowi kontynuację działalności Centrum Zaufania i Certyfikacji CENTRAST S.A..

Narodowe Centrum Certyfikacji, w zakresie objętym niniejszą Polityką Certyfikacji, nie jest kwalifikowanym podmiotem świadczącym usługi certyfikacyjne.

Narodowe Centrum Certyfikacji, jako podmiot upoważniony, w imieniu ministra właściwego do spraw gospodarki:

1. Wytwarza i wydaje zaświadczenia certyfikacyjne podmiotom wpisanym do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, o których mowa w *art. 23 ust. 2 Ustawy o podpisie elektronicznym*;
2. Publikuje listy wydanych zaświadczeń certyfikacyjnych, o których mowa w punkcie 1;
3. Publikuje listy unieważnionych zaświadczeń certyfikacyjnych;
4. Publikuje dane służące do weryfikacji wydanych zaświadczeń certyfikacyjnych, o których mowa w punkcie 1;
5. Prowadzi rejestr kwalifikowanych podmiotów świadczących usługi certyfikacyjne, o którym mowa w *art. 30 ust. 2 pkt 1 Ustawy o podpisie elektronicznym*, zgodnie z Rozporządzeniem Ministra Gospodarki z dnia 6 sierpnia 2002 r. w sprawie sposobu prowadzenia rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne związane z podpisem elektronicznym, wzoru tego rejestru oraz szczegółowego trybu postępowania w sprawach o wpis do rejestru (Dz. U. Nr 128, poz. 1099) [1].

Działalność Narodowego Centrum Certyfikacji regulowana jest prawem obowiązującym na terytorium Rzeczpospolitej Polskiej, w szczególności *Ustawą o podpisie elektronicznym* oraz odpowiednimi przepisami wykonawczymi.

Narodowe Centrum Certyfikacji, w oparciu o zalecenia standardu [RFC2527], opracowało i opublikowało Politykę Certyfikacji. Dokument ten informuje o zasadach obowiązujących podmiot upoważniony, Subskrybenta oraz Stronę ufającą wykorzystującą wydane przez Narodowe Centrum Certyfikacji zaświadczenia certyfikacyjne.

Polityka Certyfikacji określa w szczególności: typy wydawanych zaświadczeń certyfikacyjnych, zakres zastosowania wydawanych zaświadczeń certyfikacyjnych, zasady wydawania zaświadczeń certyfikacyjnych, uczestników procesu wydawania zaświadczeń certyfikacyjnych, ich odpowiedzialność i obowiązki, zasady unieważniania wydanych zaświadczeń certyfikacyjnych oraz zasady publikacji informacji związanych z pełnieniem roli podmiotu upoważnionego.

2.1.1 Ważne informacje dla Subskrybentów i Stron ufających

Dane służące do składania poświadczenia elektronicznego przejęte od CENTRAST S.A. w 2005 roku zostały wygenerowane 17 grudnia 2002 r. z okresem ważności do dnia **14 grudnia 2013 r.** Zgodnie z pkt. 5. 7. 1 Polityki Certyfikacji, proces wymiany danych służących do składania poświadczenia elektronicznego Narodowego Centrum Certyfikacji rozpoczęto po upływie połowy okresu ważności zaświadczenia certyfikacyjnego ministra właściwego do spraw gospodarki, tj. w drugiej połowie 2008 r.

W uzgodnieniu z Ministrem Gospodarki przyjęto koncepcję wymiany zaświadczenia certyfikacyjnego ministra właściwego do spraw gospodarki bez certyfikacji wzajemnej, z jednoczesną rezygnacją ze wskazania w zaświadczeniu na CZiC Centrast SA. Wszystkie trzy działające na rynku podmioty kwalifikowane świadczące usługi certyfikacyjne zadeklarowały gotowość spełnienia wymagań technicznych i organizacyjnych związanych z takim modelem wymiany

[1] od dnia 1 października 2005r.

zaświadczenia certyfikacyjnego ministra właściwego do spraw gospodarki w Narodowym Centrum Certyfikacji.

W celu usunięcia z dotychczasowego identyfikatora wyróżniającego, tj.:

Kraj	**PL**
Organizacja	**CZiC Centrast SA w imieniu Ministra Gospodarki**
Nazwa powszechna	**CZiC Centrast SA**

nazwy nieistniejącego już podmiotu CZiC Centrast SA, przyjęto, że identyfikator wyróżniający zaświadczenia certyfikacyjnego ministra właściwego do spraw gospodarki będzie miał następującą postać:

Kraj	**PL**
Organizacja	**Minister wlasciwy do spraw gospodarki**[2]
Nazwa powszechna	**Narodowe Centrum Certyfikacji (NCCert)**

Zmiana ta wiąże się z utworzeniem technologicznie nowego urzędu, ponieważ algorytm budowy ścieżki certyfikacji rozpoznaje główny urząd certyfikacji w oparciu o jego identyfikator wyróżniający.

W związku z powyższym, w celu zachowania ciągłości krajowej infrastruktury klucza publicznego w szczególności zachowania ważności wystawionych zaświadczeń certyfikacyjnych i certyfikatów, do dnia 14 grudnia 2013 r. niezbędne jest równoległe funkcjonowanie dwóch urzędów certyfikacji w Narodowym Centrum Certyfikacji, tj.: **dotychczasowego urzędu (*stary Root*)**, z identyfikatorem wyróżniającym wskazującym na CZiC Centrast SA, realizującego następujące czynności:

1. unieważnianie zaświadczeń certyfikacyjnych Subskrybentów, wydanych przez urząd ***stary Root***,
2. wystawianie i publikowanie list unieważnionych zaświadczeń certyfikacyjnych ARL (**nccert.crl**) wydanych przez urząd ***stary Root***.

oraz **nowego urzędu (*nowy Root*)**, z nowym identyfikatorem wyróżniającym wskazującym na ministra właściwego do spraw gospodarki (j.w.), realizującego następujące czynności:

1. wytwarzanie, wydawanie i publikowanie zaświadczeń certyfikacyjnych dla Subskrybentów, wydanych przez urząd ***nowy Root***,
2. unieważnianie zaświadczeń certyfikacyjnych Subskrybentów, wydanych przez urząd ***nowy Root*** ,
3. wystawianie i publikowanie list unieważnionych zaświadczeń certyfikacyjnych ARL (**nccert-n.crl**) wydanych przez urząd ***nowy Root***.

Oba urzędy będą funkcjonować równolegle do czasu wygaśnięcia zaświadczenia certyfikacyjnego Ministra Gospodarki wskazującego na CZiC Centrast SA, tzn. do dnia 14 grudnia 2013 r.

Od dnia 15 grudnia 2013 r. funkcjonować będzie jedynie urząd ***nowy Root***.

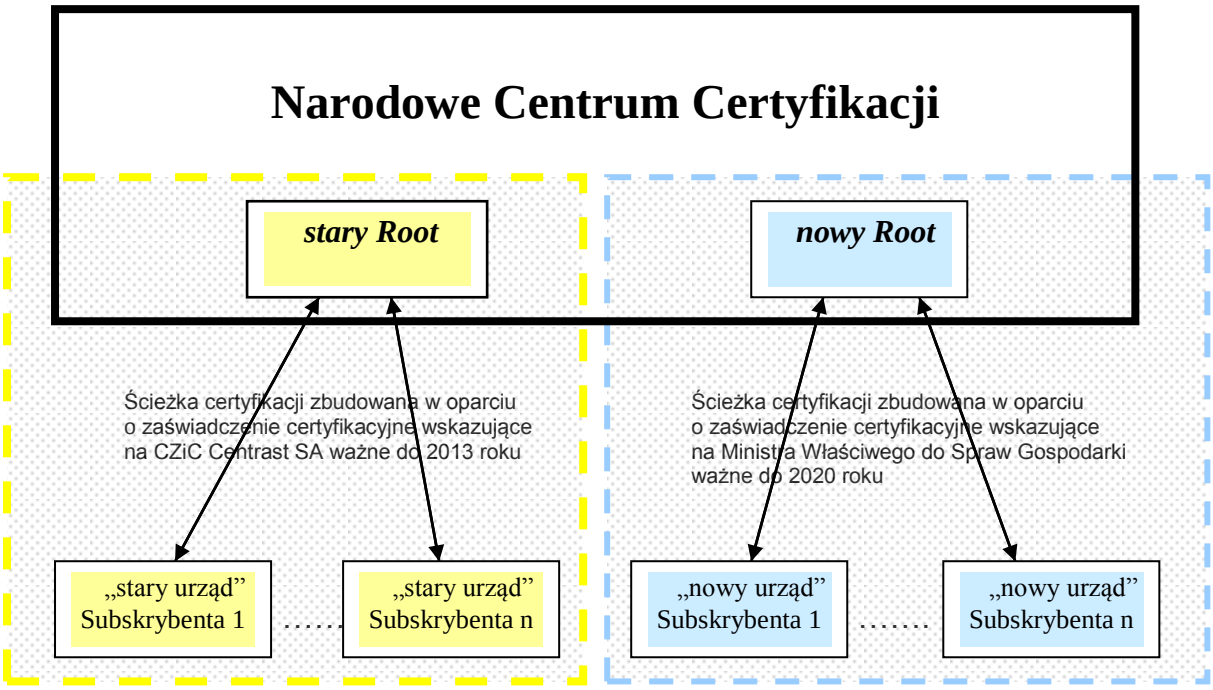
[2] Z nazwy *minister właściwy do spraw gospodarki* usunięto polskie znaki diakrytyczne, aby zapewnić możliwość współpracy z narzędziami, które nie współpracują z polskimi znakami diakrytycznymi

Należy zwrócić uwagę, że zastosowany model wymiany zaświadczenia certyfikacyjnego ministra właściwego do spraw gospodarki wymaga, aby aplikacja weryfikująca podpis elektroniczny wybierała odpowiednią ścieżkę certyfikacji, tj.

- **ścieżkę zbudowaną w oparciu o zaświadczenie certyfikacyjne wskazujące na CZiC Centrast SA, ważne do 2013 r.**

  lub

- **ścieżkę zbudowaną w oparciu o zaświadczenie certyfikacyjne wskazujące na ministra właściwego do spraw gospodarki, ważne do 2020 r.**[3]



Rysunek 1 Dwie ścieżki certyfikacji w ramach krajowej infrastruktury klucza publicznego

2.1.2 Standardy

Zgodnie z zaleceniami standardów międzynarodowych, aby umożliwić aktualnym oraz przyszłym odbiorcom usług Narodowego Centrum Certyfikacji zapoznanie się z ogólnymi zasadami procesu certyfikacji, a także porównanie tych zasad z informacjami zawartymi w podobnych dokumentach wydanych przez podmioty świadczące usługi certyfikacyjne, struktura oraz zawartość Polityki Certyfikacji oparta została na wytycznych określonych w dokumentach *IETF RFC2527 X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* oraz *ANS X.9.79-1:2001 Part1: PKI Practices and Policy Framework*

[3] wygenerowane po uruchomieniu urzędu nowy Root.

Struktura dokumentu Polityka Certyfikacji, oparta o strukturę proponowaną przez standard [RFC2527], dostosowana została do specyfiki roli pełnionej przez Narodowe Centrum Certyfikacji.

2.1.3 Zaświadczenia certyfikacyjne

Narodowe Centrum Certyfikacji wydaje zaświadczenia certyfikacyjne wyłącznie Subskrybentowi.

Wydanie Subskrybentowi zaświadczenia certyfikacyjnego wymaga wcześniejszego uzyskania przez niego wpisu w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne. Aby uzyskać akredytację ministra właściwego do spraw gospodarki:

1. Podmiot ubiegający się o wpis do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne składa odpowiedni wniosek do ministra właściwego do spraw gospodarki;
2. Minister właściwy do spraw gospodarki, po zaakceptowaniu wniosku, wyznacza kontrolerów oraz zakres kontroli, której poddany zostanie ubiegający się o akredytację podmiot;
3. Przeprowadzana jest kontrola podmiotu ubiegającego się o wpis do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne;
4. Kontrolerzy przedstawiają ministrowi właściwemu do spraw gospodarki raport pokontrolny;
5. Minister właściwy do spraw gospodarki podejmuje decyzję o dokonaniu wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne lub decyzję o odmowie dokonania wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne;
6. Dokonywany jest wpis do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne obejmujący nazwę polityki certyfikacji, w ramach której podmiot może świadczyć usługi certyfikacyjne;
7. Po dokonaniu wpisu podmiot dostarczyć musi ministrowi właściwemu do spraw gospodarki dowód zawarcia umowy ubezpieczenia;
8. Po otrzymaniu dowodu zawarcia umowy ubezpieczenia minister właściwy do spraw gospodarki wydaje Narodowemu Centrum Certyfikacji polecenie wytworzenia i wydania zaświadczenia certyfikacyjnego;
9. Narodowe Centrum Certyfikacji wytwarza, wydaje i publikuje zaświadczenie certyfikacyjne.

Proces akredytacji regulowany jest postanowieniami rozdziału VI *Ustawy o podpisie elektronicznym* oraz odpowiednimi przepisami wykonawczymi.

2.1.4 Informacje o unieważnieniach zaświadczeń certyfikacyjnych

Listy unieważnionych zaświadczeń certyfikacyjnych wydanych Subskrybentom przez Narodowe Centrum Certyfikacji publikowane są w Repozytorium.

Narodowe Centrum Certyfikacji publikuje dwie listy ARL:

1. listę unieważnionych zaświadczeń certyfikacyjnych wydanych przez urząd ***stary Root***, – pod adresem *www.nccert.pl/arl/nccert.crl*

2. listę unieważnionych zaświadczeń certyfikacyjnych wydanych przez urząd ***nowy Root***, – pod adresem *www.nccert.pl/arl/nccert-n.crl*

2.1.5 Identyfikatory obiektów (OID)[4]

Minister właściwy ds. gospodarki zarejestrował w Krajowym Rejestrze Identyfikatorów Obiektów[5] następujący identyfikator obiektu (OID):

{ iso(1) member-body(2) pl(616) organization(1) gov(101) moe(3)}

oraz

Identyfikator obiektu przypisany Polityce Certyfikacji Narodowego Centrum Certyfikacji:

{ iso(1) member-body(2) pl(616) organization(1) gov(101) moe(3) pki(1) certificate-policy(2) in-doc(1) pc(1) version(x) subversion(y)}

gdzie: x – numer wersji polityki certyfikacji

y – numer podwersji polityki certyfikacji

2.2 Identyfikacja

Nazwa polityki	Polityka Certyfikacji Narodowego Centrum Certyfikacji
Wersja	2.0
Status	Wersja aktualna
Identyfikator (OID) Polityki Certyfikacji	id-gov-pc-indoc OBJECT IDENTIFIER ::= { iso(1) member-body(2) pl(616) organization(1) gov(101) moe(3) pki(1) certificate-policy(2) in-doc(1) pc(1) version(x) subversion(y) }
Data wydania	26 października 2009 r.
Data ważności	Do odwołania

2.3 Podmiotowy i przedmiotowy zakres zastosowania Polityki Certyfikacji

Polityka Certyfikacji opisuje zasady stosowane przez Narodowe Centrum Certyfikacji podczas pełnienia roli podmiotu upoważnionego, której elementami są:

1. Narodowe Centrum Certyfikacji,
2. Użytkownicy końcowi:
   a. Subskrybent,
   b. Strona ufająca.

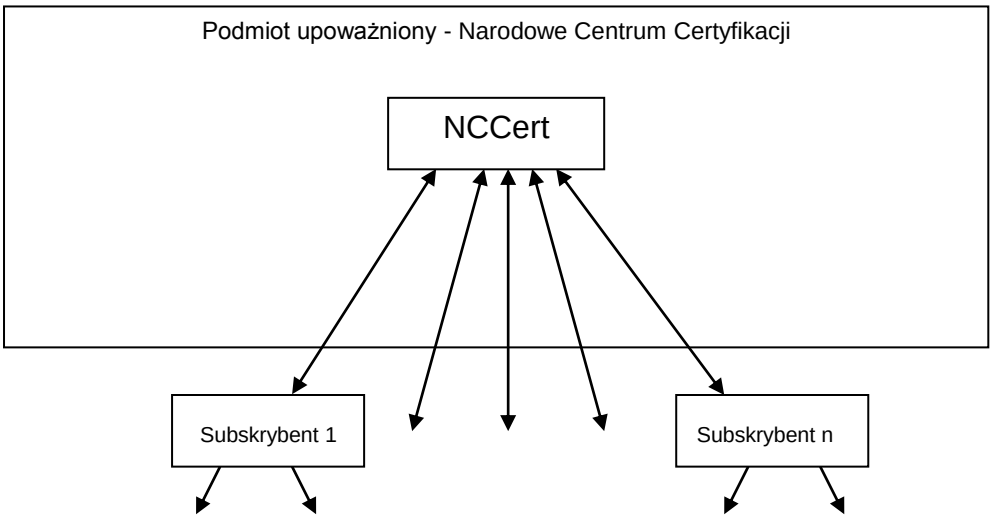
[4] Identyfikator obiektu (ang. object identifier) – identyfikator alfanumeryczny / numeryczny zarejestrowany zgodnie z normą ISO/IEC 9834-1, wskazujący w sposób unikalny na określony obiekt lub klasę obiektów.

[5] Krajowy Rejestr Identyfikatorów Obiektów (KRIO) prowadzony jest przez Unizeto Technologies SA z upoważnienia Polskiego Komitetu Normalizacyjnego, http://www.krio.pl

Postanowienia Polityki Certyfikacji są wiążące dla Narodowego Centrum Certyfikacji, Subskrybenta oraz Strony ufającej.

2.3.1 Urzędy certyfikacyjne krajowej infrastruktury klucza publicznego

Strukturę urzędów certyfikacyjnych krajowej infrastruktury klucza publicznego przedstawia Rysunek 2



Rysunek 2 Struktura krajowej infrastruktury klucza publicznego.

Narodowe Centrum Certyfikacji

Narodowe Centrum Certyfikacji jest „wierzchołkiem drzewa certyfikacji" i za zgodą oraz w imieniu ministra właściwego do spraw gospodarki wytwarza i publikuje zaświadczenie certyfikacyjne ministra właściwego do spraw gospodarki oraz wytwarza, wydaje i publikuje zaświadczenia certyfikacyjne Subskrybenta, a także wykorzystuje klucze infrastruktury poświadczone danymi służącymi do składania poświadczenia elektronicznego przez Narodowe Centrum Certyfikacji. Klucze infrastruktury są wykorzystywane do zapewnienia uwierzytelnienia osób realizujących funkcje w systemie oraz do zapewnienia integralności danych.

W ramach Narodowego Centrum Certyfikacji funkcjonują dwa niezależne urzędy:

Urząd *stary Root*, z identyfikatorem wyróżniającym wskazującym na CZiC Centrast SA, realizujący następujące czynności:

1. unieważnianie zaświadczeń certyfikacyjnych Subskrybentów, wydanych przez urząd ***Stary Root***,
2. wystawianie i publikowanie list unieważnionych zaświadczeń certyfikacyjnych ARL wydanych przez urząd ***stary Root***.

Urząd ***Stary Root*** funkcjonuje do czasu wygaśnięcia zaświadczenia certyfikacyjnego Ministra Gospodarki wskazującego na CZiC Centrast SA, tzn. do dnia 14 grudnia 2013 r. Po zakończeniu działalności urzędu ***Stary Root***, na stronie internetowej **www.nccert.pl** będą dostępne: ostatnia lista unieważnionych

zaświadczeń certyfikacyjnych ARL oraz lista zaświadczeń certyfikacyjnych wydanych przez urząd ***stary Root***.[6]

Urząd *nowy Root*, z nowym identyfikatorem wyróżniającym wskazującym na ministra właściwego do spraw gospodarki, realizujący następujące czynności:
1. wystawianie, wydawanie i publikowanie zaświadczeń certyfikacyjnych dla Subskrybentów, wydanych przez urząd ***nowy Root***,
2. unieważnianie zaświadczeń certyfikacyjnych Subskrybentów, wydanych przez urząd ***nowy Root***,
3. wystawianie i publikowanie list unieważnionych zaświadczeń certyfikacyjnych ARL wydanych przez urząd ***nowy Root***.

Subskrybent

Subskrybent, to, zgodnie z art. 3 pkt 15 *Ustawy o podpisie elektronicznym*, podmiot świadczący usługi certyfikacyjne, wpisany do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne.

2.3.2 Punkty rejestracji

Punkt rejestracji Narodowego Centrum Certyfikacji jest w Narodowym Banku Polskim odpowiedzialny za odbieranie i realizację poleceń ministra właściwego do spraw gospodarki, w tym poleceń publikacji informacji o unieważnieniu zaświadczeń certyfikacyjnych, a także za wymianę dokumentów oraz informacji pomiędzy Subskrybentem oraz ministrem właściwym do spraw gospodarki, a Narodowym Centrum Certyfikacji.

2.3.3 Użytkownicy końcowi

Użytkownikami końcowymi zaświadczeń certyfikacyjnych wydawanych przez Narodowe Centrum Certyfikacji są Subskrybent oraz Strona ufająca.

Subskrybentem jest kwalifikowany podmiot świadczący usługi certyfikacyjne, któremu zaświadczenie certyfikacyjne, w imieniu i na polecenie ministra właściwego do spraw gospodarki, wydaje Narodowe Centrum Certyfikacji.

Strona ufająca to osoba fizyczna, osoba prawna lub jednostka organizacyjna nie posiadająca osobowości prawnej, która zawarła z podmiotem świadczącym usługi certyfikacyjne umowę o świadczenie usług certyfikacyjnych, lub mogąca działać w granicach określonych w polityce certyfikacji, w oparciu o certyfikat lub inne dane elektroniczne poświadczone przez podmiot świadczący usługi certyfikacyjne.

2.3.4 Zakres zastosowania Polityki Certyfikacji

Polityka Certyfikacji znajduje zastosowanie w procesie wytwarzania i zarządzania zaświadczeniami certyfikacyjnymi wydanymi przez Narodowe Centrum Certyfikacji w imieniu ministra właściwego do spraw gospodarki.

Narodowe Centrum Certyfikacji wydaje, w imieniu i na polecenie ministra

[6] Umożliwi to przeprowadzenie ewentualnej weryfikacji zaświadczeń certyfikacyjnych i certyfikatów „w przeszłości”, np. dla celów procesowych.

właściwego do spraw gospodarki, zaświadczenia certyfikacyjne Subskrybenta. Zaświadczenia certyfikacyjne wydane Subskrybentom:

1. Przyporządkowują dane służące do weryfikacji poświadczenia elektronicznego do danego kwalifikowanego podmiotu świadczącego usługi certyfikacyjne – Subskrybenta;
2. Określają zakres zastosowania danych służących do składania poświadczenia elektronicznego;
3. Zawierają następujący identyfikator polityki certyfikacji: „{ 2 5 29 32 0 }".

2.4 Kontakt z Narodowym Centrum Certyfikacji

2.4.1 Zatwierdzanie polityki certyfikacji

Polityka Certyfikacji stosowana przez Narodowe Centrum Certyfikacji, podczas pełnienia roli podmiotu upoważnionego, zatwierdzana jest przez Zarząd Narodowego Banku Polskiego, z uwzględnieniem opinii ministra właściwego do spraw gospodarki.

2.4.2 Kontakt z Narodowym Centrum Certyfikacji

W celu uzyskania dalszych informacji dotyczących usług i działalności Narodowego Centrum Certyfikacji prosimy o kontakt:

Narodowy Bank Polski
Departament Ochrony
Narodowe Centrum Certyfikacji
ul. Świętokrzyska 11/21
00-919 Warszawa
Polska
tel.: (+48 22) 653 -13 -18
fax: (+48 22) 653 11 74, 826 55 86
http://www.nccert.pl
e-mail: nccert@nccert.pl

3 Postanowienia ogólne

3.1 Zobowiązania

Rozdział przedstawia postanowienia Polityki Certyfikacji związane z zobowiązaniami i odpowiedzialnością Narodowego Centrum Certyfikacji w stosunku do Subskrybenta oraz Strony ufającej.

3.1.1 Zobowiązania Narodowego Centrum Certyfikacji

Narodowe Centrum Certyfikacji zobowiązuje się do należytego pełnienia roli podmiotu upoważnionego, zgodnie z wymogami prawa obowiązującego na terytorium Rzeczypospolitej Polskiej oraz postanowieniami Polityki Certyfikacji, a w szczególności do:

1. Wytwarzania zaświadczeń certyfikacyjnych ministra właściwego do spraw gospodarki;
2. Wytwarzania, wydawania i publikacji informacji o unieważnieniu zaświadczeń certyfikacyjnych na polecenie ministra właściwego do spraw gospodarki;
3. Publikacji zaświadczeń certyfikacyjnych ministra właściwego do spraw gospodarki;
4. Publikacji wydanych zaświadczeń certyfikacyjnych;
5. Publikacji list wydanych zaświadczeń certyfikacyjnych;
6. Terminowej publikacji aktualnych list unieważnionych zaświadczeń certyfikacyjnych;
7. Zapewnienia należytego poziomu bezpieczeństwa prowadzenia działalności;
8. Zapewnienia odpowiedniej ochrony przetwarzanych danych osobowych;
9. Używania danych służących do składania poświadczenia elektronicznego zgodnie z *Ustawą o podpisie elektronicznym* wraz z aktami wykonawczymi;
10. Wykorzystywania przy pełnieniu roli podmiotu upoważnionego, w szczególności przy tworzeniu rejestrów zdarzeń oraz tworzeniu listy unieważnionych zaświadczeń certyfikacyjnych, rozwiązań zapewniających synchronizację z Międzynarodowym Wzorcem Czasu (Coordinated Universal Time), zwanym dalej "UTC", z dokładnością do 1 sekundy;
11. Publikowania w Repozytorium skrótów danych służących do weryfikacji poświadczeń elektronicznych wykorzystywanych do weryfikacji poświadczeń elektronicznych składanych przez Narodowe Centrum Certyfikacji, jako podmiot upoważniony, uzyskanych w wyniku funkcji skrótu SHA-1, której specyfikacja techniczna jest jednoznacznie określona poprzez następujący identyfikator obiektu: "iso(1) identifiedOrganization(3) olW(14) olWSecSig (3) olWSecAlgorithm(2) 26".

3.1.2 Zobowiązania Subskrybenta

Subskrybent jest zobowiązany w szczególności do:

1. Stosowania się do postanowień *Ustawy o podpisie elektronicznym*, odpowiednich przepisów wykonawczych oraz właściwych aktów prawnych obowiązujących na terytorium Rzeczypospolitej Polskiej;
2. Zapoznania się i akceptacji oraz przestrzegania zasad określonych w Polityce Certyfikacji;
3. Spełniania wymogów bezpieczeństwa, nakładanych przez *Ustawę o podpisie elektronicznym*, stosowne przepisy wykonawcze oraz normy i obowiązujące standardy, w tym do prawidłowego i bezpiecznego wytworzenia danych służących do składania poświadczenia elektronicznego oraz ochrony tych danych przed utratą, kradzieżą, ujawnieniem, modyfikacją oraz nieautoryzowanym dostępem i użyciem;
4. Niezwłocznego powiadomienia ministra właściwego do spraw gospodarki o naruszeniu bezpieczeństwa lub o podejrzeniu naruszenia bezpieczeństwa danych służących do składania poświadczenia elektronicznego;
5. Sprawdzenia i potwierdzenia poprawności danych zawartych w wydanym zaświadczeniu certyfikacyjnym;
6. Wytworzenia i dostarczenia zaświadczenia certyfikacyjnego dla Narodowego Centrum Certyfikacji;
7. Zapoznawania się z treścią korespondencji przesyłanej przez Narodowe Centrum Certyfikacji.

3.1.3 Zobowiązania Strony ufającej

Strona ufająca powinna rzetelnie, zgodnie z wymogami *Ustawy o podpisie elektronicznym*, dokonać weryfikacji każdego podpisu i poświadczenia elektronicznego, któremu zamierza zaufać, ze szczególnym uwzględnieniem informacji zawartych w pkt. 2.1.1 niniejszej Polityki Certyfikacji..

3.1.4 Repozytorium Narodowego Centrum Certyfikacji

Narodowe Centrum Certyfikacji gwarantuje – zgodne z *Ustawą o podpisie elektronicznym* oraz odpowiednimi przepisami wykonawczymi – publikowanie w Repozytorium Narodowego Centrum Certyfikacji:

1. Zaświadczeń certyfikacyjnych wydanych przez Narodowe Centrum Certyfikacji;
2. Wytworzonych i wydanych przez Narodowe Centrum Certyfikacji aktualnych list unieważnionych zaświadczeń certyfikacyjnych;
3. Rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne.

3.2 Odpowiedzialność

Rozdział przedstawia zakres odpowiedzialności Narodowego Centrum Certyfikacji oraz zakres odpowiedzialności użytkowników końcowych.

3.2.1 Odpowiedzialność Narodowego Centrum Certyfikacji

Narodowe Centrum Certyfikacji odpowiada za:

1. Prawidłowe wytwarzanie zaświadczeń certyfikacyjnych ministra właściwego do spraw gospodarki;
2. Prawidłowe wytwarzanie, wydawanie i publikację informacji o unieważnieniu zaświadczeń certyfikacyjnych na polecenie ministra właściwego do spraw gospodarki;
3. Prawidłową publikację zaświadczeń certyfikacyjnych ministra właściwego do spraw gospodarki;
4. Publikację wydanych zaświadczeń certyfikacyjnych;
5. Publikację list wydanych zaświadczeń certyfikacyjnych;
6. Terminową publikację aktualnych list unieważnionych zaświadczeń certyfikacyjnych;
7. Zapewnienie należytego poziomu bezpieczeństwa prowadzenia działalności;
8. Zapewnienie odpowiedniej ochrony przetwarzanych danych osobowych;
9. Używanie danych służących do składania poświadczenia elektronicznego zgodnie z *Ustawą o podpisie elektronicznym* wraz z aktami wykonawczymi;
10. Wykorzystywanie przy pełnieniu roli podmiotu upoważnionego, w szczególności przy tworzeniu rejestrów zdarzeń oraz tworzeniu list unieważnionych zaświadczeń certyfikacyjnych, rozwiązań zapewniających synchronizację z "UTC", z dokładnością do 1 sekundy;
11. Publikowanie w Repozytorium skrótów danych służących do weryfikacji poświadczeń elektronicznych wykorzystywanych do weryfikacji poświadczeń elektronicznych składanych przez Narodowe Centrum Certyfikacji, jako podmiot upoważniony, uzyskanych w wyniku funkcji skrótu SHA-1, której specyfikacja techniczna jest jednoznacznie określona poprzez następujący identyfikator obiektu: "iso(1) identifiedOrganization(3) olW(14) olWSecSig (3) olWSecAlgorithm(2) 26".

3.2.2 Odpowiedzialność Subskrybenta

Subskrybent jest odpowiedzialny w szczególności za:

1. Wypełnianie postanowień *Ustawy o podpisie elektronicznym*, odpowiednich przepisów wykonawczych oraz innych aktów prawnych obowiązujących na terytorium Rzeczypospolitej Polskiej;
2. Przestrzeganie zasad określonych w Polityce Certyfikacji;
3. Poprawne wypełnianie wniosków i żądań składanych w punkcie rejestracji Narodowego Centrum Certyfikacji;
4. Spełnienie wymogów bezpieczeństwa, nakładanych przez *Ustawę o podpisie elektronicznym*, obowiązujące przepisy wykonawcze oraz normy i standardy, w tym do prawidłowego i bezpiecznego wytworzenia danych służących do składania poświadczenia elektronicznego oraz ochrony tych danych przed utratą, kradzieżą, ujawnieniem, modyfikacją oraz nieautoryzowanym użyciem;
5. Niezwłoczne powiadomienie ministra właściwego do spraw gospodarki o naruszeniu bezpieczeństwa lub o podejrzeniu naruszenia bezpieczeństwa danych służących do składania poświadczenia elektronicznego używanych przez Subskrybenta;
6. Sprawdzenie poprawności danych zawartych w wydanym zaświadczeniu certyfikacyjnym;

7. Wytworzenie i wydanie zaświadczenia certyfikacyjnego dla Narodowego Centrum Certyfikacji, o którym mowa w § 1 pkt 3 Rozporządzenia Ministra Gospodarki z dnia 9 sierpnia 2002 r. w sprawie określenia szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem elektronicznym (Dz. U. Nr 128, poz. 1101);
8. Przesłanie potwierdzenia poprawności danych zawartych w wydanym zaświadczeniu certyfikacyjnym;
9. Niezwłoczne zawiadamianie, nie później niż w terminie 7 dni od zmiany stanu faktycznego lub prawnego, ministra właściwego do spraw gospodarki o każdej zmianie danych zawartych we wniosku, o którym mowa w art. 24 ust. 2 *Ustawy o podpisie elektronicznym*.

3.2.3 Odpowiedzialność Strony ufającej

Nikt (ani Narodowe Centrum Certyfikacji ani Subskrybent) poza Stroną ufającą nie ponosi odpowiedzialności za dokonanie przez Stronę ufającą poprawnej i rzetelnej weryfikacji każdego podpisu i poświadczenia elektronicznego, któremu zamierza zaufać, w tym certyfikatów oraz zaświadczeń certyfikacyjnych.

Zaufanie niekompletnie lub negatywnie zweryfikowanemu podpisowi lub poświadczeniu elektronicznemu następuje na wyłączną odpowiedzialność Strony ufającej.

3.3 Odpowiedzialność odszkodowawcza

Narodowe Centrum Certyfikacji ponosi odpowiedzialność za szkody związane z pełnieniem roli podmiotu upoważnionego.

3.3.1 Wyłączenia odpowiedzialności

Narodowe Centrum Certyfikacji nie ponosi wobec Strony ufającej odpowiedzialności za szkody powstałe na skutek niedopełnienia przez nie swoich obowiązków oraz niedopełnienia obowiązków przez Subskrybenta lub inną Stronę ufającą, włączając w to:

1. Zaniedbanie obowiązku weryfikacji podpisu elektronicznego;
2. Zaniedbanie obowiązku weryfikacji poświadczenia elektronicznego;
3. Zaufanie zweryfikowanemu niekompletnie lub negatywnie podpisowi bądź poświadczeniu elektronicznemu;
4. Zaufanie podpisanym lub poświadczonym elektronicznie dokumentom zawierającym nieprawdziwe dane;
5. Poświadczenie elektroniczne nieprawdziwych danych przez Subskrybenta;
6. Niedopełnienie obowiązku ochrony danych służących do składania poświadczenia elektronicznego przez Subskrybenta;
7. Niedopełnienie obowiązku ochrony danych służących do składania podpisu elektronicznego.

3.3.2 Relacje powiernicze

Wydanie zaświadczenia certyfikacyjnego nie czyni z Narodowego Centrum Certyfikacji agenta, powiernika czy reprezentanta podmiotu, któremu wydane zostaje zaświadczenie certyfikacyjne.

3.3.3 Procesy zarządzania infrastrukturą klucza publicznego

Narodowe Centrum Certyfikacji nie odpowiada za procesy związane ze świadczeniem usług certyfikacyjnych przez Subskrybenta.

3.4 Interpretacja i wykonywanie aktów prawnych

3.4.1 Obowiązujące akty prawne

Działalność Narodowego Centrum Certyfikacji zgodna jest z obowiązującymi na terytorium Rzeczypospolitej Polskiej aktami prawnymi, w szczególności z:

1. *Ustawą o podpisie elektronicznym* i jej zapisami dotyczącymi wymagań oraz obowiązków związanych z pełnieniem roli podmiotu upoważnionego;
2. Odpowiednimi aktami wykonawczymi do *Ustawy o podpisie elektronicznym*.

3.4.2 Rozłączność postanowień, zachowanie ważności postanowień, zasady powiadamiania

Jeśli jakiekolwiek postanowienie Polityki Certyfikacji stałoby się nieważne lub niewykonalne, nie wpłynie to w żaden sposób na ważność i wykonalność pozostałych postanowień.

Każde postanowienie Polityki Certyfikacji dotyczące ograniczenia odpowiedzialności jest wiążące i niezależne od pozostałych postanowień.

Narodowe Centrum Certyfikacji powiadamia Subskrybenta o:

1. Planowanych zmianach w Polityce Certyfikacji;
2. Terminie wejścia w życie nowej wersji Polityki Certyfikacji;
3. Zbliżającym się terminie wymiany danych służących do składania poświadczenia elektronicznego, wykorzystywanych przez podmiot upoważniony.

Powiadomienie, o którym mowa powyżej, dokonywane jest za pomocą poczty elektronicznej. Dodatkowo informacje te publikowane są w Repozytorium.

Subskrybent ma obowiązek zapoznawania się z treścią przesyłanej przez Narodowe Centrum Certyfikacji poczty elektronicznej. Potwierdzenie odebrania i zapoznania się z treścią poczty elektronicznej nie jest wymagane.

3.5 Opłaty

3.5.1 Opłaty za wydanie lub odnowienie zaświadczenia certyfikacyjnego

Narodowe Centrum Certyfikacji nie pobiera od Subskrybenta opłat za wytwarzanie, wydawanie i publikację zaświadczeń certyfikacyjnych.

Zgodnie z ustawą o podpisie elektronicznym nie przewiduje się odnawiania zaświadczeń certyfikacyjnych.

3.5.2 Opłaty za dostęp do wydanego zaświadczenia certyfikacyjnego

Narodowe Centrum Certyfikacji nie pobiera opłat za dostęp do danych umieszczonych w Repozytorium, w tym za pobieranie zaświadczeń certyfikacyjnych.

3.5.3 Opłaty za publikację informacji o unieważnieniu oraz dostęp do list unieważnionych zaświadczeń certyfikacyjnych

Narodowe Centrum Certyfikacji nie pobiera opłat za publikację informacji o unieważnieniu zaświadczenia certyfikacyjnego.

Narodowe Centrum Certyfikacji nie pobiera opłat za dostęp do list unieważnionych zaświadczeń certyfikacyjnych umieszczonych w Repozytorium.

3.5.4 Inne opłaty

Polityka Certyfikacji jest w wersji elektronicznej nieodpłatnie dostępna w Repozytorium.

Narodowe Centrum Certyfikacji może pobierać opłaty za udostępnienie kopii powyższych dokumentów w postaci wydrukowanej.

3.5.5 Zasady zwrotu wniesionych opłat

Nie ma zastosowania.

3.6 Repozytorium i publikacje

3.6.1 Informacje publikowane

Narodowe Centrum Certyfikacji publikuje następujące dokumenty i informacje związane z pełnieniem roli podmiotu upoważnionego:

1. Zaświadczenia certyfikacyjne ministra właściwego do spraw gospodarki,
2. Wydane zaświadczenia certyfikacyjne;
3. Listy wydanych zaświadczeń certyfikacyjnych kwalifikowanych podmiotów świadczących usługi certyfikacyjne;
4. Aktualne listy unieważnionych zaświadczeń certyfikacyjnych;
5. Rejestr kwalifikowanych podmiotów świadczących usługi certyfikacyjne;
6. Politykę Certyfikacji (wersję poprzednią i aktualnie obowiązującą);
7. Informacje o proponowanych zmianach w Polityce Certyfikacji;
8. Ogłoszenia dotyczące bieżącej działalności.

Wyżej wymienione informacje i dokumenty są dostępne w Repozytorium.

3.6.2 Częstotliwość publikacji

Narodowe Centrum Certyfikacji publikuje w Repozytorium:

1. Zaświadczenie certyfikacyjne ministra właściwego do spraw gospodarki – niezwłocznie po jego wytworzeniu;
2. Zaświadczenie certyfikacyjne Subskrybenta – niezwłocznie po jego wytworzeniu i wydaniu;

3. Aktualną listę wydanych zaświadczeń certyfikacyjnych Subskrybenta – po wytworzeniu i wydaniu zaświadczenia certyfikacyjnego;
4. Aktualne listy unieważnionych zaświadczeń certyfikacyjnych – raz dziennie (z wyłączeniem sobót, niedziel oraz wszystkich dni ustawowo wolnych od pracy) oraz każdorazowo, niezwłocznie po unieważnieniu zaświadczenia certyfikacyjnego – nie później niż w ciągu 1 godziny od otrzymania przez Narodowe Centrum Certyfikacji, od ministra właściwego do spraw gospodarki, polecenia publikacji informacji o unieważnieniu zaświadczenia certyfikacyjnego Subskrybenta[7];
5. Aktualny rejestr kwalifikowanych podmiotów świadczących usługi certyfikacyjne, modyfikowany każdorazowo, niezwłocznie po otrzymaniu polecenia dokonania (usunięcia) wpisu do (z) rejestru od ministra właściwego do spraw gospodarki;
6. Politykę Certyfikacji – wersję poprzednią i aktualnie obowiązującą, po każdorazowej zmianie dokumentu, niezwłocznie po zatwierdzeniu zmian przez Zarząd Narodowego Banku Polskiego, wraz z informacją o dacie wejścia w życie uchwalonych zmian;
7. Informacje dodatkowe, np. ogłoszenia oraz informacje o proponowanych zmianach w Polityce Certyfikacji – w razie takiej potrzeby.

3.6.3 Kontrola dostępu

Informacje publikowane w Repozytorium są publicznie dostępne do odczytu.

Publikacja tych informacji dokonywana jest wyłącznie przez uprawnionych pracowników Narodowego Banku Polskiego.

3.6.4 Repozytorium

W Repozytorium publikuje się:

1. Zaświadczenia certyfikacyjne ministra właściwego do spraw gospodarki;
2. Zaświadczenia certyfikacyjne wytworzone i wydane na polecenie ministra właściwego do spraw gospodarki;
3. Listy wydanych zaświadczeń certyfikacyjnych kwalifikowanych podmiotów świadczących usługi certyfikacyjne
4. Listy unieważnionych zaświadczeń certyfikacyjnych;
5. Rejestr kwalifikowanych podmiotów świadczących usługi certyfikacyjne;
6. Politykę Certyfikacji (wersję poprzednią i aktualnie obowiązującą);
7. Informacje dodatkowe.

3.7 Kontrola działalności Narodowego Centrum Certyfikacji

Narodowe Centrum Certyfikacji, jako podmiot upoważniony, podlega szczególnemu nadzorowi ministra właściwego do spraw gospodarki.

Na polecenie ministra właściwego do spraw gospodarki wykonywane są kontrole zgodności działalności Narodowego Centrum Certyfikacji z postanowieniami *Ustawy o podpisie elektronicznym* oraz odpowiednimi przepisami wykonawczymi.

[7] opracowane są procedury awaryjne w przypadku zaistnienia konieczności wykonania w/w działań w sobotę, niedzielę lub dzień ustawowo wolny od pracy.

Dodatkowo, w celu zapewnienia należytego wywiązywania się ze swoich obowiązków, Narodowe Centrum Certyfikacji wdrożyło procedury wewnętrznego nadzoru nad zgodnością stosowanych praktyk z wymogami *Ustawy o podpisie elektronicznym* oraz Polityki Certyfikacji i wypełnianiem postanowień innych dokumentów regulujących działanie Narodowego Centrum Certyfikacji.

3.7.1 Częstotliwość kontroli

Kontrola sprawdzająca prawidłowość pełnienia przez Narodowe Centrum Certyfikacji roli podmiotu upoważnionego, dokonywana jest na zlecenie ministra właściwego do spraw gospodarki w zakresie przez niego wskazanym. Kontrolę przeprowadzają upoważnieni przez ministra właściwego do spraw gospodarki kontrolerzy, na podstawie dowodu tożsamości i imiennego upoważnienia określającego zakres i podstawę prawną podjęcia kontroli.

Wewnętrzna kontrola zgodności z wymogami *Ustawy o podpisie elektronicznym* przeprowadzana jest zgodnie z zasadami obowiązującymi w Narodowym Banku Polskim.

3.7.2 Tożsamość i kwalifikacje kontrolera

Kontrolę działalności Narodowego Centrum Certyfikacji pod względem zgodności z postanowieniami *Ustawy o podpisie elektronicznym*, przeprowadzają upoważnieni przez ministra pracownicy komórki organizacyjnej ministerstwa zapewniającego obsługę ministra właściwego do spraw gospodarki, zwani dalej "kontrolerami", identyfikowani na podstawie dowodu tożsamości i imiennego upoważnienia określającego zakres i podstawę prawną podjęcia kontroli.

Kontrolę wewnętrzną przeprowadzają upoważnieni pracownicy Narodowego Banku Polskiego lub wskazanego przez Narodowy Bank Polski audytora, na podstawie zawartej umowy.

3.7.3 Związek kontrolera z podmiotem kontroli

Zleconej przez ministra kontroli działalności Narodowego Centrum Certyfikacji nie mogą dokonywać pracownicy zatrudnieni w Narodowym Banku Polskim.

Kontrolę wewnętrzną przeprowadzają upoważnieni pracownicy Narodowego Banku Polskiego bezpośrednio niezwiązani z obsługą Narodowego Centrum Certyfikacji lub wskazanego przez Narodowy Bank Polski audytora, na podstawie zawartej umowy.

3.7.4 Zakres kontroli

Zakres kontroli przeprowadzanej na zlecenie ministra określany jest w upoważnieniu do przeprowadzenia kontroli.

3.7.5 Usuwanie usterek

Wyniki kontroli wewnętrznej przekazywane są Dyrektorowi Departamentu Ochrony w Narodowym Banku Polskim, który sprawuje nadzór nad funkcjonowaniem Narodowego Centrum Certyfikacji. W przypadku stwierdzenia przez kontrolerów

nieprawidłowości, Dyrektor Departamentu Ochrony podejmuje niezwłocznie działania mające na celu realizację zaleceń pokontrolnych.

Uchybienia wykryte w trakcie kontroli dokonanej na polecenie ministra właściwego do spraw gospodarki muszą zostać usunięte w terminie przez niego określonym.

Uchybienia wykryte w trakcie kontroli wewnętrznej muszą zostać usunięte w terminie określonym przez Dyrektora Departamentu Ochrony.

3.7.6 Publikacja wyników kontroli

Wyniki kontroli wewnętrznej przedstawiane są Dyrektorowi Departamentu Ochrony, a wyniki kontroli Narodowego Centrum Certyfikacji przeprowadzanej na zlecenie ministra właściwego do spraw gospodarki – ministrowi oraz Narodowemu Centrum Certyfikacji.

Wybrane fragmenty raportu z kontroli wewnętrznej mogą, za zgodą Dyrektora Departamentu Ochrony, zostać opublikowane w Repozytorium.

3.8 Poufność informacji

Wszelkie informacje chronione są odpowiednio przed ujawnieniem zgodnie z zasadami określonymi w obowiązujących w tym zakresie aktach prawnych: *Ustawie o podpisie elektronicznym, Ustawie z dnia 29 sierpnia 1997 roku o ochronie danych osobowych* i towarzyszących im przepisach wykonawczych.

3.8.1 Informacje objęte tajemnicą

Tajemnicą objęte są wszelkie informacje związane z wypełnianiem przez Narodowe Centrum Certyfikacji roli podmiotu upoważnionego, których nieuprawnione ujawnienie mogłoby narazić na szkodę Narodowe Centrum Certyfikacji, Subskrybenta lub Stronę ufającą, a w szczególności:

1. Dane służące do składania poświadczenia elektronicznego przez Narodowe Centrum Certyfikacji;
2. Wszelkie prywatne klucze infrastruktury Narodowego Centrum Certyfikacji;
3. Parametry systemów zabezpieczeń;
4. Wszelkie informacje chronione przez prawo;
5. Dzienniki systemowe;
6. Informacje otrzymane od Subskrybenta z wyjątkiem tych, bez ujawnienia których niemożliwe jest prawidłowe wypełnianie przez Narodowe Centrum Certyfikacji roli podmiotu upoważnionego.

Nie są objęte tajemnicą informacje o naruszeniach *Ustawy o podpisie elektronicznym* przez podmiot świadczący usługi certyfikacyjne.

Obowiązek zachowania tajemnicy, o której mowa w art. 12 ust. 1 *Ustawy o podpisie elektronicznym*, trwa przez okres 10 lat od ustania stosunków prawnych wymienionych w art. 12 ust. 2 *Ustawy o podpisie elektronicznym*.

Obowiązek zachowania tajemnicy danych służących do składania poświadczeń elektronicznych trwa bezterminowo.

3.8.2 Informacje jawne

Do informacji jawnych zaliczane są w szczególności:

1. Zaświadczenia certyfikacyjne ministra właściwego do spraw gospodarki;
2. Wydane zaświadczenia certyfikacyjne;
3. Listy wydanych zaświadczeń certyfikacyjnych kwalifikowanych podmiotów świadczących usługi certyfikacyjne;
4. Listy unieważnionych zaświadczeń certyfikacyjnych;
5. Rejestr kwalifikowanych podmiotów świadczących usługi certyfikacyjne;
6. Polityka Certyfikacji;
7. Informacje o proponowanych zmianach w Polityce Certyfikacji;
8. Ogłoszenia dotyczące bieżącej działalności.

3.8.3 Udostępnianie informacji o przyczynach unieważnienia

Informacja o unieważnieniu zaświadczenia certyfikacyjnego oraz jego szczegółowych przyczynach przekazywana jest pocztą elektroniczną Subskrybentowi, którego zaświadczenie certyfikacyjne unieważniono.

Powód unieważnienia zaświadczenia certyfikacyjnego umieszczany jest na liście unieważnionych zaświadczeń certyfikacyjnych.

3.8.4 Ujawnianie informacji objętych tajemnicą

Narodowe Centrum Certyfikacji ujawnia dane traktowane jako objęte tajemnicą wyłącznie następującym podmiotom:

1. Sądom i prokuraturze – w związku z toczącym się postępowaniem;
2. Ministrowi właściwemu do spraw gospodarki – w związku ze sprawowaniem przez niego nadzoru nad działalnością podmiotów świadczących usługi certyfikacyjne oraz kontroli wypełniania przez Narodowe Centrum Certyfikacji roli podmiotu upoważnionego;
3. Innym organom państwowym upoważnionym do tego na podstawie odrębnych ustaw – w związku z prowadzonymi przez nie postępowaniami w sprawach podmiotów świadczących usługi certyfikacyjne.

Danych służących do składania poświadczenia elektronicznego wykorzystywanych przez Narodowe Centrum Certyfikacji nie udostępnia się.

3.8.5 Udostępnianie informacji za zgodą podmiotu

Nie opublikowane informacje jawne mogą być udostępnione przez Narodowe Centrum Certyfikacji na umotywowany wniosek wyłącznie za zgodą podmiotu, którego dotyczą.

3.8.6 Inne okoliczności udostępniania informacji

Nie przewiduje się udostępniania informacji w innych okolicznościach niż wymienione powyżej.

3.9 Ochrona własności intelektualnej

Narodowy Bank Polski zastrzega sobie wszelkie prawa autorskie dokumentów, w tym w postaci elektronicznej, stron internetowych oraz innych dokumentów opracowanych przez Narodowe Centrum Certyfikacji.

Jednocześnie Narodowy Bank Polski zezwala na pobieranie, kopiowanie i publikację, w tym w częściach, publikowanych dokumentów związanych z pełnieniem roli podmiotu upoważnionego, a w szczególności:

1. Wydanych zaświadczeń certyfikacyjnych;
2. List wydanych zaświadczeń certyfikacyjnych kwalifikowanych podmiotów świadczących usługi certyfikacyjne;
3. List unieważnionych zaświadczeń certyfikacyjnych;
4. Rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne;
5. Polityki Certyfikacji;
6. Zaświadczeń certyfikacyjnych ministra właściwego do spraw gospodarki.

Narodowy Bank Polski oświadcza, że jest właścicielem lub posiada licencje pozwalające na użycie sprzętu i oprogramowania koniecznego do pełnienia roli podmiotu upoważnionego.

4 Weryfikacja poleceń

Poniżej przedstawiono ogólne zasady przyjmowania poleceń ministra właściwego do spraw gospodarki dotyczących wytwarzania i wydania zaświadczenia certyfikacyjnego oraz publikacji informacji o unieważnieniu zaświadczenia certyfikacyjnego obowiązujące w Narodowym Centrum Certyfikacji.

Polityka Certyfikacji wyróżnia:

1. Przyjęcie polecenia wytworzenia i wydania zaświadczenia certyfikacyjnego Subskrybenta oraz jego odbiór– rejestrację początkową;
2. Przyjęcie polecenia publikacji informacji o unieważnieniu zaświadczenia certyfikacyjnego.

Ponieważ zawieszanie zaświadczenia certyfikacyjnego jest – zgodnie z *Ustawą o podpisie elektronicznym* – niedopuszczalne, nie przewiduje się przyjmowania wniosków związanych z tymi operacjami.

4.1 Rejestracja początkowa

Po dokonaniu wpisu podmiotu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne gospodarczych minister właściwy do spraw gospodarki wydaje Narodowemu Centrum Certyfikacji polecenie wytworzenia i wydania zaświadczenia certyfikacyjnego.

Dane zawarte w poleceniu wytworzenia zaświadczenia certyfikacyjnego są identyczne (identyfikują w sposób jednoznaczny Subskrybenta) z danymi podanymi przez Subskrybenta we wniosku o dokonanie wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne przesłanym ministrowi – wzór wniosku stanowi Załącznik nr 1 do Rozporządzeniu Ministra Gospodarki z dnia 6 sierpnia 2002 r. w sprawie wzoru i szczegółowego zakresu wniosku o dokonanie wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne (Dz. U. Nr 128, poz. 1097).

Kwalifikowany podmiot dostarcza żądanie certyfikacji w formacie PKCS#10. Żądanie certyfikacji zawiera dane niezbędne do wytworzenia zaświadczenia certyfikacyjnego, a w szczególności: określenie nazwy Subskrybenta oraz dane służące do weryfikacji poświadczenia elektronicznego Subskrybenta.

Uprawnione osoby, pełniące funkcje w Narodowym Centrum Certyfikacji, wczytują dostarczone żądanie certyfikacji i wytwarzają zaświadczenie certyfikacyjne.

4.1.1 Typy nazw

Format zaświadczenia certyfikacyjnego jest określony przez przepisy wykonawcze do *Ustawy o podpisie elektronicznym.*

Zaświadczenie certyfikacyjne zawiera w swojej treści szereg nazw określających w szczególności wydawcę zaświadczenia certyfikacyjnego oraz Subskrybenta.

4.1.2 Konieczność używania nazw znaczących

Nazwy umieszczone w zaświadczeniu certyfikacyjnym muszą umożliwiać jednoznaczną identyfikację Subskrybenta oraz wydawcę zaświadczenia

certyfikacyjnego – Narodowe Centrum Certyfikacji w imieniu ministra właściwego do spraw gospodarki[8].

Szczegółowe wymagania dotyczące nazw umieszczanych w zaświadczeniach certyfikacyjnych określono w Załączniku nr 2 do Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. Nr 128, poz. 1094).

4.1.3 Unikalność nazw

Nazwa wyróżniająca Subskrybenta musi zapewnić jednoznaczne rozróżnienie Subskrybenta w ramach krajowej infrastruktury klucza publicznego.

4.1.4 Procedura rozstrzygania sporów związanych z reklamacją nazw

Nie ma zastosowania.

4.1.5 Rozpoznawanie, uwierzytelnienie oraz rola znaków towarowych

Nie ma zastosowania.

4.1.6 Dowód posiadania danych służących do składania poświadczenia elektronicznego

Dowodem posiadania danych służących do składania poświadczenia elektronicznego skojarzonych z danymi służącymi do weryfikacji poświadczenia elektronicznego znajdującymi się w żądaniu certyfikacji, jest weryfikacja poświadczenia elektronicznego złożonego pod tym żądaniem certyfikacji, dokonana przy pomocy danych służących do weryfikacji poświadczenia elektronicznego znajdujących się w żądaniu certyfikacji.

Narodowe Centrum Certyfikacji dokonuje porównania danych służących do weryfikacji poświadczenia elektronicznego znajdujących się w żądaniu certyfikacji z danymi służącymi do weryfikacji poświadczenia elektronicznego, które zostały już wcześniej przyporządkowane do innego Subskrybenta w wydanych zaświadczeniach certyfikacyjnych.

W przypadku powtórzenia się tych danych Narodowe Centrum Certyfikacji powiadamia o tym ministra właściwego do spraw gospodarki.

4.1.7 Uwierzytelnienie tożsamości Subskrybenta

Narodowe Centrum Certyfikacji nie uwierzytelnia tożsamości Subskrybenta.

Zaświadczenia certyfikacyjne wydawane są wyłącznie na polecenie ministra właściwego do spraw gospodarki, po uzyskaniu wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne.

[8] do momentu wymiany w 2009 roku danych służących do składania poświadczeń elektronicznych Narodowego Centrum Certyfikacji przejętych od Centrum Zaufania i Certyfikacji CENTRAST S.A., nazwą wydawcy zaświadczenia certyfikacyjnego, w imieniu ministra właściwego do spraw gospodarki, był CENTRAST SA (patrz rozdział 2.1.1).

4.2 Odnowienie zaświadczenia certyfikacyjnego

Nie ma zastosowania.

4.3 Odnowienie zaświadczenia certyfikacyjnego po unieważnieniu

Nie ma zastosowania.

4.4 Żądanie unieważnienia zaświadczenia certyfikacyjnego

Publikacja informacji o unieważnieniu zaświadczenia certyfikacyjnego może być dokonana jedynie na polecenie ministra właściwego do spraw gospodarki.

Żądanie unieważnienia zaświadczenia certyfikacyjnego należy kierować bezpośrednio do ministra właściwego do spraw gospodarki.

5 Wymagania eksploatacyjne

5.1 Wniosek o wydanie zaświadczenia certyfikacyjnego

5.1.1 Wniosek składany przez Subskrybenta

Narodowe Centrum Certyfikacji wytwarza i wydaje zaświadczenie certyfikacyjne po otrzymaniu stosownego polecenia od ministra właściwego do spraw gospodarki.

Zaświadczenie certyfikacyjne wydawane przez Narodowe Centrum Certyfikacji Subskrybentowi jest zaświadczeniem certyfikacyjnym, o którym mowa w § 1 pkt 2 Rozporządzenia Ministra Gospodarki z dnia 9 sierpnia 2002 r. w sprawie określenia szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem elektronicznym (Dz. U. Nr 128, poz. 1101).

Wydane zaświadczenie certyfikacyjne przeznaczone jest do świadczenia usług certyfikacyjnych przez Subskrybenta. Zakres zastosowania zaświadczenia certyfikacyjnego wydanego przez Narodowe Centrum Certyfikacji nie jest przez Narodowe Centrum Certyfikacji ograniczany i wynika z *Ustawy o podpisie elektronicznym* oraz towarzyszących jej aktów wykonawczych. Zakres zastosowania zaświadczenia certyfikacyjnego wynika z jego treści.

Zgodnie z § 27 Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. Nr 128, poz. 1094), dane służące do składania poświadczenia elektronicznego kwalifikowanych certyfikatów, wykorzystywane przez Subskrybenta w ramach danej polityki certyfikacji, mogą być dodatkowo wykorzystywane wyłącznie do poświadczania kluczy infrastruktury, list zawieszonych i unieważnionych certyfikatów, list unieważnionych zaświadczeń certyfikacyjnych oraz zaświadczeń certyfikacyjnych, zgodnie z § 4 ust. 2 i 10 Rozporządzenia Ministra Gospodarki z dnia 9 sierpnia 2002 r. w sprawie określania szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem elektronicznym (Dz. U. Nr 128, poz. 1101).

W celu wytworzenia zaświadczenia certyfikacyjnego Subskrybent przygotowuje żądanie certyfikacji w formacie PKCS#10, zgodne z profilem określonym w załączniku nr 3 do niniejszej Polityki Certyfikacji. Żądanie certyfikacji powinno być dostarczone na nośniku elektronicznym.

5.2 Wytworzenie i wydanie zaświadczenia certyfikacyjnego

5.2.1 Wytworzenie i wydanie zaświadczenia certyfikacyjnego Subskrybenta

Przygotowane przez Subskrybenta żądanie certyfikacji w formacie PKCS#10 wprowadzane jest do systemu przez uprawnioną osobę pełniącą funkcję w Narodowym Centrum Certyfikacji. Osoba, o której mowa dokonuje weryfikacji

danych zawartych w żądaniu z poleceniem wytworzenia i wydania zaświadczenia certyfikacyjnego przesłanym przez ministra właściwego do spraw gospodarki, po czym zatwierdza operację wytworzenia zaświadczenia certyfikacyjnego.

Narodowe Centrum Certyfikacji wytwarza zaświadczenie certyfikacyjne niezwłocznie po otrzymaniu od ministra właściwego do spraw gospodarki polecenia jego wytworzenia.

Wytworzone zaświadczenie certyfikacyjne wraz z informacją o zakresie zastosowania zaświadczenia certyfikacyjnego oraz wykorzystania danych służących do składania poświadczenia elektronicznego doręczane jest – niezwłocznie po wytworzeniu – przedstawicielowi Subskrybenta za pisemnym potwierdzeniem odbioru, w terminie zgodnym z art. 26 ust. 2 *Ustawy o podpisie elektronicznym*.

Wytworzenie i wydanie Subskrybentowi kolejnego zaświadczenia certyfikacyjnego jest dokonywane na polecenie ministra właściwego do spraw gospodarki.

Po uzyskaniu zgody ministra na wydanie kolejnego zaświadczenia certyfikacyjnego dostarczane jest do Narodowego Centrum Certyfikacji żądanie certyfikacji w formacie PKCS#10.

Wytworzone i wydane zaświadczenie certyfikacyjne jest publikowane w Repozytorium.

Operacje związane z wytworzeniem i wydaniem zaświadczenia certyfikacyjnego zapisywane są w odpowiednim rejestrze zdarzeń systemu informatycznego.

5.3 Akceptacja zaświadczenia certyfikacyjnego

Subskrybent zobowiązany jest do sprawdzenia poprawności danych zawartych w wydanym zaświadczeniu certyfikacyjnym.

Jeśli zaświadczenie certyfikacyjne, o którym mowa w § 1 pkt 2 Rozporządzenia Ministra Gospodarki z dnia 9 sierpnia 2002 r. w sprawie określania szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem elektronicznym (Dz. U. Nr 128, poz. 1101), zawiera poprawne dane, to Subskrybent jest zobowiązany do wytworzenia zaświadczenia certyfikacyjnego, o którym mowa w § 1 pkt 3 tego Rozporządzenia Ministra Gospodarki.

Subskrybent jest zobowiązany do wytworzenia i wydania powyższego zaświadczenia certyfikacyjnego zgodnie z § 4 ust. 3 Rozporządzenia Ministra Gospodarki z dnia 9 sierpnia 2002 r. w sprawie określenia szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem elektronicznym (Dz. U. Nr 128, poz. 1101).

W razie stwierdzenia nieprawidłowości w treści wydanego zaświadczenia certyfikacyjnego Subskrybent zobowiązany jest niezwłocznie zawiadomić o tym fakcie ministra właściwego do spraw gospodarki oraz Narodowe Centrum Certyfikacji. Informacja musi być złożona na piśmie nie później niż w terminie 7 dni od daty wydania zaświadczenia certyfikacyjnego.

W przypadku opisanym powyżej, na żądanie ministra właściwego do spraw gospodarki, Narodowe Centrum Certyfikacji publikuje informację o unieważnieniu tego zaświadczenia certyfikacyjnego i niezwłocznie wytwarza i wydaje nowe zaświadczenie certyfikacyjne.

Wykorzystanie przez Subskrybenta danych służących do składania poświadczenia elektronicznego do świadczenia usług certyfikacyjnych jest jednoznaczne z akceptacją wydanego zaświadczenia certyfikacyjnego.

5.4 Unieważnienie i zawieszanie zaświadczenia certyfikacyjnego

Publikacji informacji o unieważnieniu zaświadczenia certyfikacyjnego może zażądać jedynie minister właściwy do spraw gospodarki.

Unieważnienie zaświadczenia certyfikacyjnego nie może następować z mocą wsteczną.

Zawieszanie zaświadczeń certyfikacyjnych jest niedopuszczalne.

5.4.1 Okoliczności unieważnienia zaświadczenia certyfikacyjnego

Zaświadczenie certyfikacyjne unieważnia jedynie minister właściwy do spraw gospodarki.

Polityka Certyfikacji nie określa okoliczności wydania decyzji unieważnienia zaświadczenia certyfikacyjnego przez ministra właściwego do spraw gospodarki.

5.4.2 Podmioty uprawnione do żądania publikacji informacji o unieważnieniu zaświadczeń certyfikacyjnych

Jedynie minister właściwy do spraw gospodarki może zażądać publikacji informacji o unieważnieniu zaświadczenia certyfikacyjnego na liście unieważnionych zaświadczeń certyfikacyjnych.

5.4.3 Procedura publikacji informacji o unieważnieniu zaświadczenia certyfikacyjnego

Po odebraniu polecenia publikacji informacji o unieważnieniu zaświadczenia certyfikacyjnego od ministra właściwego do spraw gospodarki osoba pełniąca funkcję w systemie unieważnia zaświadczenie certyfikacyjne. Następnie tworzona jest i publikowana w Repozytorium aktualna lista unieważnionych zaświadczeń certyfikacyjnych, przy czym:

1. listę unieważnionych zaświadczeń certyfikacyjnych wydanych przez urząd ***stary Root*** (**nccert.crl**), publikuje się pod adresem www.nccert.pl/arl/nccert.crl
2. listę unieważnionych zaświadczeń certyfikacyjnych wydanych przez urząd ***nowy Root*** (**nccert-n.crl**), publikuje się pod adresem www.nccert.pl/arl/nccert-n.crl

Informację o unieważnieniu zaświadczenia certyfikacyjnego umieszcza się na każdej liście unieważnionych zaświadczeń certyfikacyjnych publikowanej przed dniem upływu ważności zaświadczenia certyfikacyjnego oraz na pierwszej liście po upływie tego okresu.

Po opublikowaniu listy unieważnionych zaświadczeń certyfikacyjnych Narodowe Centrum Certyfikacji przekazuje ministrowi właściwemu do spraw gospodarki potwierdzenie dokonania publikacji informacji o unieważnieniu zaświadczenia certyfikacyjnego na liście unieważnionych zaświadczeń certyfikacyjnych.

Operacje związane z unieważnieniem zaświadczenia certyfikacyjnego oraz wytworzeniem i publikacją aktualnej listy unieważnionych zaświadczeń certyfikacyjnych zapisywane są w rejestrze zdarzeń.

Lista unieważnionych zaświadczeń certyfikacyjnych zapewnia określenie czasu unieważnienia zaświadczenia certyfikacyjnego z dokładnością do jednej sekundy. Czas ten jest zapisywany automatycznie przez oprogramowanie stosowane do unieważniania zaświadczeń certyfikacyjnych. Narodowe Centrum Certyfikacji zapewnia przyjmowanie i weryfikację pod względem formalnym poleceń ministra właściwego do spraw gospodarki publikacji informacji o unieważnieniu zaświadczenia certyfikacyjnego przez całą dobę.

5.4.4 Dopuszczalne okresy zwłoki publikacji informacji o unieważnieniu zaświadczenia certyfikacyjnego

Narodowe Centrum Certyfikacji publikuje aktualną listę unieważnionych zaświadczeń certyfikacyjnych w ciągu 1 godziny od momentu otrzymania polecenia publikacji informacji o unieważnieniu zaświadczenia certyfikacyjnego od ministra właściwego do spraw gospodarki.

Unieważnienie i publikacja listy unieważnionych zaświadczeń certyfikacyjnych zostają odnotowane w odpowiednich rejestrach zdarzeń.

5.4.5 Okoliczności zawieszania zaświadczeń certyfikacyjnych

Nie ma zastosowania.

5.4.6 Podmioty uprawnione do żądania zawieszenia zaświadczeń certyfikacyjnych

Nie ma zastosowania.

5.4.7 Procedura zawieszania i wycofywania unieważnień zaświadczeń certyfikacyjnych

Nie ma zastosowania.

5.4.8 Ograniczenia okresu zawieszenia zaświadczeń certyfikacyjnych

Nie ma zastosowania.

5.4.9 Częstotliwość publikacji list unieważnionych zaświadczeń certyfikacyjnych

Aktualne listy unieważnionych zaświadczeń certyfikacyjnych publikowane są w następujących sytuacjach:

1) niezwłocznie po dokonaniu unieważnienia, w terminie do 1 godziny od otrzymania od ministra właściwego do spraw gospodarki polecenia unieważnienia zaświadczenia certyfikacyjnego;

2) co najmniej raz dziennie (z wyłączeniem sobót, niedziel oraz wszystkich dni ustawowo wolnych od pracy)[9].

5.4.10 Obowiązek sprawdzania list unieważnionych zaświadczeń certyfikacyjnych

Przed akceptacją poświadczenia elektronicznego weryfikowanego z wykorzystaniem zaświadczenia certyfikacyjnego wydanego przez Narodowe Centrum Certyfikacji Strona ufająca powinna sprawdzić, czy zaświadczenie certyfikacyjne nie znajduje się na odpowiedniej liście unieważnionych zaświadczeń certyfikacyjnych, tzn. dla zaświadczeń certyfikacyjnych wydanych przez urząd ***stary Root***, na liście **nccert.crl** publikowanej pod adresem *www.nccert.pl/arl/nccert.crl*, dla zaświadczeń wydanych przez urząd ***nowy Root***, na liście **nccert-n.crl** publikowanej pod adresem *www.nccert.pl/arl/nccert-n.crl*.

Należy jednak zwrócić uwagę, że publikacja listy unieważnionych zaświadczeń certyfikacyjnych, podobnie jak listy unieważnionych i zawieszonych certyfikatów publikowanej przez Subskrybenta, następuje później niż unieważnienie zaświadczenia certyfikacyjnego. Narodowe Centrum Certyfikacji gwarantuje, że czas od unieważnienia do publikacji listy będzie zgodny z *ustawą o podpisie elektronicznym*, i nie przekroczy 1 godziny. Powyższe zależności należy uwzględnić w procedurach weryfikacji zaświadczeń certyfikacyjnych i certyfikatów, a tym samym podpisu elektronicznego i poświadczenia elektronicznego.

Weryfikacja taka musi być dokonana zgodnie z odpowiednią ścieżką certyfikacji[10].

5.4.11 Dostępność usługi weryfikacji statusu zaświadczenia certyfikacyjnego (OCSP) w trybie on-line

Narodowe Centrum Certyfikacji pełniąc rolę podmiotu upoważnionego nie udostępnia usługi weryfikacji statusu zaświadczenia certyfikacyjnego w trybie on-line.

5.4.12 Obowiązek korzystania z usługi weryfikacji statusu zaświadczenia certyfikacyjnego (OCSP) w trybie on-line

Nie ma zastosowania.

5.4.13 Inne dostępne formy ogłaszania unieważnień zaświadczenia certyfikacyjnego

Informacja o unieważnieniu zaświadczenia certyfikacyjnego jest również umieszczana w odpowiedniej karcie rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne.

[9] opracowane są procedury awaryjne w przypadku zaistnienia konieczności wykonania w/w działań w sobotę, niedzielę lub dzień ustawowo wolny od pracy.

[10] patrz pkt 2.1.1

5.4.14 Obowiązek sprawdzania innych form publikacji informacji o unieważnieniu zaświadczenia certyfikacyjnego

Zastosowanie się przez Stronę ufającą do punktu 5.4.10 jest jedyną obowiązkową formą sprawdzenia informacji o unieważnieniu zaświadczenia certyfikacyjnego.

5.4.15 Obowiązek powiadamiania w przypadku naruszenia bezpieczeństwa danych służących do składania poświadczenia elektronicznego

W przypadku naruszenia bezpieczeństwa lub podejrzenia naruszenia bezpieczeństwa danych służących do składania poświadczenia elektronicznego Subskrybent zobowiązany jest do niezwłocznego powiadomienia o zdarzeniu ministra właściwego do spraw gospodarki.

5.5 Procedury kontroli bezpieczeństwa prowadzenia działalności

W celu zapewnienia właściwego poziomu bezpieczeństwa swojej działalności Narodowe Centrum Certyfikacji opracowało i wdrożyło procedury kontroli bezpieczeństwa prowadzenia działalności, a w szczególności procedury:

1. Monitorowania stanu systemu;
2. Tworzenia rejestrów zdarzeń na potrzeby kontroli bezpieczeństwa prowadzenia działalności;
3. Okresowego przeglądu i analizy rejestrów zdarzeń;
4. Inspekcji wdrożonych mechanizmów i środków bezpieczeństwa;
5. Postępowania w przypadku naruszenia bezpieczeństwa.

Uprawnione osoby pełniące funkcje w Narodowym Centrum Certyfikacji dokonują okresowego przeglądu rejestrów zdarzeń. Przegląd rejestrów zdarzeń ma na celu wykrycie prób naruszenia bezpieczeństwa działalności systemu, a w szczególności:

1. Nieuprawnionych prób uzyskania dostępu do wykorzystywanych systemów;
2. Nieuprawnionych prób uzyskania dostępu do wykorzystywanych i przetwarzanych danych;
3. Nieuprawnionych prób uzyskania dostępu do pomieszczeń Narodowego Centrum Certyfikacji;
4. Prób zakłócenia działalności wykorzystywanych systemów;
5. Prób uniemożliwienia pełnienia roli podmiotu upoważnionego.

5.5.1 Rodzaje informacji zapisywanych w rejestrach zdarzeń

Rejestry zdarzeń tworzone są w czasie bieżącej pracy systemów teleinformatycznych Narodowego Centrum Certyfikacji. Rejestry zdarzeń zawierają zapisy dotyczące operacji wykonywanych w związku z pełnieniem funkcji podmiotu upoważnionego, w szczególności:

1. Żądania świadczenia usługi normalnie udostępnianej przez system lub usług nie wykonywanych przez system oraz informacja o zrealizowaniu lub niewykonaniu usługi (w przypadku niewykonania również jego powód);
2. Istotne zdarzenia związane ze zmianami w środowisku systemu, w tym w podsystemie zarządzania kluczami infrastruktury, zaświadczeniami certyfikacyjnymi oraz danymi służącymi do składania poświadczenia

elektronicznego przez Narodowe Centrum Certyfikacji, np. tworzenie kont użytkowników i rodzaj przydzielanych uprawnień;
3. Instalacje nowego oprogramowania lub aktualizacje;
4. Rozpoczęcie i przerwanie funkcji rejestrujących zdarzenia;
5. Zmiany w konfiguracji funkcji rejestrujących zdarzenia, w tym w szczególności każdą modyfikację czasu systemowego;
6. Data i czas tworzenia kopii zapasowych;
7. Data i czas archiwizowania rejestrów zdarzeń;
8. Zamykanie, otwieranie i restart systemu;
9. Czynności podjęte po wykryciu złego funkcjonowania funkcji rejestrujących zdarzenia;
10. Negatywne wyniki testów badania jakości generatorów losowych;
11. Wszystkie polecenia unieważnienia zaświadczenia certyfikacyjnego oraz wszystkie wiadomości z tym związane, a w szczególności wysłane i odebrane komunikaty przesyłane w relacjach ministra właściwego do spraw gospodarki z Narodowym Centrum Certyfikacji.

Każdy wpis do rejestru zdarzeń zawiera, co najmniej następujące informacje:
1. Datę i czas zdarzenia, z dokładnością do jednej sekundy;
2. Rodzaj zdarzenia;
3. Identyfikator lub inne dane pozwalające na określenie osoby odpowiedzialnej za zdarzenie;
4. Określenie czy zdarzenie dotyczy operacji zakończonej sukcesem czy błędem.

System teleinformatyczny stosowany przez Narodowe Centrum Certyfikacji umożliwia przeglądanie rejestrów zdarzeń, co najmniej w zakresie informacji, o których mowa w akapicie powyżej, i zapewnia uprawnionym osobom dokonującym przeglądu zawartości, czytelną formę zapisów umożliwiającą ich interpretację.

Zmiany zapisów dotyczących zarejestrowanych zdarzeń są zabronione.

System zawiera mechanizmy zapewniające zachowanie integralności rejestrów zdarzeń w stopniu uniemożliwiającym ich modyfikację po przeniesieniu do archiwum.

Rejestry zdarzeń dotyczące instalacji nowego oprogramowania lub jego aktualizacji, archiwizacji lub kopii zapasowych mogą być tworzone w formie innej niż elektroniczna.

Tworzy się kopie zapasowe rejestrów zdarzeń.

Kopie zapasowe tworzy się z wykorzystaniem technik zapewniających integralność danych.

Przy tworzeniu kopii zapasowych powinny być obecne, co najmniej dwie spośród osób, o których mowa w pkt 6.2.1 niniejszej Polityki Certyfikacji.

Czynności polegające na tworzeniu kopii zapasowych nadzoruje bezpośrednio Inspektor Bezpieczeństwa Systemu.

W celu rozpoznania ewentualnych nieuprawnionych działań Administrator Systemu i Inspektor do spraw Audytu analizują informacje zapisane w rejestrach zdarzeń przynajmniej raz w każdym dniu roboczym.

5.5.2 Częstotliwość analiz zapisów w rejestrach zdarzeń

Rejestry zdarzeń są przeglądane, co najmniej raz dziennie.

Zasady kontroli i analizy rejestrach zdarzeń określają procedury Narodowego Centrum Certyfikacji.

5.5.3 Okres przechowywania rejestrów zdarzeń

Rejestry zdarzeń będą przechowywane przez minimum 3 lata, od chwili zarejestrowania zdarzenia, w sposób umożliwiający elektroniczne przeszukiwanie rejestrów.

Po upływie okresu przechowywania rejestry zdarzeń, powinny być zniszczone w bezpieczny sposób lub przeniesione do archiwum zgodnie z aktualnie obowiązującymi przepisami prawa, normami i standardami.

5.5.4 Ochrona rejestrów zdarzeń

Rejestry zdarzeń przechowywane są w środowisku zapewniającym odpowiedni poziom bezpieczeństwa. Zapewnia się integralność plików w rejestrach zdarzeń.

5.5.5 Procedura tworzenia kopii zapasowych rejestrów zdarzeń

Kopie rejestrów zdarzeń są tworzone wraz z kopiami bezpieczeństwa systemu. Identyczne kopie rejestrów zdarzeń przechowywane są w dwóch różnych lokalizacjach.

Zasady tworzenia kopii zapasowych definiują procedury Narodowego Centrum Certyfikacji.

5.5.6 Tworzenie rejestrów zdarzeń

Rejestry zdarzeń w formie elektronicznej są tworzone automatycznie przez wykorzystywane oprogramowanie oraz systemy operacyjne. Dodatkowo, tworzone są dzienniki pracy systemu, obejmujące zdarzenia nie rejestrowane przez system teleinformatyczny, w których odpowiednie wpisy umieszczają uprawnione osoby, pełniące funkcje w Narodowym Centrum Certyfikacji.

Poniższa tabela przedstawia przykładowe informacje dotyczące sposobu zbierania informacji na potrzeby kontroli bezpieczeństwa:

	Typ zdarzenia	Sposób zbierania	Zapewniony przez
1.	Udane i nieudane próby zmiany parametrów systemu operacyjnego.	automatyczny	System operacyjny
2.	Otwarcie i zamknięcie systemów i aplikacji.	automatyczny / manualny	System operacyjny
3.	Udane i nieudane próby logowania i wylogowania.	automatyczny	System operacyjny
4.	Udane i nieudane próby tworzenia, modyfikacji lub usunięcia kont systemowych.	automatyczny	System operacyjny

	Typ zdarzenia	Sposób zbierania	Zapewniony przez
5.	Udane i nieudane próby tworzenia, modyfikacji lub usunięcia upoważnionego użytkownika systemu.	automatyczny / manualny	System operacyjny i personel
6.	Udane i nieudane operacje wytwarzania i unieważniania zaświadczeń certyfikacyjnych.	automatyczny	Oprogramowanie
7.	Udane i nieudane operacje związane z publikacją zaświadczeń certyfikacyjnych oraz informacji o unieważnieniach zaświadczeń certyfikacyjnych.	automatyczny / manualny	Oprogramowanie i personel
8.	Udane i nieudane operacje związane z publikacją innych informacji.	automatyczny / manualny	Oprogramowanie i personel
9.	Tworzenie, archiwizowanie kopii bezpieczeństwa.	automatyczny i manualny	System operacyjny i personel
10.	Zmiany konfiguracji systemu.	manualny	Personel operacyjny
11.	Uaktualnienia oprogramowania i zmiany w sprzęcie komputerowym.	manualny	Personel operacyjny
12.	Czynności związane z serwisem systemu.	manualny	Personel operacyjny
13.	Zmiany w personelu.	manualny	Personel operacyjny

5.5.7 Powiadamianie osób odpowiedzialnych w przypadku podejrzenia naruszenia lub naruszenia bezpieczeństwa systemu

Osoby pełniące funkcje w Narodowym Centrum Certyfikacji powiadamiają Inspektora Bezpieczeństwa Systemu o wszystkich wydarzeniach mających wpływ na bezpieczeństwo systemu oraz wszystkich wydarzeniach wskazujących na możliwe naruszenie bezpieczeństwa.

5.5.8 Oszacowanie podatności na zagrożenia

Dokonuje się okresowej oceny poziomu ryzyka systemu, w celu identyfikacji zagrożeń, oszacowania prawdopodobieństwa ich wystąpienia oraz podatności na nie systemu. Na podstawie wyników analizy ryzyka wprowadzone zostają rozwiązania mające na celu eliminację lub zmniejszenie podatności systemu na zagrożenia.

5.6 Archiwizacja

5.6.1 Rodzaje archiwizowanych danych

Narodowe Centrum Certyfikacji archiwizuje i przechowuje następujące informacje:

1. Zaświadczenia certyfikacyjne ministra właściwego do spraw gospodarki;
2. Wytworzone i wydane zaświadczenia certyfikacyjne;
3. Wytworzone listy unieważnionych zaświadczeń certyfikacyjnych;
4. Rejestr kwalifikowanych podmiotów świadczących usługi certyfikacyjne;
5. Przyjęte żądania certyfikacji;
6. Kopie bezpieczeństwa elementów systemu;
7. Kopie bezpieczeństwa baz danych;
8. Kopie korespondencji Narodowego Centrum Certyfikacji prowadzonej w związku z pełnieniem roli podmiotu upoważnionego;

9. Rejestry zdarzeń;
10. Inne informacje związane z pełnieniem roli podmiotu upoważnionego, publikowane przez Narodowe Centrum Certyfikacji.

5.6.2 Okres przechowywania archiwizowanych danych

Rejestry zdarzeń są przechowywane w sposób umożliwiający przeglądanie elektroniczne przez okres, co najmniej 3 lat. Po upływie tego okresu mogą zostać zniszczone w bezpieczny sposób bądź zarchiwizowane.

Narodowe Centrum Certyfikacji przechowuje wszystkie dokumenty oraz dane elektroniczne wymienione w pkt 5.6.1, bezpośrednio związane z pełnieniem roli podmiotu upoważnionego, przez okres 20 lat od chwili powstania danego dokumentu lub danych.

5.6.3 Zabezpieczenia archiwum

Narodowe Centrum Certyfikacji zapewnia, że wszystkie dokumenty oraz dane elektroniczne bezpośrednio związane z pełnieniem roli podmiotu upoważnionego są przechowywane w sposób zapewniający bezpieczeństwo przechowywanych dokumentów oraz danych, zgodnie z wymogami *Ustawy o podpisie elektronicznym* oraz odpowiednimi przepisami wykonawczymi, a w szczególności:

1. Zasoby archiwalne zabezpieczone są środkami ochrony fizycznej;
2. Dostęp do archiwum jest ograniczony jedynie do upoważnionych osób pełniących funkcje w Narodowym Centrum Certyfikacji;
3. Pomieszczenia archiwum są monitorowane.

5.6.4 Procedury tworzenia kopii zapasowych

Zgodnie z wymogami *Ustawy o podpisie elektronicznym* oraz odpowiednich przepisów wykonawczych, tworzone są kopie zapasowe umożliwiające pełne odtworzenie funkcjonalności systemu teleinformatycznego Narodowego Centrum Certyfikacji.

5.6.5 Wymagania znakowania czasem archiwizowanych danych

Znakowanie czasem zasobów archiwalnych nie jest wymagane.

5.6.6 System archiwizacji

Narodowe Centrum Certyfikacji posiada wdrożone procedury zbierania i zarządzania zasobami archiwalnymi, a w szczególności:

1. Klasyfikacji zasobów;
2. Automatycznego zbierania danych w postaci elektronicznej;
3. Przetwarzania do postaci elektronicznej dokumentów tradycyjnych;
4. Zapewnienia bezpieczeństwa zasobów archiwalnych.

Zasady zbierania i zarządzania zasobami archiwalnymi określają procedury Narodowego Centrum Certyfikacji.

5.6.7 Procedury dostępu i weryfikacji danych

Informacje są udostępniane jedynie uprawnionym podmiotom.

Informacje mogą być dodawane i usuwane do/z archiwum jedynie przez upoważnione osoby pełniące funkcje w Narodowym Centrum Certyfikacji.

W regularnych odstępach czasu sprawdzana jest możliwość odtwarzania informacji z archiwizowanych kopii bezpieczeństwa.

W razie stwierdzenia problemów z odtwarzaniem danych archiwalnych zasobów są one odtwarzane na podstawie informacji istniejącej w systemie bądź kopii zasobów archiwalnych.

Szczegółowe procedury zdefiniowano w odpowiednich dokumentach Narodowego Centrum Certyfikacji.

5.7 Procedura wymiany danych służących do składania poświadczenia elektronicznego

5.7.1 Procedura wymiany danych służących do składania poświadczenia elektronicznego przez Narodowe Centrum Certyfikacji

Okresy ważności zaświadczeń certyfikacyjnych, w tym zaświadczenia certyfikacyjnego ministra właściwego do spraw gospodarki, określają akty wykonawcze do *Ustawy o podpisie elektronicznym,* na okresy nie dłuższe niż:

1. 11 lat dla zaświadczenia certyfikacyjnego ministra właściwego do spraw gospodarki;
2. 5 lat dla zaświadczenia certyfikacyjnego Subskrybenta.

Dane służące do składania poświadczenia elektronicznego i dane służące do weryfikacji poświadczenia elektronicznego są ważne tak długo, jak ważne jest zaświadczenie certyfikacyjne.

Czas początku ważności zaświadczenia certyfikacyjnego nie może być wcześniejszy niż moment jego wytworzenia.

Wymiana danych służących do składania poświadczenia elektronicznego przez Narodowe Centrum Certyfikacji wymaga wytworzenia nowego zaświadczenia certyfikacyjnego ministra właściwego do spraw gospodarki.

Procedura wytworzenia nowego zaświadczenia certyfikacyjnego ministra właściwego do spraw gospodarki rozpoczyna się przed upływem ważności poprzednich danych.

Dane służące do składania poświadczenia elektronicznego przejęte od CENTRAST S.A. w 2005 roku zostały wygenerowane 17 grudnia 2002 r. z okresem ważności do dnia **14 grudnia 2013 r.**

W związku z koncepcją wymiany zaświadczenia certyfikacyjnego ministra właściwego do spraw gospodarki uzgodnioną z Ministrem Gospodarki[11], w której przyjęto nową postać identyfikatora wyróżniającego zaświadczenia certyfikacyjnego ministra właściwego do spraw gospodarki, tzn.:

[11] Została omówiona szczegółowo w pkt 2.1.1

Kraj	**PL**
Organizacja	**Minister wlasciwy do spraw gospodarki**
Nazwa powszechna	**Narodowe Centrum Certyfikacji (NCCert)**

po wejściu w życie niniejszej wersji Polityki Certyfikacji w Narodowym Centrum Certyfikacji został utworzony drugi urząd – ***nowy Root***, w którym zostało wygenerowane nowe zaświadczenie certyfikacyjne ministra właściwego do spraw gospodarki.

Urząd ***stary Root*** oraz urząd ***nowy Root*** będą funkcjonować równolegle do czasu wygaśnięcia zaświadczenia certyfikacyjnego Ministra Gospodarki wskazującego na CZiC Centrast SA, tzn. do dnia 14 grudnia 2013 r.

Od dnia 15 grudnia 2013 r. funkcjonować będzie jedynie urząd ***nowy Root***.

Procedura wytworzenia nowego zaświadczenia certyfikacyjnego ministra właściwego do spraw gospodarki w urzędzie ***nowy Root***, przebiega następująco:

1. Wytworzenie nowych danych służących do składania/weryfikacji poświadczenia elektronicznego przyporządkowanych ministrowi właściwemu do spraw gospodarki;
2. Wytworzenie i publikacja zaświadczenia certyfikacyjnego ministra właściwego do spraw gospodarki.

Od momentu rozpoczęcia okresu ważności nowo wytworzonego zaświadczenia certyfikacyjnego ministra właściwego do spraw gospodarki poprzednio używane dane służące do składania poświadczenia elektronicznego nie są wykorzystywane do poświadczania elektronicznego zaświadczeń certyfikacyjnych, z wyjątkiem zaświadczenia certyfikacyjnego ministra właściwego do spraw gospodarki.

Proces wymiany danych służących do weryfikacji poświadczenia elektronicznego rozpoczyna się po upływie połowy okresu ważności zaświadczenia certyfikacyjnego ministra właściwego do spraw gospodarki.

Proces wymiany kluczy infrastruktury wykorzystywanych przez Narodowe Centrum Certyfikacji rozpoczyna się po upływie połowy okresu ważności tych kluczy.

5.7.2 Procedura wymiany danych służących do składania poświadczenia elektronicznego przez Subskrybenta

5.7.2.1 Procedura wymiany danych służących do składania poświadczenia elektronicznego przez Subskrybenta wydanych w urzędzie *stary Root*

Zgodnie z koncepcją przedstawioną w pkt 2.1.1, po uruchomieniu urzędu ***nowy Root***, w urzędzie ***stary Root*** nie przewiduje się wytwarzania i wydawania zaświadczeń certyfikacyjnych dla Subskrybentów. W związku z powyższym, zaświadczenia certyfikacyjne wydane przez urząd ***stary Root*** będą funkcjonowały do momentu ich wygaśnięcia, bez wymiany.

5.7.2.2 Procedura wymiany danych służących do składania poświadczenia elektronicznego przez Subskrybenta w urzędzie *nowy Root*

Wymiana danych służących do składania poświadczenia elektronicznego przez Subskrybenta wydanych w urzędzie ***nowy Root***, wiąże się z uzyskaniem nowego zaświadczenia certyfikacyjnego dla nowych danych służących do weryfikacji poświadczenia elektronicznego. Subskrybent kieruje odpowiedni wniosek do ministra właściwego do spraw gospodarki, który poleca Narodowemu Centrum Certyfikacji wydać zaświadczenie certyfikacyjne dla nowych danych służących do składania poświadczenia elektronicznego przez Subskrybenta. Stosuje się wymagania punktu 5.3. Dodatkowo, zgodnie z § 10 Rozporządzenia Ministra Gospodarki z dnia 9 sierpnia 2002 r. w sprawie określenia szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem elektronicznym (Dz. U. Nr 128, poz. 1101), Subskrybent dokonuje wzajemnej certyfikacji nowego i poprzedniego zaświadczenia certyfikacyjnego.

5.8 Naruszenie bezpieczeństwa oraz uruchamianie po klęskach żywiołowych i katastrofach

Narodowe Centrum Certyfikacji posiada opracowany i przetestowany plan awaryjny (zwany dalej „Planem"), który:

1. Obejmuje informacje dotyczące ustawień oraz sposobu konfiguracji sprzętu oraz oprogramowania;
2. Określa szczegółowe procedury odtwarzania oraz przewidywany czas ich wykonywania;
3. Określa warunki oraz okoliczności uruchomienia Planu;
4. Wskazuje osoby odpowiedzialne za uruchomienie procedur mających ograniczyć skutki zdarzenia lub klęski żywiołowej, przywrócić wymagany poziom bezpieczeństwa systemu oraz właściwy poziom świadczonych usług;
5. Identyfikuje osoby odpowiedzialne za opracowanie i utrzymanie Planu, w tym odpowiedzialne za regularne przeprowadzanie testów opisanych procedur;
6. Określa priorytety podejmowania poszczególnych działań;
7. Określa środki oraz procedury konieczne do odtworzenia systemu.

Narodowe Centrum Certyfikacji posiada ośrodek zapasowy zapewniający możliwość pełnienia roli podmiotu upoważnionego w przypadku zakłócenia działalności ośrodka podstawowego. Plan określa okoliczności i procedury uruchamiania systemu w ośrodku zapasowym.

5.8.1 Uszkodzenie sprzętu, oprogramowania i/lub danych

Plan obejmuje postępowanie w przypadku awarii sprzętu technicznego, oprogramowania oraz uszkodzenia przetwarzanych i przechowywanych danych.

Plan zawiera opis bazowej konfiguracji systemu oraz procedury instalacji i konfiguracji oraz procedury odtwarzania elementów systemu z kopii zapasowych.

Plan określa okoliczności, w jakich następuje uruchomienie systemu w ośrodku zapasowym.

5.8.2 Unieważnienie zaświadczenia certyfikacyjnego ministra właściwego do spraw gospodarki

Narodowe Centrum Certyfikacji przyjęło procedurę postępowania w przypadku unieważnienia zaświadczenia certyfikacyjnego ministra właściwego do spraw gospodarki przez ministra właściwego do spraw gospodarki.

5.8.3 Naruszenie bezpieczeństwa danych służących do składania poświadczenia elektronicznego

Narodowe Centrum Certyfikacji przyjęło plan postępowania w przypadku naruszenia bezpieczeństwa danych służących do poświadczenia elektronicznego, wykorzystywanych przez Narodowe Centrum Certyfikacji jako podmiotu upoważnionego.

Plan określa sposób powiadamiania ministra właściwego do spraw gospodarki oraz Subskrybenta.

5.8.4 Zabezpieczanie po klęskach żywiołowych i katastrofach

Plan, o którym mowa w rozdziale 5.8, obejmuje działania konieczne do przywrócenia odpowiedniego poziomu bezpieczeństwa oraz właściwego poziomu świadczenia usług, w przypadku wystąpienia klęski żywiołowej, ataku terrorystycznego, aktu sabotażu lub wystąpienia innych zagrożeń mogących naruszyć ciągłość działania Narodowego Centrum Certyfikacji.

5.9 Zakończenie działalności podmiotu świadczącego usługi certyfikacyjne

5.9.1 Zakończenie świadczenia usług certyfikacyjnych przez Subskrybenta

W przypadku zakończenia działalności przez Subskrybenta, minister właściwy do spraw gospodarki wskazuje podmiot przejmujący zasoby archiwalne podmiotu zaprzestającego działalności.

5.9.2 Zakończenie działalności Narodowego Centrum Certyfikacji

W przypadku:

1. zamiaru zaprzestania pełnienia roli podmiotu upoważnionego,
2. niemożności pełnienia roli podmiotu upoważnionego albo
3. poinformowania Narodowego Centrum Certyfikacji przez ministra właściwego do spraw gospodarki o zamiarze cofnięcia upoważnienia, o którym mowa w art. 23 ust. 5 *Ustawy o podpisie elektronicznym*.

Narodowe Centrum Certyfikacji zobowiązuje się do zapewnienia ciągłości pełnienia roli podmiotu upoważnionego, do czasu wyłonienia przez ministra właściwego do spraw gospodarki nowego podmiotu, który przejąłby jego obowiązki, jednak nie dłużej niż przez okres:

a) 6 miesięcy od dnia poinformowania ministra właściwego do spraw gospodarki o okolicznościach, o których mowa w pkt 1 i 2,
b) 4 miesięcy od dnia poinformowania Narodowego Centrum Certyfikacji o okoliczności, o której mowa w pkt 3.

W przypadku cofnięcia przez ministra właściwego do spraw gospodarki upoważnienia, o którym mowa w art. 23 ust. 5 *Ustawy o podpisie elektronicznym*, Narodowe Centrum Certyfikacji zaprzestaje pełnienia roli podmiotu upoważnionego, ze skutkiem natychmiastowym.

Narodowe Centrum Certyfikacji pełniąc rolę podmiotu upoważnionego, w przypadku zaprzestania działalności zobowiązuje się do:

1. umożliwienia przejęcia i kontynuacji pełnienia tej roli przez inny podmiot, w tym ministra właściwego do spraw gospodarki,
2. przekazania podmiotowi przejmującemu pełnienie tej roli – na żądanie ministra właściwego do spraw gospodarki – wszelkich informacji i danych, które umożliwią wykonywanie tej roli przez nowy podmiot.

Narodowe Centrum Certyfikacji nie udostępnia danych i informacji, o których mowa w pkt. 3.8.1 pkt 1-3, z wyłączeniem sytuacji, gdy podmiot wskazany przez ministra właściwego do spraw gospodarki, przejmuje i kontynuuje rolę podmiotu upoważnionego.

6 Zabezpieczenia fizyczne, organizacyjne oraz osobowe

6.1 Zabezpieczenia fizyczne

6.1.1 Lokalizacja i konstrukcja budynku

Systemy teleinformatyczne Narodowego Centrum Certyfikacji są zlokalizowane w obiektach Narodowego Banku Polskiego, zabezpieczonych systemami ochrony fizycznej, spełniających wymagania określone w § 42 Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. Nr 128, poz. 1094).

6.1.2 Dostęp fizyczny

Zapewnia się kontrolę dostępu do pomieszczeń, w których zlokalizowany jest system teleinformatyczny Narodowego Centrum Certyfikacji.

Dostęp do elementów systemu Narodowego Centrum Certyfikacji mają wyłącznie uprawnione osoby pełniące funkcje w Narodowym Centrum Certyfikacji.

Dopuszcza się pracę w systemie osób niebędących pracownikami Narodowego Banku Polskiego, w związku z realizacją zadań określonych w umowach, zawartych przez Narodowy Bank Polski. Umowy te zawierają zapisy zapewniające: właściwy poziom bezpieczeństwa wykonywanych prac serwisowych i konserwacyjnych, które są wykonywane wyłącznie pod nadzorem pracowników Narodowego Centrum Certyfikacji a także, w odniesieniu do komponentu on-line[12], właściwy poziom bezpieczeństwa obsługi tego komponentu oraz integralność i dostępność publikowanych danych.

6.1.3 Zasilanie oraz klimatyzacja

W celu przeciwdziałania przerwaniu działalności na skutek przerw w dopływie energii elektrycznej Narodowe Centrum Certyfikacji posiada system zasilania awaryjnego.

Odpowiednia temperatura oraz wilgotność powietrza w pomieszczeniach ośrodka podstawowego oraz zapasowego zapewnione są przez systemy klimatyzacji.

6.1.4 Zagrożenie zalaniem

Krytyczne elementy systemu wykorzystywanego przez Narodowe Centrum Certyfikacji, są rozmieszczone w pomieszczeniach o małym ryzyku zalania, w tym w wyniku uszkodzenia instalacji budynku.

[12] Element systemu NCCert, służący do publikacji informacji dotyczących NCCert, w tym list unieważnionych zaświadczeń certyfikacyjnych

W przypadku wystąpienia zagrożenia zalaniem, postępuje się zgodnie z procedurami obowiązującymi w Narodowym Banku Polskim oraz uruchamia się procedury zapewnienia ciągłości działania Narodowego Centrum Certyfikacji, zdefiniowane w Planie.

6.1.5 Ochrona przeciwpożarowa

Pomieszczenia Narodowego Centrum Certyfikacji są chronione przez automatyczną instalację przeciwpożarową.

W przypadku wystąpienia zagrożenia pożarowego postępuje się zgodnie z procedurami obowiązującymi w Narodowym Banku Polskim oraz uruchamia się procedury zapewnienia ciągłości działania Narodowego Centrum Certyfikacji, zdefiniowane w Planie.

6.1.6 Nośniki informacji

Szczególnej kontroli, w tym ograniczeniu ruchu pomiędzy strefami bezpieczeństwa, w centrach komputerowych podlegają wszelkie urządzenia umożliwiające utrwalenie lub przesłanie informacji.

Dostęp do nośników informacji jest ograniczony, a nośniki przechowywane są w nadzorowanych pomieszczeniach.

Dane wprowadzane do systemu z zewnętrznych elektronicznych nośników informacji są, przed ich wprowadzaniem do systemu, badane na obecność wirusów komputerowych lub innego złośliwego oprogramowania.

6.1.7 Niszczenie informacji

Zbędne dokumenty papierowe, dokumenty w formie elektronicznej oraz inne nośniki informacji używane przez Narodowe Centrum Certyfikacji są niszczone w bezpieczny sposób, zgodnie z obowiązującymi przepisami prawa, normami i standardami.

6.1.8 Archiwa oddalone

Kopie bezpieczeństwa oraz kopie zasobów archiwalnych są przechowywane w różnych lokalizacjach.

Ośrodek zapasowy, zapewniający możliwość pełnego odtworzenia funkcjonalności systemu z ośrodka podstawowego oraz przechowywanie kopii zasobów archiwalnych, jest dostępny dla upoważnionych osób pełniących funkcje w Narodowym Centrum Certyfikacji 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.

6.2 Zabezpieczenia organizacyjne

6.2.1 Role

Zgodnie z wymogami *Ustawy o podpisie elektronicznym* oraz odpowiednimi przepisami wykonawczymi, w systemie Narodowego Centrum Certyfikacji funkcjonują następujące role:

1. **Inspektor Bezpieczeństwa Systemu**, który nadzoruje wdrożenie i stosowanie wszystkich procedur bezpiecznej eksploatacji systemów teleinformatycznych wykorzystywanych do pełnienia roli podmiotu upoważnionego;
2. **Inspektor ds. Rejestracji** zatwierdzający żądania certyfikacji lub tworzenie listy unieważnionych zaświadczeń certyfikacyjnych;
3. **Administrator Systemu**, który instaluje, konfiguruje i zarządza systemem teleinformatycznym, w tym wykonuje kopie zapasowe;
4. **Operator Systemu** wykonujący codzienną obsługę systemu;
5. **Inspektor ds. Audytu** analizujący zapisy rejestrów zdarzeń mających miejsce w systemach teleinformatycznych, wykorzystywanych do pełnienia roli podmiotu upoważnionego.

6.2.2 Liczba osób wymaganych do realizacji zadania

Zgodnie z wymogami *Ustawy o podpisie elektronicznym* oraz odpowiednimi przepisami wykonawczymi, w systemie Narodowego Centrum Certyfikacji przyjęto, że jednej osobie może zostać powierzone wykonywanie więcej niż jednej roli, z tym że:

1. Rola Inspektora ds. Audytu nie może być łączona z żadną inną funkcją;
2. Rola Inspektora Bezpieczeństwa Systemu nie może być łączona z rolą Inspektora ds. Audytu, Operatora Systemu ani Administratora Systemu.

Zakres uprawnień oraz liczba osób wymaganych do realizacji zadań jest określona w procedurach Narodowego Centrum Certyfikacji.

6.2.3 Identyfikacja oraz uwierzytelnienie osób funkcyjnych

Identyfikacja oraz uwierzytelnienie osób funkcyjnych jest dokonywane dzięki systemowi zabezpieczeń fizycznych i organizacyjnych obejmujących w szczególności:

1. Kontrolę i ograniczenie dostępu do poszczególnych pomieszczeń Narodowego Centrum Certyfikacji;
2. Przydział kont w systemie i określony zakres uprawnień uzasadniony zakresem wykonywanych obowiązków;
3. Zastosowanie kart elektronicznych do uaktywniania elementów systemu.

6.3 Bezpieczeństwo osobowe

6.3.1 Wykształcenie, kwalifikacje, doświadczenie

Narodowe Centrum Certyfikacji gwarantuje, że pracownicy którym powierzono obowiązki związane z pełnieniem przez Narodowe Centrum Certyfikacji roli podmiotu upoważnionego:

1. Mają pełną zdolność do czynności prawnych;
2. Nie są skazani prawomocnym wyrokiem za przestępstwo przeciwko wiarygodności dokumentów, obrotowi gospodarczemu, obrotowi pieniędzmi i papierami wartościowymi, przestępstwo skarbowe lub przestępstwa, o których mowa w rozdziale VIII *Ustawy o podpisie elektronicznym;*
3. Posiadają niezbędną wiedzę i umiejętności w zakresie technologii tworzenia zaświadczeń certyfikacyjnych, certyfikatów i świadczenia innych usług związanych z podpisem elektronicznym, sprzętu i oprogramowania stosowanego do elektronicznego przetwarzania danych, automatycznego przetwarzania danych w sieciach i systemach teleinformatycznych.

6.3.2 Dobór osób pełniących funkcje w Narodowym Centrum Certyfikacji

Osoby pełniące funkcje w Narodowym Centrum Certyfikacji są dobierane zgodnie z kwalifikacjami oraz na zasadach zatrudniania, obowiązujących w Narodowym Banku Polskim.

6.3.3 Szkolenia

Osoby pełniące funkcje w Narodowym Centrum Certyfikacji są przeszkolone, w szczególności w zakresie:

1. technologii tworzenia zaświadczeń certyfikacyjnych, certyfikatów i świadczenia innych usług związanych z podpisem elektronicznym,
2. obsługi sprzętu i oprogramowania stosowanego do elektronicznego przetwarzania danych, automatycznego przetwarzania danych w sieciach i systemach teleinformatycznych,
3. przestrzegania zasad bezpieczeństwa systemów teleinformatycznych;
4. przestrzegania procedur awaryjnych;
5. przestrzegania procedur stosowanych w czasie wykonywania czynności służbowych;

Osoby pełniące funkcje w Narodowym Centrum Certyfikacji posiadają dostęp do dokumentacji w zakresie uzasadnionym zajmowanym stanowiskiem oraz powierzonymi obowiązkami, w tym do niezbędnych procedur, polityk i regulaminów.

6.3.4 Wymagania dotyczące zakresu i częstotliwości szkoleń

Szkolenia obejmują zakres wiedzy wymagany na danym stanowisku pracy.

Osoby pełniące funkcje w Narodowym Centrum Certyfikacji przechodzą szkolenia udoskonalające, zgodnie z zasadami szkoleń obowiązującymi w Narodowym Banku Polskim.

W przypadku zmiany w funkcjonowaniu Narodowego Centrum Certyfikacji pracownicy przechodzą dodatkowe szkolenia.

6.3.5 Rotacja osób pełniących funkcje w Narodowym Centrum Certyfikacji

Polityka Certyfikacji nie nakłada obowiązku stosowania rotacji osób pełniących funkcje w Narodowym Centrum Certyfikacji.

6.3.6 Sankcje z tytułu nieuprawnionych działań

Wszystkie czynności wykonywane w ramach pełnienia obowiązków związanych z pełnieniem przez Narodowe Centrum Certyfikacji roli podmiotu upoważnionego, są dokumentowane i nadzorowane.

Analiza zapisów umożliwia w szczególności wykrycie ewentualnych nieuprawnionych działań osób pełniących funkcje w Narodowym Centrum Certyfikacji i idącego za tym naruszenia poziomu bezpieczeństwa.

Naruszanie zasad bezpieczeństwa, obowiązujących regulaminów i polityk jest karane. W zależności od skutków incydentu osoby odpowiedzialne za wystąpienie incydentu poniosą kary dyscyplinarne lub pociągnięte zostaną do odpowiedzialności zgodnie z przepisami prawa, w tym w szczególności *Ustawy o podpisie elektronicznym*.

6.3.7 Dokumentacja przekazywana osobom pełniącym funkcje w Narodowym Centrum Certyfikacji

Osoby pełniące funkcje w Narodowym Centrum Certyfikacji otrzymują opis obowiązków dotyczący zajmowanego stanowiska pracy, na zasadach obowiązujących w Narodowym Banku Polskim.

7 Procedury bezpieczeństwa technicznego

7.1 Wytwarzanie i instalacja danych służących do składania poświadczenia elektronicznego

7.1.1 Wytwarzanie danych służących do składania poświadczenia elektronicznego

W systemie teleinformatycznym wykorzystywanym przez Narodowe Centrum Certyfikacji, do tworzenia danych służących do składania poświadczenia elektronicznego stosuje się mechanizmy zabezpieczające przed nieupoważnionym dostępem.

Narodowe Centrum Certyfikacji nie wytwarza danych służących do składania podpisu bądź poświadczenia elektronicznego na potrzeby innych podmiotów.

7.1.2 Przekazywanie wytworzonych danych służących do składania poświadczenia elektronicznego

Nie dotyczy, ponieważ Narodowe Centrum Certyfikacji wytwarza dane służące do składania poświadczenia elektronicznego oraz dane służące do weryfikacji poświadczenia elektronicznego wyłącznie na potrzeby własnej działalności.

7.1.3 Przekazywanie Narodowemu Centrum Certyfikacji danych służących do weryfikacji poświadczenia elektronicznego Subskrybenta

Subskrybent przekazuje Narodowemu Centrum Certyfikacji dane służące do weryfikacji poświadczenia elektronicznego za pośrednictwem ministra właściwego do spraw gospodarki, załączając je do wniosku o wpis do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne oraz do żądania certyfikacji.

7.1.4 Przekazywanie danych służących do weryfikacji poświadczenia dokonywanego przez Narodowe Centrum Certyfikacji

Dane służące do weryfikacji poświadczenia elektronicznego Narodowego Centrum Certyfikacji wydawane są Subskrybentowi w formie zaświadczenia certyfikacyjnego ministra właściwego do spraw gospodarki. Zaświadczenie to jest publikowane w Repozytorium.

7.1.5 Wymagania dla danych służących do składania poświadczenia elektronicznego

Dla Narodowego Centrum Certyfikacji, zgodnie z wymogami *Ustawy o podpisie elektronicznym*, określono następujący algorytm i długość danych służących do składania poświadczenia elektronicznego:

1. Algorytm – asymetryczny algorytm RSA wraz z funkcją skrótu SHA-1 (OID: { iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 });
2. Długość – 2048 bitów.

Parametry algorytmu RSA spełniają wymagania dla algorytmów szyfrowych określone w załączniku nr 3 do Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. Nr 128, poz. 1094).

7.1.6 Wytwarzanie parametrów danych służących do weryfikacji poświadczenia elektronicznego

Parametry służące do wytworzenia danych służących do składania poświadczenia elektronicznego wykorzystywanych przez Narodowe Centrum Certyfikacji oraz danych służących do weryfikacji poświadczenia elektronicznego wykonanego przez Narodowe Centrum Certyfikacji są tworzone w komponencie technicznym, pozostającym pod wyłączną kontrolą Narodowego Centrum Certyfikacji.

Komponenty techniczne wykorzystywane do świadczenia usług certyfikacyjnych w ramach niniejszej Polityki Certyfikacji, nie są stosowane do żadnego innego celu.

Narodowe Centrum Certyfikacji wytwarza dane służące do składania poświadczenia elektronicznego oraz związane z nimi dane służące do weryfikacji poświadczenia elektronicznego wyłącznie na potrzeby własnej działalności.

Dane służące do składania poświadczenia elektronicznego wykorzystywane przez Subskrybenta oraz związane z nimi dane służące do weryfikacji poświadczenia elektronicznego są wytwarzane przez Subskrybenta.

7.1.7 Sprawdzenie jakości danych służących do weryfikacji poświadczenia elektronicznego

Komponenty techniczne wykorzystywane przez Narodowe Centrum Certyfikacji, zapewniają odpowiednią jakość danych służących do weryfikacji poświadczenia elektronicznego dokonywanych przez Narodowe Centrum Certyfikacji, w szczególności są zgodne z § 15 Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. Nr 128, poz. 1094) oraz spełniają wymagania dla algorytmów szyfrowych, określone w załączniku nr 3 do w/w Rozporządzenia.

Za jakość danych służących do weryfikacji poświadczenia elektronicznego dokonywanych przez Subskrybenta odpowiedzialny jest Subskrybent.

Narodowe Centrum Certyfikacji weryfikuje jedynie długość oraz algorytm danych, służących do weryfikacji poświadczenia elektronicznego. Algorytm i minimalna długość danych służących do weryfikacji poświadczenia elektronicznego muszą być zgodne z wymaganiami Załącznika nr 1 do Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne,

polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. Nr 128, poz. 1094).

7.1.8 Sprzętowe lub programowe tworzenie danych służących do składania i weryfikacji poświadczenia elektronicznego

Dane służące do składania poświadczenia elektronicznego wykorzystywane przez Narodowe Centrum Certyfikacji oraz dane służące do weryfikacji poświadczenia elektronicznego wykorzystywane do weryfikacji poświadczenia elektronicznego złożonego przez Narodowe Centrum Certyfikacji, tworzone są w komponencie technicznym pozostającym pod wyłączną kontrolą Narodowego Centrum Certyfikacji.

Dane służące do składania i weryfikacji poświadczenia elektronicznego Subskrybenta muszą być wytwarzane w komponentach technicznych spełniających wymagania Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. Nr 128, poz. 1094), w tym przepisów § 4, 5, 7 i 18.

7.1.9 Zastosowanie danych służących do składania poświadczenia elektronicznego

Zakres zastosowania danych służących do składania poświadczenia elektronicznego przez Narodowe Centrum Certyfikacji określony jest przez dwa atrybuty zaświadczenia certyfikacyjnego ministra właściwego do spraw gospodarki: *keyUsage* oraz *basicConstraints*[13].

Dopuszcza się wykorzystanie tych danych jedynie do:

1. Poświadczania elektronicznego wydawanych zaświadczeń certyfikacyjnych;
2. Poświadczania elektronicznego list unieważnionych zaświadczeń certyfikacyjnych.

Zakres zastosowania danych służących do składania poświadczenia elektronicznego przez Subskrybenta określony jest przez trzy atrybuty zaświadczenia certyfikacyjnego: *keyUsage, extKeyUsage* oraz *basicConstraints*[14].

Dopuszcza się wykorzystanie tych danych jedynie do:

1. Poświadczania elektronicznego wydawanych certyfikatów;
2. Poświadczania elektronicznego list unieważnionych i zawieszonych certyfikatów;
3. Poświadczania elektronicznego list unieważnionych zaświadczeń certyfikacyjnych;

[13] Rozszerzenie *basicConstraints* służy do ograniczania długości ścieżki certyfikacji, co tylko pośrednio wpływa na zakres zastosowania klucza.
[14] Jak w przypisie 5.

4. Poświadczania elektronicznego zaświadczeń certyfikacyjnych, o których mowa w § 1 pkt 3 i 4 Rozporządzenia Ministra Gospodarki z dnia 9 sierpnia 2002 r. w sprawie określenia szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem elektronicznym (Dz. U. Nr 128, poz. 1101);
5. Poświadczania elektronicznego kluczy infrastruktury;
6. Poświadczania elektronicznego tokenów znacznika czasu, w przypadku świadczenia usługi certyfikacyjnej polegającej na znakowaniu czasem;
7. Poświadczeń elektronicznych dokonywanych w związku ze świadczeniem innych usług certyfikacyjnych przez Subskrybenta.

Wykorzystanie danych służących do składania poświadczenia elektronicznego musi być zgodne z polityką wyspecyfikowaną w odpowiedniej karcie rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne.

7.2 Ochrona danych służących do składania poświadczenia elektronicznego przez Narodowe Centrum Certyfikacji

Dane służące do składania poświadczenia elektronicznego, stosowane przez Narodowe Centrum Certyfikacji są wytwarzane, przechowywane i używane wyłącznie w bezpiecznym środowisku informatycznym z zastosowaniem komponentów technicznych.

7.2.1 Certyfikaty zgodności komponentów technicznych

Komponenty techniczne służące do tworzenia i przechowywania danych służących do składania poświadczenia elektronicznego spełniają wymagania przewidziane przez *Ustawę o podpisie elektronicznym* oraz odpowiednie akty wykonawcze.

7.2.2 Ochrona danych służących do składania poświadczenia elektronicznego z wykorzystaniem schematu progowego

Dane służące do składania poświadczenia elektronicznego w przypadku eksportu poza komponent techniczny przenoszone są przy wykorzystaniu schematu progowego stopnia (m, n), gdzie wartość „m” wynosi co najmniej 2, natomiast $n > m + 1$.

7.2.3 Deponowanie części danych służących do odtwarzania danych służących do składania poświadczenia elektronicznego

Dane służące do składania poświadczenia elektronicznego nie są składowane ani deponowane (z wyjątkiem części danych służących do składania poświadczenia elektronicznego, przechowywanych w modułach kluczowych, umożliwiających odtworzenie danych służących do składania poświadczenia elektronicznego).

7.2.4 Dane służące do odtwarzania danych służących do składania poświadczenia elektronicznego

Części danych służących do składania poświadczenia elektronicznego, przechowywane w modułach kluczowych, umożliwiających odtworzenie danych

służących do składania poświadczenia elektronicznego przy wykorzystaniu schematu progowego, są przechowywane w ośrodku podstawowym i zapasowym.

Procedury Narodowego Centrum Certyfikacji określają zasady bezpiecznego przeniesienia danych służących do odtworzenia danych służących do składania poświadczenia elektronicznego do ośrodka zapasowego.

7.2.5 Archiwizacja danych służących do weryfikacji poświadczenia elektronicznego

Wszystkie dane służące do weryfikacji poświadczenia elektronicznego Narodowego Centrum Certyfikacji oraz publiczne klucze infrastruktury wykorzystywane przez Narodowe Centrum Certyfikacji są archiwizowane po upływie okresu ich ważności.

Zasady archiwizacji określają procedury Narodowego Centrum Certyfikacji.

7.2.6 Wprowadzanie danych służących do składania poświadczenia elektronicznego do komponentu technicznego

Dane służące do składania poświadczenia elektronicznego są tworzone w ośrodku podstawowym. Następnie zapisuje się je w modułach kluczowych w postaci danych służących do odtworzenia danych służących do składania poświadczenia elektronicznego. Dane służące do odtworzenia danych do składania poświadczenia elektronicznego są przechowywane w wymienionych modułach kluczowych w ośrodku podstawowym.

W przypadku zaistnienia takiej potrzeby, dane służące do składania poświadczenia elektronicznego są instalowane w komponencie technicznym ośrodka zapasowego przy zastosowaniu odpowiednich środków zapewnienia bezpieczeństwa zgodnych z wymogami *Ustawy o podpisie elektronicznym*.

Do komponentu technicznego wprowadza się dane służące do składania poświadczenia elektronicznego przy wykorzystaniu modułów kluczowych zawierających dane służące do odtworzenia danych służących do składania poświadczenia elektronicznego.

7.2.7 Metody aktywacji danych służących do składania poświadczenia elektronicznego

Dane służące do składania poświadczenia elektronicznego wykorzystywane przez Narodowe Centrum Certyfikacji odtwarza się i aktywuje się przy wykorzystaniu modułów kluczowych zawierających dane służące do odtwarzania danych służących do składania poświadczenia elektronicznego.

Stosowane są równocześnie mechanizmy kontroli dostępu do pomieszczeń, rejestracji w systemie oraz mechanizmy kontroli dostępu do aplikacji obejmujących zastosowanie modułów kluczowych.

7.2.8 Metody dezaktywacji danych służących do składania poświadczenia elektronicznego

Dane służące do składania poświadczenia elektronicznego mogą być dezaktywowane poprzez ich usunięcie z komponentu technicznego za pomocą aplikacji zarządzającej tym komponentem.

7.2.9 Metody niszczenia danych służących do składania poświadczenia elektronicznego

Dane służące do składania poświadczenia elektronicznego przez Narodowe Centrum Certyfikacji są niszczone poprzez usunięcie ich z komponentów technicznych w bezpieczny sposób zgodnie z następującymi zasadami:

1. Dane służące do składania poświadczenia elektronicznego niszczy się, gdy upłynie termin ważności zaświadczenia certyfikacyjnego lub zostanie ono unieważnione;
2. Komponenty techniczne umożliwiają skasowanie danych służących do składania poświadczenia elektronicznego i kluczy infrastruktury na żądanie podmiotu upoważnionego;
3. Niszczenie danych służących do składania poświadczenia elektronicznego i prywatnych kluczy infrastruktury uniemożliwia ich odtworzenie na podstawie analizy zapisów w urządzeniach, w których były tworzone, przechowywane lub stosowane.

W przypadku usuwania danych służących do składania poświadczenia elektronicznego z modułów kluczowych niszczy się moduł kluczowy.

Zasady niszczenia definiują procedury Narodowego Centrum Certyfikacji.

7.3 Inne aspekty zarządzania danymi służącymi do składania i weryfikacji poświadczenia elektronicznego

7.3.1 Archiwizacja danych służących do weryfikacji poświadczenia elektronicznego

Dane służące do weryfikacji poświadczenia elektronicznego Narodowego Centrum Certyfikacji oraz zaświadczenia certyfikacyjne Subskrybenta są archiwizowane po wygaśnięciu okresu ważności tych danych i przechowywane przez okres co najmniej 20 lat.

7.3.2 Długość okresu ważności danych służących do składania poświadczenia elektronicznego

Długość okresu ważności danych służących do składania poświadczenia elektronicznego i danych służących do weryfikacji poświadczenia elektronicznego jest równa okresowi ważności zaświadczenia certyfikacyjnego, który został określony w § 8 ust 1 i 2 Rozporządzenia Ministra Gospodarki z dnia 9 sierpnia 2002 r. w sprawie określenia szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem elektronicznym (Dz. U. Nr 128, poz 1101).

7.4 Dane aktywujące

Dane służące do składania poświadczenia elektronicznego są chronione przed nieuprawnioną aktywacją poprzez zastosowanie odpowiednich mechanizmów kontroli dostępu, obejmujących między innymi konieczność posiadania odpowiednich kart elektronicznych i znajomość PIN-ów tych kart oraz haseł dostępu do systemu teleinformatycznego.

7.4.1 Tworzenie i instalacja danych aktywujących

Dane aktywujące komponent techniczny obejmują dane służące do uwierzytelnienia Operatora Systemu, zapisane na kartach elektronicznych, PIN-y tych kart oraz hasła do dostępu do systemu teleinformatycznego.

Dane te są tworzone, instalowane oraz udostępniane odpowiednio przez uprawnione osoby pełniące funkcje w Narodowym Centrum Certyfikacji, na zasadach określonych w procedurach Narodowego Centrum Certyfikacji.

7.4.2 Ochrona danych aktywujących

Dane aktywujące komponenty techniczne podlegają szczególnej ochronie. Karty elektroniczne są przechowywane w Narodowym Centrum Certyfikacji w sposób zapewniający odpowiedni poziom bezpieczeństwa, pod nadzorem Inspektora Bezpieczeństwa Systemu. PIN-y kart oraz hasła dostępu do systemu teleinformatycznego są znane jedynie ich właścicielom.

Dodatkowo, opracowane są procedury udostępniania PIN-ów kart i haseł dostępu do systemu teleinformatycznego innym upoważnionym osobom, w sytuacjach awaryjnych.

7.4.3 Inne aspekty dotyczące danych aktywujących

Nie dotyczy.

7.5 Bezpieczeństwo systemów informatycznych Narodowego Centrum Certyfikacji

7.5.1 Ocena poziomu zabezpieczeń systemu informatycznego

Narodowe Centrum Certyfikacji wykorzystuje system zapewniający poziom bezpieczeństwa wymagany przez *Ustawę o podpisie elektronicznym* oraz odpowiednie akty wykonawcze.

7.5.2 Bezpieczny rozwój systemu informatycznego

Rozwój aplikacji na potrzeby własne oraz użytkowników końcowych odbywa się w wydzielonym środowisku testowym, przy zastosowaniu odpowiednich środków kontroli jakości.

Praca nad rozwojem aplikacji odbywa się w wydzielonym środowisku testowym.

7.5.3 Środki zabezpieczenia sieci komputerowej

Komponenty techniczne służące do składania poświadczenia elektronicznego nie są dołączone do sieci zewnętrznej. Komunikacja ze światem zewnętrznym odbywa się za pomocą nośników danych.

Elementy systemu teleinformatycznego służące do publikacji informacji związanych z pełnieniem przez Narodowe Centrum Certyfikacji roli podmiotu upoważnionego są chronione przed nieuprawnionym dostępem.

7.5.4 Środki zabezpieczenia komponentów technicznych

Komponenty techniczne używane przez Narodowe Centrum Certyfikacji spełniają wymagania określone w Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. Nr 128, poz. 1094), w tym przepisy § 4, 5, 7 i 18.

8 Profile zaświadczenia certyfikacyjnego oraz listy unieważnionych zaświadczeń certyfikacyjnych

8.1 Profil zaświadczenia certyfikacyjnego

Profil zaświadczenia certyfikacyjnego zdefiniowano w Załączniku nr 2 do Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. Nr 128, poz. 1094).

Na użytek Narodowego Centrum Certyfikacji jako podmiotu upoważnionego profil zaświadczeń certyfikacyjnych oraz list unieważnionych zaświadczeń certyfikacyjnych został określony w załączniku nr 1 i 2.

8.1.1 Wersja formatu zaświadczenia certyfikacyjnego

Zgodnie z Załącznikiem nr 2 do Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. Nr 128, poz. 1094) wartość pola powinna wynosić 2 wskazując, że numerem wersji certyfikatu jest v3.

8.1.2 Rozszerzenia zaświadczeń certyfikacyjnych

Zgodnie z Załącznikiem nr 2 do Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. Nr 128, poz. 1094) stosowane będą następujące rozszerzenia zaświadczeń certyfikacyjnych:

1. authorityKeyIdentifier;
2. subjectKeyIdentifier;
3. keyUsage;
4. certificatePolicies;
5. basicConstrains;
6. extKeyUsage;

8.1.3 Identyfikatory obiektów stosowanych algorytmów

Dopuszczalne są następujące identyfikatory algorytmów dla zdefiniowanych powyżej kluczy publicznych:

Algorytm	Identyfikator
RsaEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }

Patrz Załącznik nr 2 do Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. Nr 128, poz. 1094).

8.1.4 Nazwy

Patrz Załącznik nr 2 do Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. Nr 128, poz. 1094).

8.1.5 Zasady dotyczące nazw

Patrz Załącznik nr 2 do Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. Nr 128, poz. 1094).

8.1.6 Informacje dotyczące polityki certyfikacji

Patrz Załącznik nr 2 do Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. Nr 128, poz. 1094).

8.2 Profil listy unieważnionych zaświadczeń certyfikacyjnych

Profil listy unieważnionych zaświadczeń certyfikacyjnych zdefiniowano w załączniku nr 2.

8.2.1 Wersja formatu listy unieważnionych zaświadczeń certyfikacyjnych

Wartość pola powinna wynosić 1 wskazując, że numerem wersji CRL jest v2 - patrz Załącznik nr 2 do Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r.

w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. Nr 128, poz. 1094).

8.2.2 Rozszerzenia listy unieważnionych zaświadczeń certyfikacyjnych

W skład profilu listy unieważnionych zaświadczeń certyfikacyjnych, wydawanej przez Narodowe Centrum Certyfikacji, jako podmiot upoważniony, wchodzą pola określone w załączniku nr 2.

9 Zarządzanie zawartością Polityki Certyfikacji

9.1 Procedura wprowadzania zmian

Za wprowadzanie zmian do Polityki Certyfikacji odpowiedzialny jest Dyrektor Departamentu Ochrony Narodowego Banku Polskiego.

Za zatwierdzenie bądź odrzucenie wprowadzonych zmian, odpowiedzialny jest Zarząd Narodowego Banku Polskiego. Wszelkie zmiany dokonywane są z uwzględnieniem opinii ministra właściwego do spraw gospodarki.

9.1.1 Elementy Polityki Certyfikacji, które mogą być zmieniane bez powiadamiania

Jedyne zmiany, które można wprowadzić do Polityki Certyfikacji bez powiadamiania Subskrybenta to poprawki błędów edytorskich oraz zmiana danych kontaktowych.

9.1.2 Zmiany wprowadzane z powiadomieniem

Dowolny zapis w Polityce Certyfikacji może być zmieniony z uwzględnieniem 30-dniowego okresu zgłaszania uwag i poprawek. W razie uzasadnionej potrzeby okres zgłaszania uwag i poprawek może zostać skrócony do 5 dni.

Wszelkie proponowane zmiany, które mogą w istotny sposób wywrzeć wpływ na użytkowników Polityki Certyfikacji, będą zamieszczane w Repozytorium.

Podmioty, których interesów dotyczy proponowana zmiana, mogą zgłaszać do Dyrektora Departamentu Ochrony komentarze dotyczące proponowanych zmian.

Działania podjęte jako skutek zgłoszonych komentarzy są niezawisłą decyzją Narodowego Banku Polskiego.

Jeżeli zaproponowana zmiana, na skutek zgłoszonego komentarza ulega modyfikacji, to zawiadomienie o treści zmodyfikowanej zmiany powinno być ogłoszone na minimum 20 dni przed momentem wprowadzenia zmiany w życie.

9.2 Publikacja Polityki Certyfikacji

Aktualna i poprzednia wersja Polityki Certyfikacji są dostępne w Repozytorium (adres podano w definicji Repozytorium).

9.3 Procedura zatwierdzania Polityki Certyfikacji

Zmiany w Polityce Certyfikacji wprowadzane są przez Dyrektora Departamentu Ochrony Narodowego Banku Polskiego. Zarząd Narodowego Banku Polskiego zatwierdza wprowadzone zmiany.

Załącznik nr 1 - Profil zaświadczenia certyfikacyjnego

Zaświadczenie certyfikacyjne	
Pole (typ pola)	**Uwagi**
tbsCertificate (*TBSCertificate*)	Właściwa treść zaświadczenia certyfikacyjnego.
version (*Version*)	Wersja zaświadczenia certyfikacyjnego, wartość pola: 2 (wersja v3) .
serialNumber (*CertificateSerialNumber*)	Unikalny numer seryjny.
signature (*AlgorithmIdentifier*)	Identyfikator algorytmu poświadczenia elektronicznego stosowanego przez podmiot upoważniony.
algorithm (*OBJECT IDENTIFIER*)	Identyfikator obiektu: { iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }
parameters	**null**
issuer (*Name*)	Unikalna nazwa wyróżniająca podmoitu upoważnionego: a. Dla zaświadczeń certyfikacyjnych wydanych przez urząd ***stary Root***: CN = CZiC Centrast SA O = CZiC Centrast SA w imienu Ministra Gospodarki C=PL b. Dla zaświadczeń certyfikacyjnych wydanych przez urząd ***nowy Root***: CN = Narodowe Centrum Certyfikacji (NCCert) O = Minister wlasciwy do spraw gospodarki C = PL
validity (*Validity*)	Oznaczenie okresu ważności zaświadczenia certyfikacyjnego.
notBefore (*Time*)	Początek okresu ważności zaświadczenia certyfikacyjnego.
notAfter (*Time*)	Koniec okresu ważności zaświadczenia certyfikacyjnego.
subject (*Name*)	Unikalna nazwa wyróżniająca: a. w przypadku zaświadczenia certyfikacyjnego dla kwalifikowanego podmiotu świadczącego usługi certyfikacyjne nazwa określana jest przez kwalifikowany podmiot świadczący usługi certyfikacyjne i dostarczana do Narodowego Centrum Certyfikacji wraz z decyzją ministra właściwego do spraw gospodarki. Pole to zawiera również numer wpisu w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne, b. w przypadku zaświadczenia certyfikacyjnego dla podmiotu upoważnionego pole ma wartość: – dla zaświadczenia certyfikacyjnego wydanego przez urząd ***stary Root***: CN = CZiC Centrast SA O = CZiC Centrast SA w imieniu Ministra Gospodarki C = PL – dla zaświadczenia certyfikacyjnego wydanego przez urząd ***nowy Root***: CN = Narodowe Centrum Certyfikacji (NCCert) O = Minister wlasciwy do spraw gospodarki C = PL
subjectPublicKeyInfo (*SubjectPublicKeyInfo*)	Wartość: 1. w przypadku zaświadczenia certyfikacyjnego dla kwalifikowanego podmiotu świadczącego usługi certyfikacyjne – danych służących do weryfikacji poświadczenia elektronicznego kwalifikowanego podmiotu świadczącego usługi certyfikacyjne wraz z identyfikatorem algorytmu, z którym stowarzyszone są te dane, 2. w przypadku zaświadczenia certyfikacyjnego dla podmiotu upoważnionego – danych służących do weryfikacji poświadczenia elektronicznego podmiotu upoważnionego wraz z identyfikatorem algorytmu, z którym stowarzyszone są te dane.

algorithm (*AlgorithmIdentifier*)	Identyfikator algorytmu, z którym stowarzyszone są dane służące do składania poświadczenia elektronicznego: 1. w przypadku zaświadczenia certyfikacyjnego dla kwalifikowanego podmiotu świadczącego usługi certyfikacyjne – wykorzystywane przez kwalifikowany podmiot świadczący usługi certyfikacyjne, 2. w przypadku zaświadczenia certyfikacyjnego dla podmiotu upoważnionego – wykorzystywane przez podmiot upoważniony.
algorithm (*OBJECT IDENTIFIER*)	Identyfikator obiektu przypisany algorytmowi, z którym stowarzyszone są dane służące do składania poświadczenia elektronicznego: 1. w przypadku zaświadczenia certyfikacyjnego dla kwalifikowanego podmiotu świadczącego usługi certyfikacyjne identyfikator określany jest przez kwalifikowany podmiot świadczący usługi certyfikacyjne i dostarczany do Narodowego Centrum Certyfikacji wraz z decyzją ministra właściwego do spraw gospodarki, 2. w przypadku zaświadczenia certyfikacyjnego dla podmiotu upoważnionego pole ma wartość: { iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 1}.
parameters	Atrybut: 1. w przypadku zaświadczenia certyfikacyjnego dla kwalifikowanego podmiotu świadczącego usługi certyfikacyjne – zgodny z polem **algorithm** i określany przez kwalifikowany podmiot świadczący usługi certyfikacyjne oraz dostarczany do Narodowego Centrum Certyfikacji wraz z decyzją ministra właściwego do spraw gospodarki, 2. w przypadku zaświadczenia certyfikacyjnego dla podmiotu upoważnionego: **null**
subjectPublicKey (*BIT STRING*)	Dane służące do weryfikacji poświadczenia elektronicznego: 1. w przypadku zaświadczenia certyfikacyjnego dla kwalifikowanego podmiotu świadczącego usługi certyfikacyjne – określane przez kwalifikowany podmiot świadczący usługi certyfikacyjne i dostarczane do Narodowego Centrum Certyfikacji wraz z decyzją ministra właściwego do spraw gospodarki, 2. w przypadku zaświadczenia certyfikacyjnego dla podmiotu upoważnionego – dane służące do weryfikacji poświadczenia elektronicznego podmiotu upoważnionego.
extensions (*Extensions*)	Rozszerzenia zaświadczenia certyfikacyjnego.
authorityKeyIdentifier (*AuthorityKeyIdentifier*)	**Rozszerzenie niekrytyczne** - Identyfikator danych służących do weryfikacji poświadczenia elektronicznego podmiotu upoważnionego.
keyIdentifier **(*KeyIdentifier*)**	Wartość skrótu (algorytm SHA-1) z danych służących do weryfikacji poświadczenia elektronicznego podmiotu upoważnionego.
authorityCertIssuer (*GeneralNames*)	Unikalna nazwa wyróżniająca zgodna z polem **issuer**.
authorityCertSerialNumber (*AuthorityCertSerialNumber*)	Numer seryjny zaświadczenia certyfikacyjnego podmiotu upoważnionego.
subjectKeyIdentifier (*KeyIdentifier)*	**Rozszerzenie niekrytyczne** - Identyfikator – wartość skrótu uzyskana przy użyciu algorytmu SHA-1 z danych służących do weryfikacji poświadczenia elektronicznego: 1. w przypadku zaświadczenia certyfikacyjnego dla kwalifikowanego podmiotu świadczącego usługi certyfikacyjne – komplementarnych z danymi służącymi do składania poświadczenia elektronicznego wykorzystywanymi przez kwalifikowany podmiot świadczący usługi certyfikacyjne, jeżeli pole to będzie znajdować się w żądaniu certyfikacji, 2. w przypadku zaświadczenia certyfikacyjnego dla podmiotu upoważnionego – komplementarnych z danymi służącymi do składania poświadczenia elektronicznego wykorzystywanymi przez podmiot upoważniony.

KeyUsage (*KeyUsage*)	**Rozszerzenie krytyczne** – sposób wykorzystania: 1. w przypadku zaświadczenia certyfikacyjnego dla kwalifikowanego podmiotu świadczącego usługi certyfikacyjne – danych służących do składania poświadczenia elektronicznego wykorzystywanych przez kwalifikowany podmiot świadczący usługi certyfikacyjne, 2. w przypadku zaświadczenia certyfikacyjnego dla podmiotu upoważnionego – danych służących do składania poświadczenia elektronicznego wykorzystywanych przez podmiot upoważniony.
certificatePolicies (*CertificatePolicies*)	**Rozszerzenie krytyczne** – Polityka certyfikacji podmiotu upoważnionego.
policyIdentifier (OBJECT IDENTIFIER)	Identyfikator polityki (anyPolicy) – wartość pola **{ 2 5 29 32 0 }**
policyQualifiers (PolicyQualifierInfo)	Informacja o polityce certyfikacji podmiotu upoważnionego.
qualifier (PolicyQualifierInfo)	Identyfikator rodzaju informacji o polityce certyfikacji (id-qt-cps) – wartość pola **{ 1 3 6 1 5 5 7 2 1 }**
cPSuri (IA5String)	URI do polityki certyfikacji – wartość pola: „www.nccert.pl”
basicConstrains (*BasicConstrains*)	**Rozszerzenie krytyczne** - Określenie, czy zaświadczenie certyfikacyjne jest dla kwalifikowanego podmiotu świadczącego usługi certyfikacyjne polegające na wydawaniu certyfikatów albo dla podmiotu upoważnionego.
cA (*BOOLEAN*)	Pole ma wartość: 1. **True** – w przypadku zaświadczenia certyfikacyjnego dla kwalifikowanego podmiotu świadczącego usługi certyfikacyjne polegające na wydawaniu certyfikatów albo dla podmiotu upoważnionego, 2. **False** – w pozostałych przypadkach.
extKeyUsage (lista pól typu *OBJECT IDENTIFIER*)	Rozszerzenie krytyczne: 1. w przypadku zaświadczenia certyfikacyjnego dla kwalifikowanego podmiotu świadczącego usługi certyfikacyjne polegające na wydawaniu certyfikatów albo dla podmiotu upoważnionego – pole nie występuje, **2.** w pozostałych przypadkach pole zawiera identyfikator obiektu wskazujący na rodzaj usługi certyfikacyjnej określony przez kwalifikowany podmiot świadczący usługi certyfikacyjne i dostarczany do Narodowego Centrum Certyfikacji wraz z decyzją ministra właściwego do spraw gospodarki.
SignatureAlgorithm (*AlgorithmIdentifier*)	identyfikator algorytmu poświadczenia elektronicznego podmiotu upoważnionego.
Algorithm (*OBJECT IDENTIFIER*)	identyfikator obiektu: { iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }
parameters	**null**
signatureValue (*BIT STRING*)	Wartość poświadczenia elektronicznego złożonego przez podmiot upoważniony.

Załącznik nr 2 - Profil listy unieważnionych zaświadczeń certyfikacyjnych

Lista unieważnionych zaświadczeń certyfikacyjnych	
Pole (typ pola)	**Uwagi**
tbsCertList (*TBSCertList*)	Poświadczona elektronicznie lista unieważnionych zaświadczeń certyfikacyjnych.
version (*Version*)	Wersja listy unieważnionych zaświadczeń certyfikacyjnych – wartość pola: 1 (wersja v2).
signature (*AlgorithmIdentifier*)	Identyfikator algorytmu poświadczenia elektronicznego stosowanego przez podmiot upoważniony.
algorithm (*OBJECT IDENTIFIER*)	identyfikator obiektu: { iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }
parameters	**null**
issuer (*Name*)	Unikalna nazwa wyróżniająca podmiotu upoważnionego: a. W przypadku listy generowanej przez urząd ***stary Root***: CN = CZiC Centrast SA O = CZiC Centrast SA w imieniu Ministra Gospodarki C = PL b. W przypadku listy generowanej przez urząd ***nowy Root***: CN = Narodowe Centrum Certyfikacji (NCCert) O = Minister wlasciwy do spraw gospodarki C = PL
thisUpdate (*Time*)	Data wydania listy.
nextUpdate (*Time*)	Przewidywana data wydania następnej listy.
revokedCertificates (*Name*)	Lista unieważnionych zaświadczeń certyfikacyjnych.
userCertificate (*CertificateSerialNumber*)	Numer seryjny unieważnionego zaświadczenia certyfikacyjnego.
revocationDate (*Time*)	Data i czas unieważnienia.
crlEntryExtensions (*Extensions*)	Rozszerzenia informacji o unieważnieniu dotyczące każdego zaświadczenia certyfikacyjnego oddzielnie.
cRLReason (*CRLReason*)	Przyczyna unieważnienia zaświadczenia certyfikacyjnego.
crlExtensions (*Extensions*)	Rozszerzenia listy unieważnionych zaświadczeń certyfikacyjnych.
authorityKeyIdentifier (*AuthorityKeyIdentifier*)	Identyfikator danych służących do składania poświadczenia elektronicznego wykorzystywanych przez podmiot upoważniony.
keyIdentifier (*KeyIdentifier*)	Wartość skrótu (algorytm SHA-1) z danych służących do weryfikacji poświadczenia elektronicznego podmiotu upoważnionego.
authorityCertIssuer (*GeneralNames*)	Unikalna nazwa wyróżniająca zgodna z polem **issuer**.
authorityCertSerialNumber (*AuthorityCertSerialNumber*)	Numer seryjny zaświadczenia certyfikacyjnego podmiotu upoważnionego.
cRLNumber (*Integer (0..MAX)*)	Numer kolejny listy unieważnionych zaświadczeń certyfikacyjnych.
signatureAlgorithm (*AlgorithmIdentifier*)	Ientyfikator algorytmu poświadczenia elektronicznego złożonego przez podmiot upoważniony.
algorithm (*OBJECT IDENTIFIER*)	identyfikator obiektu: { iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }
parameters	**null**
signatureValue (*BIT STRING*)	Wartość poświadczenia elektronicznego listy złożonego przez podmiot upoważniony.

Załącznik nr 3 - Profil żądania certyfikacji PKCS#10

Żądanie certyfikacji	
Pole (typ pola)	**Uwagi**
CertificationRequest (*CertificationRequest*)	Żądanie certyfikacji PKCS#10.
certificationRequestInfo (*CertificationRequestInfo*)	Właściwa treść żądania certyfikacji.
version (*Version*)	Wersja żądania certyfikacji, wartość pola: 0 (wersja v1)
subject (*Name*)	Unikalna nazwa wyróżniająca kwalifikowanego podmiotu świadczącego usługi certyfikacyjne – nazwa określana jest przez kwalifikowany podmiot świadczący usługi certyfikacyjne. Pole to musi zawierać również numer wpisu w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne.
subjectPKInfo (*SubjectPublicKeyInfo*)	Wartość danych służących do weryfikacji poświadczenia elektronicznego kwalifikowanego podmiotu świadczącego usługi certyfikacyjne wraz z identyfikatorem algorytmu, z którym stowarzyszone są te dane.
algorithm (*AlgorithmIdentifier*)	Identyfikator algorytmu, z którym stowarzyszone są dane służące do weryfikacji poświadczenia elektronicznego kwalifikowanego podmiotu świadczącego usługi certyfikacyjne.
Algorithm(1) (*OBJECT IDENTIFIER*)	Identyfikator obiektu przypisany algorytmowi, z którym stowarzyszone są dane służące do weryfikacji poświadczenia elektronicznego kwalifikowanego podmiotu świadczącego usługi certyfikacyjne.
parameters	Atrybut zgodny z polem **Algorithm(1)** i określany przez kwalifikowany podmiot świadczący usługi certyfikacyjne.
subjectPublicKey (*BIT STRING*)	Dane służące do weryfikacji poświadczenia elektronicznego kwalifikowanego podmiotu świadczącego usługi certyfikacyjne.
attributes (*Attributes*)	Atrybuty żądania certyfikacji do umieszczenia w zaświadczeniu certyfikacyjnym.
subjectKeyIdentifier (*SubjectKeyIdentifier*)	Pole opcjonalne – Identyfikator danych służących do weryfikacji poświadczenia elektronicznego kwalifikowanego podmiotu świadczącego usługi certyfikacyjne.
keyUsage (*KeyUsage*)	Zamierzony sposób wykorzystania danych służących do składania poświadczenia elektronicznego.
extKeyUsage (*ExtendedKeyUsage*)	Zamierzone rozszerzone zastosowanie danych służących do składania poświadczenia elektronicznego. **Pole nie występuje** w przypadku kwalifikowanego podmiotu świadczącego usługi certyfikacyjne polegające na wydawaniu certyfikatów.
signatureAlgorithm (*AlgorithmIdentifier*)	Identyfikator algorytmu poświadczenia elektronicznego składanego przez kwalifikowany podmiot świadczący usługi certyfikacyjne.
Algorithm(2) (*OBJECT IDENTIFIER*)	Identyfikator obiektu przypisany algorytmowi, z którym stowarzyszone są dane służące do składania poświadczenie elektronicznego.
parameters	Atrybut zgodny z polem **Algorithm(2)** i określany przez kwalifikowany podmiot świadczący usługi certyfikacyjne.
signatureValue (*BIT STRING*)	Wartość poświadczenia elektronicznego złożonego przez kwalifikowany podmiot świadczący usługi certyfikacyjne.

Załącznik nr 4 – Profil zaświadczenia certyfikacyjnego i listy CRL wydawanych przez Narodowe Centrum Certyfikacji w notacji ASN.1[15]

[15] opisana w normie ISO/IEC 8824 – Information technology – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1), wydanej przez International Organization for Standardization.

1 Zaświadczenie certyfikacyjne dla podmiotu kwalifikowanego świadczącego usługi certyfikacyjne polegające na wydawaniu certyfikatów

Zaświadczenie certyfikacyjne jest zgodne ze składnią obiektu Certificate opisanego przez normę X.509.

Zaświadczenie certyfikacyjne jest ciągiem trzech wymaganych pól, których typy przedstawiono poniżej:

```
| Certificate  ::=  SEQUENCE  {
|     tbsCertificate       TBSCertificate,
|     signatureAlgorithm   AlgorithmIdentifier,
|     signaturevalue       BIT STRING }
```

Poświadczona elektronicznie treść Zaświadczenia certyfikacyjnego określona jest przez typ TBSCertificate:

```
| TBSCertificate  ::=  SEQUENCE  {
|     version         [0]  Version DEFAULT v1,
|     serialNumber         CertificateSerialNumber,
|     signature            AlgorithmIdentifier,
|     issuer               Name,
|     validity             validity,
|     subject              Name,
|     subjectPublicKeyInfo SubjectPublicKeyInfo,
|     issuerUniqueID  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
|     subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
|     extensions      [3]  Extensions OPTIONAL }
|
| Version   ::= INTEGER {
|     v1(0), v2(1), v3(2) }
|
| CertificateSerialNumber  ::=  INTEGER
|
| Validity ::= SEQUENCE {
|     notBefore      Time,
|     notAfter       Time }
|
| Time ::= CHOICE {
|     utcTime        UTCTime,
|     generalTime    GeneralizedTime
|
| uniqueIdentifier ::= BIT STRING
|
| SubjectPublicKeyInfo  ::=  SEQUENCE  {
|     algorithm            AlgorithmIdentifier,
|     subjectPublicKey     BIT STRING }
|
| Extensions  ::=  SEQUENCE SIZE (1..MAX) OF Extension
|
| Extension  ::=  SEQUENCE  {
|     extnID      OBJECT IDENTIFIER,
|     critical    BOOLEAN DEFAULT FALSE,
```

```
|     extnValue   OCTET STRING }
```

1.1 Pole treści Zaświadczenia certyfikacyjnego

Pole tbsCertificate zawiera nazwy wydawcy Zaświadczenia certyfikacyjnego, nazwy użytkownika Zaświadczenia certyfikacyjnego, klucz publiczny podmiotu, okres ważności oraz inne informacje pomocnicze, w tym rozszerzenia. Zawartość tych pól przedstawiono poniżej.

1.1.1 Wersja Zaświadczenia certyfikacyjnego (version)

Wartość pola wynosi 2, wskazując że numerem wersji jest v3.

1.1.2 Numer seryjny (serialNumber)

Numer seryjny jest unikalny dla wszystkich zaświadczeń wydanych przez Narodowe Centrum Certyfikacji.
Numery seryjne generowane są w sposób losowy.
Numery seryjne zaświadczeń zaimportowanych z systemu CENTRAST mają rozmiar 4 bajtów, natomiast każde kolejne zaświadczenie certyfikacyjne, które jest wydawane przez Narodowe Centrum Certyfikacji ma 20 bajtowy, losowy numer seryjny.

1.1.3 Algorytm podpisu (signature)

Pole zawiera identyfikator oraz parametry algorytmu stosowanego do poświadczania elektronicznego zaświadczeń certyfikacyjnych. Pole to ma postać:

```
| AlgorithmIdentifier  ::=  SEQUENCE  {
|     algorithm     OBJECT IDENTIFIER,
|     parameters    ANY DEFINED BY algorithm OPTIONAL
```

W systemie Narodowego Centrum Certyfikacji pole algorithm przyjmuje następujące wartości:

Algorytm	Identyfikator
Sha-1WithRSAEncryption	{iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }

1.1.4 Wydawca (issuer)

Pole zawiera identyfikator wyróżniający podmiotu świadczącego usługi certyfikacyjne, który wydał zaświadczenie certyfikacyjne.

```
| Name ::= CHOICE {
|     rdnSequence RDNSequence}
```

```
|
| RDNSequence ::= SEQUENCE OF RelativeDistinguishedName
|
| RelativeDistinguishedName ::= SET OF AttributeTypeAndValue
|
| AttributeTypeAndValue ::= SEQUENCE {
|     type     AttributeType,
|     value    AttributeValue}
|
| AttributeType ::= OBJECT IDENTIFIER
|
| AttributeValue ::= ANY
|
| DirectoryString ::= CHOICE {
|     printablestring           PrintableString,
|     utf8String                UTF8String,
|     bmpString                 BMPString }
```

W systemie Narodowego Centrum Certyfikacji struktura identyfikatora wyróżniającego wystawcy zaświadczenia certyfikacyjnego jest następująca:

Dla urzędu ***stary Root***

* nazwa kraju (ang. countryName) = ‘PL’

* nazwa organizacji (ang. organizationName) = ‘CZiC Centrast SA w imieniu Ministra Gospodarki’

* nazwa powszechna (ang. commonName) = ‘CZiC Centrast S.A.’

Dla urzędu ***nowy Root***:

* nazwa kraju (ang. countryName) = ‘PL’

* nazwa organizacji (ang. organizationName) = ‘Minister wlasciwy do spraw gospodarki’

* nazwa powszechna (ang. commonName) = ‘Narodowe Centrum Certyfikacji (NCCert)’

1.1.5 Okres ważności zaświadczenia certyfikacyjnego (validity)

Pole zawiera oznaczenie początku i końca okresu ważności zaświadczenia certyfikacyjnego. Pole reprezentowane jest jako ciąg dwóch dat: daty początku ważności (notBefore) oraz daty końca ważności (notAfter).

Daty ważności do roku 2049 są kodowane w formacie UTCTime, począwszy zaś od 1 stycznia 2050 r. - w formacie GeneralizedTime.

```
| Validity :: = SEQUENCE {
|     notBefore       Time,
|     notAfter        Time }
```

```
|
| Time ::= CHOICE {
|      utcTime          UTCTime,
|      generalTime      GeneralizedTime }
```

Interpretacja dwucyfrowego sposobu zapisu roku w UTCTime (pola YY) jest następująca:

* jeśli YY jest większe lub równe 50, to rok powinien być interpretowany jako 19YY;

* jeśli YY jest mniejsze niż 50, to rok powinien być interpretowany jako 20YY.

1.1.6 Właściciel zaświadczenia certyfikacyjnego (subject)

Pole identyfikatora podmiotu subject umożliwia zidentyfikowanie podmiotu związanego z kluczem publicznym, umieszczonym w polu klucza publicznego wydanego zaświadczenia certyfikacyjnego.

Nazwy podmiotów, którym Narodowe Centrum Certyfikacji wydaje zaświadczenia certyfikacyjne konstruowane są z następujących pól

* nazwa kraju (ang. countryName) = PL

* organizacja (ang. organizationName)

* nazwa powszechna (ang. commonName)

* numer seryjny (ang. serialNumber)

1.1.7 Klucz publiczny podmiotu (subjectPublicKeyInfo)

Pole zawiera wartość klucza publicznego (dane służące do weryfikacji certyfikatów wydawanych przez kwalifikowany podmiot) wraz z identyfikatorem algorytmu, z którym
stowarzyszony jest klucz.

```
| SubjectPublicKeyInfo  ::=  SEQUENCE  {
|      algorithm            AlgorithmIdentifier,
|      subjectPublicKey     BIT STRING }
Dla algorytmu RSA klucz publiczny kodowany jest jako typ RSAPublicKey:

| RSAPublicKey ::= SEQUENCE {
|          modulus            INTEGER, -- n
|          publicExponent     INTEGER  -- e -- }
Dla algorytmu DSA, o którym mowa w pkt 1.1.3, kodowany jest jako typ
INTEGER.

Parametry grupy dla algorytmu DSA są zapisywane w strukturze
AlgorithmIdentifier obiektu SubjectPublicKeyInfo w postaci:
```

```
| Dss-Parms  ::=  SEQUENCE  {
|        p             INTEGER,
|        q             INTEGER,
|        g             INTEGER }
```

System Narodowego Centrum Certyfikacji obsługuje następujące identyfikatory algorytmów dla zdefiniowanych powyżej kluczy publicznych:

Algorytm	Identyfikator
RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }
Dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1 }

1.1.8 Unikalny identyfikator wystawcy (issuerUniqueIdentifier)

Pole nie występuje.

1.1.9 Unikalny identyfikator właściciela (subjectUniqueIdentifier)

Pole nie występuje.

1.1.10 Pola rozszerzeń certyfikatu X.509 v3 używane w zaświadczeniach certyfikacyjnych wydawanych przez Narodowe Centrum Certyfikacji

Pole rozszerzeń certyfikatu jest sekwencją jednego lub kilku rozszerzeń. Format oraz zawartość rozszerzeń, stosowanych w zaświadczeniach certyfikacyjnych, ma postać:

```
| Extensions  ::=  SEQUENCE SIZE (1..MAX) OF Extension
|
| Extension  ::=  SEQUENCE  {
|     extnID      OBJECT IDENTIFIER,
|     critical    BOOLEAN DEFAULT FALSE,
|     extnValue   OCTET STRING }
```

W zaświadczeniach certyfikacyjnych wydawanych przez system Narodowego Centrum Certyfikacji umieszczane są następujące rozszerzenia:

* authorityKeyIdentifier
* subjectKeyIdentifier
* keyUsage
* certificatePolicies
* basicConstraints

Ich zawartość została opisana poniżej.

1.1.10.1 Identyfikator klucza wydawcy (authorityKeyIdentifier)

Rozszerzenie to identyfikuje klucz publiczny służący do weryfikacji wydanego zaświadczenia certyfikacyjnego.

```
| id-ce   OBJECT IDENTIFIER ::=  {joint-iso-ccitt(2) ds(5) 29}
|
| id-ce-authorityKeyIdentifier  OBJECT IDENTIFIER   ::=   { id-ce 35 }
| AuthorityKeyIdentifier ::= SEQUENCE {
|     keyIdentifier             [0] Keyidentifier    OPTIONAL,
|     authorityCertIssuer       [1] GeneralNames     OPTIONAL,
|     authorityCertSerialNumber [2] CertificateSerialNumber OPTIONAL }
|
| KeyIdentifier ::= OCTET STRING
|
| GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName
|
| GeneralName ::= CHOICE {
|      otherName                      [0]     OtherName,
|      rfc822Name                     [1]     IA5String,
|      dNSName                        [2]     IA5String,
|      x400Address                    [3]     ORAddress,
|      directoryName                  [4]     Name,
|      ediPartyName                   [5]     EDIPartyName,
|      uniformResourceIdentifier      [6]     IA5String,
|      iPAddress                      [7]     OCTET STRING,
|      registeredID                   [8]     OBJECT IDENTIFIER }
```

W zaświadczeniach certyfikacyjnych wydawanych przez Narodowe Centrum Certyfikacji rozszerzenie zawiera pola:
* keyIdentifier,
* authorityCertIssuer – identyfikator wyróżniający wydawcy zaświadczenia, typu Name,
* authorityCertSerialNumber – numer seryjny aktualnego zaświadczenia certyfikacyjnego wydawcy.

Rozszerzenie nie jest krytyczne.

1.1.10.2 Identyfikator klucza podmiotu (subjectKeyIdentifier)

Rozszerzenie to umożliwia identyfikację zaświadczeń certyfikacyjnych, które zawierają określony klucz publiczny podmiotu.

```
| id-ce-subjectKeyIdentifier OBJECT IDENTIFIER ::= {id-ce 14}
| SubjectKeyIdentifier ::= KeyIdentifier
```

Rozszerzenie nie jest krytyczne.

1.1.10.3 Sposób wykorzystania klucza podmiotu (keyUsage)

Rozszerzenie to określa sposób wykorzystania klucza, np. klucz do zapewnienia poufności, klucz do wymiany kluczy, klucz do podpisywania itp.

```
| id-ce-keyUsage OBJECT IDENTIFIER ::=  { id-ce 15 }
| KeyUsage ::= BIT STRING {
```

```
|     digitalSignature    (0), -- klucz do realizacji podpisu
|                              elektronicznego
|     nonRepudiation      (1), -- klucz związany z realizacją
|                              usług niezaprzeczalności
|     keyEncipherment     (2), -- klucz do wymiany kluczy
|     dataEncipherment    (3), -- klucz do szyfrowania danych
|     keyAgreement        (4), -- klucz do uzgadniania kluczy
|     keyCertSign         (5), -- klucz do podpisywania certyfikatów i
|                              zaświadczeń certyfikacyjnych
|     cRLSign             (6), -- klucz do podpisywania list CRL
|     encipherOnly        (7), -- klucz tylko do szyfrowania
|     decipherOnly        (8)  -- klucz tylko do deszyfrowania }
```

W zaświadczeniach certyfikacyjnych wydawanych przez Narodowe Centrum Certyfikacji ustawione są następujące bity określające sposób wykorzystania klucza:

a) keyCertSign: klucz publiczny jest używany do weryfikacji poświadczeń elektronicznych w certyfikatach i zaświadczeniach certyfikacyjnych wydanych przez kwalifikowany podmiot świadczący usługi certyfikacyjne,

b) cRLSign: klucz publiczny jest używany do weryfikacji poświadczeń elektronicznych w listach unieważnionych i zawieszonych certyfikatów oraz listach unieważnionych i zawieszonych zaświadczeń certyfikacyjnych wydanych przez kwalifikowany podmiot świadczący usługi certyfikacyjne.

Rozszerzenie jest krytyczne.

1.1.10.4 Polityka certyfikacji (certificatePolicies)

Rozszerzenie określające polityki certyfikacji zawiera sekwencję jednej lub wielu polityk określających warunki świadczenia usług certyfikacyjnych przez kwalifikowany podmiot.

```
| id-ce-certificatePolicies OBJECT IDENTIFIER ::=  { id-ce 32 }
| anyPolicy OBJECT IDENTIFIER ::= {id-ce-certificate-policies 0}
|
| CertificatePolicies ::= SEQUENCE SIZE (1..MAX) OF PolicyInformation
|
| PolicyInformation ::= SEQUENCE {
|     policyIdentifier   CertPolicyId,
|     policyQualifiers   SEQUENCE SIZE (1..MAX) OF PolicyQualifierInfo
OPTIONAL }
|
| CertPolicyId ::= OBJECT IDENTIFIER
|
| PolicyQualifierInfo ::= SEQUENCE {
|     policyQualifierId  PolicyQualifierId,
|     qualifier          ANY DEFINED BY policyQualifierId }
|
| id-qt          OBJECT IDENTIFIER ::=  { id-pkix 2 }
| id-qt-cps      OBJECT IDENTIFIER ::=  { id-qt 1 }
| id-qt-unotice  OBJECT IDENTIFIER ::=  { id-qt 2 }
|
| PolicyQualifierId ::=  OBJECT IDENTIFIER ( id-qt-cps | id-qt-unotice
)
|
```

```
| Qualifier ::= CHOICE {
|     cPSuri           CPSuri,
|     userNotice       UserNOtice }
|
| CPSuri ::= IA5String
|
| UserNotice ::= SEQUENCE {
|     noticeRef        NoticeReference OPTIONAL,
|     explicitText     DisplayText OPTIONAL }
|
| NoticeReference ::= SEQUENCE {
|     organization     DisplayText,
|     noticeNumbers    SEQUENCE OF INTEGER }
|
| DisplayText ::= CHOICE {
|     visibleString    VisibleString  (SIZE (1..200)),
|     bmpString        BMPString      (SIZE (1..200)),
|     utf8String       UTF8String     (SIZE (1..200)) }
```

W zaświadczeniach certyfikacyjnych wydawanych przez Narodowe Centrum Certyfikacji umieszczany jest jeden identyfikator polityki anyPolicy z kwalifikatorem CPS, zawierającym pole CPSUri o następującej treści: ‘www.nccert.pl’.

Rozszerzenie jest krytyczne.

1.1.10.5 Podstawowe ograniczenia (basicConstraints)

Rozszerzenie umożliwia określenie, czy podmiot jest użytkownikiem końcowym, czy też podmiotem wydającym certyfikaty.

```
| id-ce-basicConstraints OBJECT IDENTIFIER ::=  { id-ce 19 }
| BasicConstraints ::= SEQUENCE {
|     cA                  BOOLEAN DEFAULT FALSE,
|     pathLenConstraint   INTEGER (0..MAX) OPTIONAL }
```

Pole cA określa, czy podmiot jest użytkownikiem końcowym (FALSE), czy też podmiotem wydającym certyfikaty lub zaświadczenia certyfikacyjne (TRUE).

W zaświadczeniach certyfikacyjnych wydawanych przez Narodowe Centrum Certyfikacji pole cA przyjmuje wartość (TRUE) oznaczającą że podmiot jest podmiotem wydającym certyfikaty, natomiast pole pathLenConstraint nie występuje.

Rozszerzenie jest krytyczne.

2 Zaświadczenie certyfikacyjne dla podmiotu kwalifikowanego świadczącego usługi w zakresie znakowania czasem

Profil zaświadczenia certyfikacyjnego dla podmiotu kwalifikowanego świadczącego usługi w zakresie znakowania czasem różni się w stosunku do profilu dla zaświadczenia certyfikacyjnego dla podmiotów kwalifikowanych świadczących usługi certyfikacyjne polegające na wydawaniu certyfikatów, jedynie w następujących pozycjach:
* właściciel zaświadczenia certyfikacyjnego (subject),
oraz w rozszerzeniach
* sposób wykorzystania klucza podmiotu (keyUsage),
* podstawowe ograniczenia (basicConstraints),
* rozszerzenie precyzujące obszar zastosowania certyfikatu (extKeyUsage).
Pozostałe pola zaświadczenia certyfikacyjnego są takie same jak w przypadku zaświadczenia dla podmiotów kwalifikowanych świadczących usługi certyfikacyjne polegające na wydawaniu certyfikatów.

2.1 Właściciel zaświadczenia certyfikacyjnego (subject)

Nazwy podmiotów, którym Narodowe Centrum Certyfikacji wydaje zaświadczenia certyfikacyjne w zakresie znakowania czasem konstruowane są z następujących pól:

* numer seryjny (ang. serialNumber)

* nazwa kraju (ang. countryName) = PL

* organizacja (ang. organizationName)

* nazwa powszechna (ang. commonName)

2.2 Rozszerzenia zaświadczenia certyfikacyjnego

Wymienione zostały tylko te rozszerzenia, które są inne niż w profilu dla podmiotu kwalifikowanego, świadczącego usługi certyfikacyjne polegające na wydawaniu certyfikatów, lub w tym profilu nie występują.

2.2.1 Sposób wykorzystania klucza podmiotu (keyUsage)

W zaświadczeniach certyfikacyjnych wydawanych przez Narodowe Centrum Certyfikacji dla podmiotów kwalifikowanych świadczących usługi w zakresie znakowania czasem ustawione są następujące bity określające sposób wykorzystania klucza:

a) digitalSignature: przeznaczenie certyfikatu do realizacji usługi uwierzytelnienia za pomocą podpisu cyfrowego w innych celach niż nonRepudiation, keyCertSign i cRLSign,

b) nonRepudiation: przeznaczenie certyfikatu dla zapewnienia usługi niezaprzeczalności przez osoby fizyczne, ale jednocześnie dla innego celu niż określony w pkt keyCertSign i cRLSign. Bit nonRepudiation może być ustawiony tylko w kwalifikowanych certyfikatach kluczy publicznych użytkowników służących do weryfikacji bezpiecznych podpisów elektronicznych i nie może być łączony z innymi przeznaczeniami, w tym w szczególności keyEncipherment, dataEncipherment i keyAgreement związanych z zapewnieniem poufności.

Rozszerzenie jest krytyczne.

2.2.2 Podstawowe ograniczenia (basicConstraints)

Dla podmiotów kwalifikowanych świadczących usługi w zakresie znakowania czasem, rozszerzenie to wskazuje, że zaświadczenie certyfikacyjne należy do użytkownika końcowego. Dlatego pole cA musi mieć wartość FALSE, która jest dla niego wartością domyślną. Z powyższych założeń wynika, że rozszerzenie to jest zapisywane jako pusta struktura SEQUENCE.

Rozszerzenie jest krytyczne.

2.2.3 Rozszerzenie precyzujące obszar zastosowania zaświadczenia certyfikacyjnego (extKeyUsage)

Pole to należy interpretować jako zawężenie dopuszczalnego obszaru zastosowania klucza, określonego w polu keyUsage.
Rozszerzenie to jest krytyczne, co oznacza, że zaświadczenie certyfikacyjne musi być stosowane tylko zgodnie ze wskazanym obszarem zastosowania.

```
| id-ce-extKeyUsage OBJECT IDENTIFIER ::= {id-ce 37}
|
| ExtKeyUsageSyntax ::= SEQUENCE SIZE (1..MAX) OF KeyPurposeId
| KeyPurposeId ::= OBJECT IDENTIFIER
```

Dla zaświadczeń wydawanych podmiotom kwalifikowanym świadczącym usługi w zakresie znakowania czasem zdefiniowano następujące zastosowanie, identyfikowane przez następujący OID:

```
| id-pkix OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
|                                 dod(6)internet(1)security(5)
|                                 mechanisms(5) pkix(7) }
|
| id-kp OBJECT IDENTIFIER ::= { id-pkix 3 }
| id-kp-timeStamping      OBJECT IDENTIFIER ::= {id-kp 8}
|      --  wiązanie wartości skrótu z czasem z wcześniej uzgodnionego
|      -- wiarygodnego źródła czasu; bity pola keyUsage, które są zgodne
|      -- z tym polem:
|      -- digitalSignature, nonRepudiation
```

Rozszerzenie jest krytyczne.

3 Zaświadczenie certyfikacyjne dla podmiotu kwalifikowanego świadczącego usługi w zakresie walidacji danych

Profil zaświadczenia certyfikacyjnego dla podmiotu kwalifikowanego świadczącego usługi w zakresie walidacji danych różni się w stosunku do profilu dla zaświadczenia certyfikacyjnego dla podmiotów kwalifikowanych świadczących usługi certyfikacyjne polegające na wydawaniu certyfikatów, jedynie w następujących pozycjach:

* właściciel zaświadczenia certyfikacyjnego (subject),

oraz w rozszerzeniach

* sposób wykorzystania klucza podmiotu (keyUsage),
* podstawowe ograniczenia (basicConstraints),
* rozszerzenie precyzujące obszar zastosowania certyfikatu (extKeyUsage).
* rozszerzenie określające sposób dostępu do usługi (subjectInfoAccess)
* punkty dystrybucji CRL (CRLDistributionPoints),

Pozostałe pola zaświadczenia certyfikacyjnego są takie same jak w przypadku zaświadczenia dla podmiotów kwalifikowanych świadczących usługi certyfikacyjne polegające na wydawaniu certyfikatów.

3.1 Właściciel zaświadczenia certyfikacyjnego (subject)

Nazwy podmiotów, którym Narodowe Centrum Certyfikacji wydaje zaświadczenia certyfikacyjne w zakresie walidacji danych konstruowane są z następujących pól:

* numer seryjny (ang. serialNumber)

* nazwa kraju (ang. countryName) = PL

* organizacja (ang. organizationName)

* nazwa powszechna (ang. commonName)

3.2 Rozszerzenia zaświadczenia certyfikacyjnego

Wymienione zostały tylko te rozszerzenia, które są inne niż w profilu dla podmiotu kwalifikowanego, świadczącego usługi certyfikacyjne polegające na wydawaniu certyfikatów, lub w tym profilu nie występują.

3.2.1 Sposób wykorzystania klucza podmiotu (keyUsage)

W zaświadczeniach certyfikacyjnych wydawanych przez Narodowe Centrum Certyfikacji dla podmiotów kwalifikowanych świadczących usługi w zakresie walidacji danych ustawione są następujące bity określające sposób wykorzystania klucza:

a) digitalSignature: przeznaczenie certyfikatu do realizacji usługi uwierzytelnienia za pomocą podpisu cyfrowego w innych celach niż nonRepudiation, keyCertSign i cRLSign,

b) nonRepudiation: przeznaczenie certyfikatu dla zapewnienia usługi niezaprzeczalności przez osoby fizyczne, ale jednocześnie dla innego celu niż określony w pkt keyCertSign i cRLSign. Bit nonRepudiation może być ustawiony tylko w kwalifikowanych certyfikatach kluczy publicznych użytkowników służących do weryfikacji bezpiecznych podpisów elektronicznych i nie może być łączony z innymi przeznaczeniami, w tym w szczególności keyEncipherment, dataEncipherment i keyAgreement związanych z zapewnieniem poufności.

Rozszerzenie jest krytyczne.

3.2.2 Podstawowe ograniczenia (basicConstraints)

Dla podmiotów kwalifikowanych świadczących usługi w zakresie walidacji danych, rozszerzenie to wskazuje, że zaświadczenie certyfikacyjne należy do użytkownika końcowego. Dlatego pole cA musi mieć wartość FALSE, ograniczenie na długość ścieżki certyfikacji – wartość zero.

Rozszerzenie jest krytyczne.

3.2.3 Rozszerzenie precyzujące obszar zastosowania zaświadczenia certyfikacyjnego (extKeyUsage)

```
| id-ce-extKeyUsage OBJECT IDENTIFIER ::= {id-ce 37}
|
| ExtKeyUsageSyntax ::= SEQUENCE SIZE (1..MAX) OF KeyPurposeId
| KeyPurposeId ::= OBJECT IDENTIFIER
```

Dla zaświadczeń wydawanych podmiotom kwalifikowanym świadczącym usługi w zakresie walidacji danych zdefiniowano następujące zastosowanie, identyfikowane przez następujący OID:

```
| id-kp-dvcs  OBJECT IDENTIFIER ::= { id-kp 10}
| id-kp OBJECT IDENTIFIER ::= { id-pkix 3 }
| id-pkix OBJECT IDENTIFIER ::={iso(1)identified-organization(3)dod(6)
|                                internet(1) security(5) mechanisms(5)
|                                pkix(7) }
```

Rozszerzenie jest krytyczne.

3.2.4 Rozszerzenie określające sposób dostępu do usługi (subjectInfoAccess)

```
| id-pe-subjectInfoAccess OBJECT IDENTIFIER ::= { id-pe 11 }
| id-pe OBJECT IDENTIFIER  ::=  { id-pkix 1 }
|
|   SubjectInfoAccessSyntax  ::=
|           SEQUENCE SIZE (1..MAX) OF AccessDescription
|
|   AccessDescription  ::=  SEQUENCE {
|          accessMethod          OBJECT IDENTIFIER,
|          accessLocation        GeneralName
```

Rozszerzenie jest niekrytyczne.

3.2.5 Rozszerzenie określające punkty dystrybucji list CRL (CRLDistributionPoints)

```
|CRLDistributionPoints ::= SEQUENCE SIZE (1..MAX) OF DistributionPoint
|
| DistributionPoint ::= SEQUENCE {
|      distributionPoint       [0]     DistributionPointName OPTIONAL,
|      reasons                 [1]     ReasonFlags OPTIONAL,
|      cRLIssuer               [2]     GeneralNames OPTIONAL }
|
| DistributionPointName ::= CHOICE {
|      fullName                [0]     GeneralNames,
|      nameRelativeToCRLIssuer [1]     RelativeDistinguishedName }
|
| ReasonFlags ::= BIT STRING {
|      unused                  (0),
|      keyCompromise           (1),
|      cACompromise            (2),
|      affiliationChanged      (3),
|      superseded              (4),
|      cessationOfOperation    (5),
|      certificateHold         (6),
|      privilegeWithdrawn      (7),
|      aACompromise            (8) }
```

4 Zaświadczenie certyfikacyjne dla podmiotu kwalifikowanego świadczącego usługi w zakresie poświadczania przedłożenia i odbioru

Profil zaświadczenia certyfikacyjnego dla podmiotu kwalifikowanego świadczącego usługi w zakresie poświadczania przedłożenia i odbioru różni się w stosunku do profilu dla zaświadczenia certyfikacyjnego dla podmiotów kwalifikowanych świadczących usługi certyfikacyjne polegające na wydawaniu certyfikatów, jedynie w następujących pozycjach:

* właściciel zaświadczenia certyfikacyjnego (subject),

oraz w rozszerzeniach

* sposób wykorzystania klucza podmiotu (keyUsage),
* podstawowe ograniczenia (basicConstraints),
* punkty dystrybucji CRL (CRLDistributionPoints),
* alternatywna nazwa podmiotu (SubjectAltName).

Pozostałe pola zaświadczenia certyfikacyjnego są takie same jak w przypadku zaświadczenia dla podmiotów kwalifikowanych świadczących usługi certyfikacyjne polegające na wydawaniu certyfikatów.

4.1 Właściciel zaświadczenia certyfikacyjnego (subject)

Nazwy podmiotów, którym Narodowe Centrum Certyfikacji wydaje zaświadczenia certyfikacyjne w zakresie poświadczania przedłożenia i odbioru konstruowane są z następujących pól:

* numer seryjny (ang. serialNumber)

* nazwa kraju (ang. countryName) = PL

* organizacja (ang. organizationName)

* nazwa powszechna (ang. commonName)

4.2 Rozszerzenia zaświadczenia certyfikacyjnego

Wymienione zostały tylko te rozszerzenia, które są inne niż w profilu dla podmiotu kwalifikowanego, świadczącego usługi certyfikacyjne polegające na wydawaniu certyfikatów, lub w tym profilu nie występują.

4.2.1 Sposób wykorzystania klucza podmiotu (keyUsage)

W zaświadczeniach certyfikacyjnych wydawanych przez Narodowe Centrum Certyfikacji dla podmiotów kwalifikowanych świadczących usługi w zakresie poświadczania przedłożenia i odbioru ustawione są bity określające sposób wykorzystania klucza:

a) digitalSignature: przeznaczenie certyfikatu do realizacji usługi uwierzytelnienia za pomocą podpisu cyfrowego w innych celach niż nonRepudiation, keyCertSign i cRLSign,

b) nonRepudiation: przeznaczenie certyfikatu dla zapewnienia usługi niezaprzeczalności przez osoby fizyczne, ale jednocześnie dla innego celu niż określony w pkt keyCertSign i cRLSign. Bit nonRepudiation może być ustawiony tylko w kwalifikowanych certyfikatach kluczy publicznych użytkowników służących do weryfikacji bezpiecznych podpisów elektronicznych i nie może być łączony z innymi przeznaczeniami, w tym w szczególności keyEncipherment, dataEncipherment i keyAgreement związanych z zapewnieniem poufności.

Rozszerzenie jest krytyczne.

4.2.2 Podstawowe ograniczenia (basicConstraints)

Dla podmiotów kwalifikowanych świadczących usługi w zakresie poświadczania przedłożenia i odbioru, rozszerzenie to wskazuje, że zaświadczenie certyfikacyjne należy do użytkownika końcowego. Pole cA musi mieć wartość FALSE, ograniczenie na długość ścieżki certyfikacji – wartość zero.

Rozszerzenie jest krytyczne.

4.2.3 Rozszerzenie określające punkty dystrybucji list CRL (CRLDistributionPoints)

```
|CRLDistributionPoints ::= SEQUENCE SIZE (1..MAX) OF DistributionPoint
|
| DistributionPoint ::= SEQUENCE {
|      distributionPoint       [0]     DistributionPointName OPTIONAL,
|      reasons                 [1]     ReasonFlags OPTIONAL,
|      cRLIssuer               [2]     GeneralNames OPTIONAL }
|
| DistributionPointName ::= CHOICE {
|      fullName                [0]     GeneralNames,
|      nameRelativeToCRLIssuer [1]     RelativeDistinguishedName }
|
| ReasonFlags ::= BIT STRING {
|      unused                  (0),
|      keyCompromise           (1),
|      cACompromise            (2),
|      affiliationChanged      (3),
|      superseded              (4),
|      cessationOfOperation    (5),
|      certificateHold         (6),
|      privilegeWithdrawn      (7),
|      aACompromise            (8) }
```

4.2.4 Rozszerzenie określające nazwę alternatywną wystawcy poświadczeń (subjectAltName)

Zaświadczenie certyfikacyjne w zakresie świadczenia usług certyfikacyjnych polegających na kwalifikowanym poświadczaniu przedłożenia i odbioru w polu alternatywna nazwa podmiotu (subjectAltName) powinno zawierać adres poczty elektronicznej (pole rfc822Name):

```
id-ce-subjectAltName OBJECT IDENTIFIER ::=  { id-ce 17 }
SubjectAltName ::= GeneralNames
GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName
GeneralName ::= CHOICE {
     otherName                       [0]     OtherName,
     rfc822Name                      [1]     IA5String,
     dNSName                         [2]     IA5String,
     x400Address                     [3]     ORAddress,
     directoryName                   [4]     Name,
     ediPartyName                    [5]     EDIPartyName,
     uniformResourceIdentifier       [6]     IA5String,
     iPAddress                       [7]     OCTET STRING,
     registeredID                    [8]     OBJECT IDENTIFIER }
```

Rozszerzenie jest niekrytyczne.

5 Zaświadczenie certyfikacyjne dla podmiotu kwalifikowanego świadczącego usługi w zakresie weryfikacji statusu certyfikatu

Profil zaświadczenia certyfikacyjnego dla podmiotu kwalifikowanego świadczącego usługi w zakresie weryfikacji statusu certyfikatu różni się w stosunku do profilu dla zaświadczenia certyfikacyjnego dla podmiotów kwalifikowanych świadczących usługi certyfikacyjne polegające na wydawaniu certyfikatów, jedynie w następujących pozycjach:

* właściciel zaświadczenia certyfikacyjnego (subject),

oraz w rozszerzeniach

* sposób wykorzystania klucza podmiotu (keyUsage),
* podstawowe ograniczenia (basicConstraints),
* rozszerzenie precyzujące obszar zastosowania certyfikatu (extKeyUsage).
* punkty dystrybucji CRL (CRLDistributionPoints),

Pozostałe pola zaświadczenia certyfikacyjnego są takie same jak w przypadku zaświadczenia dla podmiotów kwalifikowanych świadczących usługi certyfikacyjne polegające na wydawaniu certyfikatów.

5.1 Właściciel zaświadczenia certyfikacyjnego (subject)

Nazwy podmiotów, którym Narodowe Centrum Certyfikacji wydaje zaświadczenia certyfikacyjne w zakresie weryfikacji statusu certyfikatu konstruowane są z następujących pól:

* numer seryjny (ang. serialNumber)

* nazwa kraju (ang. countryName) = PL

* organizacja (ang. organizationName)

* nazwa powszechna (ang. commonName)

5.2 Rozszerzenia zaświadczenia certyfikacyjnego

Wymienione zostały tylko te rozszerzenia, które są inne niż w profilu dla podmiotu kwalifikowanego, świadczącego usługi certyfikacyjne polegające na wydawaniu certyfikatów, lub w tym profilu nie występują.

5.2.1 Sposób wykorzystania klucza podmiotu (keyUsage)

W zaświadczeniach certyfikacyjnych wydawanych przez Narodowe Centrum Certyfikacji dla podmiotów kwalifikowanych świadczących usługi w zakresie weryfikacji statusu certyfikatu ustawione są następujące bity określające sposób wykorzystania klucza:

a) digitalSignature: przeznaczenie certyfikatu do realizacji usługi uwierzytelnienia za pomocą podpisu cyfrowego w innych celach niż nonRepudiation, keyCertSign i cRLSign,

b) nonRepudiation: przeznaczenie certyfikatu dla zapewnienia usługi niezaprzeczalności przez osoby fizyczne, ale jednocześnie dla innego celu niż określony w pkt keyCertSign i cRLSign. Bit nonRepudiation może być ustawiony tylko w kwalifikowanych certyfikatach kluczy publicznych użytkowników służących do weryfikacji bezpiecznych podpisów elektronicznych i nie może być łączony z innymi przeznaczeniami, w tym w szczególności keyEncipherment, dataEncipherment i keyAgreement związanych z zapewnieniem poufności.

Rozszerzenie jest krytyczne.

5.2.2 Podstawowe ograniczenia (basicConstraints)

Dla podmiotów kwalifikowanych świadczących usługi w zakresie weryfikacji statusu certyfikatu, rozszerzenie to wskazuje, że zaświadczenie certyfikacyjne należy do użytkownika końcowego. Dlatego pole cA musi mieć wartość FALSE, ograniczenie na długość ścieżki certyfikacji – wartość zero.

Rozszerzenie jest krytyczne.

5.2.3 Rozszerzenie precyzujące obszar zastosowania zaświadczenia certyfikacyjnego (extKeyUsage)

```
| id-ce-extKeyUsage OBJECT IDENTIFIER ::= {id-ce 37}
|
| ExtKeyUsageSyntax ::= SEQUENCE SIZE (1..MAX) OF KeyPurposeId
| KeyPurposeId ::= OBJECT IDENTIFIER
```

Dla zaświadczeń wydawanych podmiotom kwalifikowanym świadczącym usługi w zakresie weryfikacji statusu certyfikatu zdefiniowano następujące zastosowanie, identyfikowane przez następujący OID:

```
| id-kp-OCSPSigning OBJECT IDENTIFIER ::= { id-kp 9 }
| id-kp OBJECT IDENTIFIER ::= { id-pkix 3 }
| id-pkix OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
|                                 dod(6)
|                                internet(1)   security(5)   mechanisms(5)
|                                pkix(7) }
```

Rozszerzenie jest krytyczne.

5.2.4 Rozszerzenie określające punkty dystrybucji list CRL (CRLDistributionPoints)

```
|CRLDistributionPoints ::= SEQUENCE SIZE (1..MAX) OF DistributionPoint
|
| DistributionPoint ::= SEQUENCE {
|      distributionPoint       [0]     DistributionPointName OPTIONAL,
|      reasons                 [1]     ReasonFlags OPTIONAL,
|      cRLIssuer               [2]     GeneralNames OPTIONAL }
|
| DistributionPointName ::= CHOICE {
|      fullName                [0]     GeneralNames,
|      nameRelativeToCRLIssuer [1]     RelativeDistinguishedName }
|
```

```
| ReasonFlags ::= BIT STRING {
|      unused                  (0),
|      keyCompromise           (1),
|      cACompromise            (2),
|      affiliationChanged      (3),
|      superseded              (4),
|      cessationOfOperation    (5),
|      certificateHold         (6),
|      privilegeWithdrawn      (7),
|      aACompromise            (8) }
```

6 Zaświadczenie certyfikacyjne dla podmiotu kwalifikowanego świadczącego usługi w zakresie poświadczeń depozytowych.

Profil zaświadczenia certyfikacyjnego dla podmiotu kwalifikowanego świadczącego usługi w zakresie poświadczeń depozytowych różni się w stosunku do profilu dla zaświadczenia certyfikacyjnego dla podmiotów kwalifikowanych świadczących usługi certyfikacyjne polegające na wydawaniu certyfikatów, jedynie w następujących pozycjach:

* właściciel zaświadczenia certyfikacyjnego (subject),

oraz w rozszerzeniach

* sposób wykorzystania klucza podmiotu (keyUsage),
* podstawowe ograniczenia (basicConstraints),
* punkty dystrybucji CRL (CRLDistributionPoints),
* alternatywna nazwa podmiotu (SubjectAltName).

Pozostałe pola zaświadczenia certyfikacyjnego są takie same jak w przypadku zaświadczenia dla podmiotów kwalifikowanych świadczących usługi certyfikacyjne polegające na wydawaniu certyfikatów.

6.1 Właściciel zaświadczenia certyfikacyjnego (subject)

Nazwy podmiotów, którym Narodowe Centrum Certyfikacji wydaje zaświadczenia certyfikacyjne w zakresie poświadczeń depozytowych konstruowane są z następujących pól:

* numer seryjny (ang. serialNumber)

* nazwa kraju (ang. countryName) = PL

* organizacja (ang. organizationName)

* nazwa powszechna (ang. commonName)

6.2 Rozszerzenia zaświadczenia certyfikacyjnego

Wymienione zostały tylko te rozszerzenia, które są inne niż w profilu dla podmiotu kwalifikowanego, świadczącego usługi certyfikacyjne polegające na wydawaniu certyfikatów, lub w tym profilu nie występują.

6.2.1 Sposób wykorzystania klucza podmiotu (keyUsage)

W zaświadczeniach certyfikacyjnych wydawanych przez Narodowe Centrum Certyfikacji dla podmiotów kwalifikowanych świadczących usługi w zakresie poświadczeń depozytowych ustawione są bity określające sposób wykorzystania klucza:

a) digitalSignature: przeznaczenie certyfikatu do realizacji usługi uwierzytelnienia za pomocą podpisu cyfrowego w innych celach niż nonRepudiation, keyCertSign i cRLSign,

b) nonRepudiation: przeznaczenie certyfikatu dla zapewnienia usługi niezaprzeczalności przez osoby fizyczne, ale jednocześnie dla innego celu niż określony w pkt keyCertSign i cRLSign. Bit nonRepudiation może być ustawiony tylko w kwalifikowanych certyfikatach kluczy publicznych użytkowników służących do weryfikacji bezpiecznych podpisów elektronicznych i nie może być łączony z innymi przeznaczeniami, w tym w szczególności keyEncipherment, dataEncipherment i keyAgreement związanych z zapewnieniem poufności.

Rozszerzenie jest krytyczne.

6.2.2 Podstawowe ograniczenia (basicConstraints)

Dla podmiotów kwalifikowanych świadczących usługi w zakresie poświadczeń depozytowych, rozszerzenie to wskazuje, że zaświadczenie certyfikacyjne należy do użytkownika końcowego. Pole cA musi mieć wartość FALSE, ograniczenie na długość ścieżki certyfikacji – wartość zero.

Rozszerzenie jest krytyczne.

6.2.3 Rozszerzenie określające punkty dystrybucji list CRL (CRLDistributionPoints)

```
|CRLDistributionPoints ::= SEQUENCE SIZE (1..MAX) OF DistributionPoint
|
| DistributionPoint ::= SEQUENCE {
|      distributionPoint       [0]     DistributionPointName OPTIONAL,
|      reasons                 [1]     ReasonFlags OPTIONAL,
|      cRLIssuer               [2]     GeneralNames OPTIONAL }
|
| DistributionPointName ::= CHOICE {
|      fullName                [0]     GeneralNames,
|      nameRelativeToCRLIssuer [1]     RelativeDistinguishedName }
|
| ReasonFlags ::= BIT STRING {
|      unused                  (0),
|      keyCompromise           (1),
|      cACompromise            (2),
|      affiliationChanged      (3),
|      superseded              (4),
|      cessationOfOperation    (5),
|      certificateHold         (6),
|      privilegeWithdrawn      (7),
|      aACompromise            (8) }
```

6.2.4 Rozszerzenie określające nazwę alternatywną wystawcy poświadczeń (subjectAltName)

Zaświadczenie certyfikacyjne w zakresie świadczenia usług polegających na kwalifikowanym poświadczaniu depozytowym w polu alternatywna nazwa podmiotu (subjectAltName) powinno zawierać adres poczty elektronicznej (pole rfc822Name):

```
id-ce-subjectAltName OBJECT IDENTIFIER ::=  { id-ce 17 }
```

```
SubjectAltName ::= GeneralNames
GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName
GeneralName ::= CHOICE {
     otherName                       [0]     OtherName,
     rfc822Name                      [1]     IA5String,
     dNSName                         [2]     IA5String,
     x400Address                     [3]     ORAddress,
     directoryName                   [4]     Name,
     ediPartyName                    [5]     EDIPartyName,
     uniformResourceIdentifier       [6]     IA5String,
     iPAddress                       [7]     OCTET STRING,
     registeredID                    [8]     OBJECT IDENTIFIER }
```

Rozszerzenie jest niekrytyczne.

7 Zaświadczenie certyfikacyjne dla podmiotu kwalifikowanego świadczącego usługi w zakresie poświadczeń rejestrowych i repozytoryjnych

Profil zaświadczenia certyfikacyjnego dla podmiotu kwalifikowanego świadczącego usługi w zakresie poświadczeń rejestrowych i repozytoryjnych różni się w stosunku do profilu dla zaświadczenia certyfikacyjnego dla podmiotów kwalifikowanych świadczących usługi certyfikacyjne polegające na wydawaniu certyfikatów, jedynie w następujących pozycjach:

* właściciel zaświadczenia certyfikacyjnego (subject),

oraz w rozszerzeniach

* sposób wykorzystania klucza podmiotu (keyUsage),
* podstawowe ograniczenia (basicConstraints),
* punkty dystrybucji CRL (CRLDistributionPoints),
* alternatywna nazwa podmiotu (SubjectAltName).

Pozostałe pola zaświadczenia certyfikacyjnego są takie same jak w przypadku zaświadczenia dla podmiotów kwalifikowanych świadczących usługi certyfikacyjne polegające na wydawaniu certyfikatów.

7.1 Właściciel zaświadczenia certyfikacyjnego (subject)

Nazwy podmiotów, którym Narodowe Centrum Certyfikacji wydaje zaświadczenia certyfikacyjne w zakresie poświadczeń rejestrowych i repozytoryjnych konstruowane są z następujących pól:

* numer seryjny (ang. serialNumber)

* nazwa kraju (ang. countryName) = PL

* organizacja (ang. organizationName)

* nazwa powszechna (ang. commonName)

7.2 Rozszerzenia zaświadczenia certyfikacyjnego

Wymienione zostały tylko te rozszerzenia, które są inne niż w profilu dla podmiotu kwalifikowanego, świadczącego usługi certyfikacyjne polegające na wydawaniu certyfikatów, lub w tym profilu nie występują.

7.2.1 Sposób wykorzystania klucza podmiotu (keyUsage)

W zaświadczeniach certyfikacyjnych wydawanych przez Narodowe Centrum Certyfikacji dla podmiotów kwalifikowanych świadczących usługi w zakresie poświadczeń rejestrowych i repozytoryjnych ustawione są bity określające sposób wykorzystania klucza:

a) digitalSignature: przeznaczenie certyfikatu do realizacji usługi uwierzytelnienia za pomocą podpisu cyfrowego w innych celach niż nonRepudiation, keyCertSign i cRLSign,

b) nonRepudiation: przeznaczenie certyfikatu dla zapewnienia usługi niezaprzeczalności przez osoby fizyczne, ale jednocześnie dla innego celu niż określony w pkt keyCertSign i cRLSign. Bit nonRepudiation może być ustawiony tylko w kwalifikowanych certyfikatach kluczy publicznych użytkowników służących do weryfikacji bezpiecznych podpisów elektronicznych i nie może być łączony z innymi przeznaczeniami, w tym w szczególności keyEncipherment, dataEncipherment i keyAgreement związanych z zapewnieniem poufności.

Rozszerzenie jest krytyczne.

7.2.2 Podstawowe ograniczenia (basicConstraints)

Dla podmiotów kwalifikowanych świadczących usługi w zakresie poświadczeń rejestrowych i repozytoryjnych, rozszerzenie to wskazuje, że zaświadczenie certyfikacyjne należy do użytkownika końcowego. Pole cA musi mieć wartość FALSE, ograniczenie na długość ścieżki certyfikacji – wartość zero.

Rozszerzenie jest krytyczne.

7.2.3 Rozszerzenie określające punkty dystrybucji list CRL (CRLDistributionPoints)

```
|CRLDistributionPoints ::= SEQUENCE SIZE (1..MAX) OF DistributionPoint
|
| DistributionPoint ::= SEQUENCE {
|      distributionPoint       [0]     DistributionPointName OPTIONAL,
|      reasons                 [1]     ReasonFlags OPTIONAL,
|      cRLIssuer               [2]     GeneralNames OPTIONAL }
|
| DistributionPointName ::= CHOICE {
|      fullName                [0]     GeneralNames,
|      nameRelativeToCRLIssuer [1]     RelativeDistinguishedName }
|
| ReasonFlags ::= BIT STRING {
|      unused                  (0),
|      keyCompromise           (1),
|      cACompromise            (2),
|      affiliationChanged      (3),
|      superseded              (4),
|      cessationOfOperation    (5),
|      certificateHold         (6),
|      privilegeWithdrawn      (7),
|      aACompromise            (8) }
```

7.2.4 Rozszerzenie określające nazwę alternatywną wystawcy poświadczeń (subjectAltName)

Zaświadczenie certyfikacyjne w zakresie świadczenia usług polegających na kwalifikowanym poświadczaniu rejestrowym i repozytoryjnym w polu alternatywna nazwa podmiotu (subjectAltName) powinno zawierać adres poczty elektronicznej (pole rfc822Name):

```
id-ce-subjectAltName OBJECT IDENTIFIER ::=  { id-ce 17 }
SubjectAltName ::= GeneralNames
GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName
GeneralName ::= CHOICE {
     otherName                       [0]     OtherName,
     rfc822Name                      [1]     IA5String,
     dNSName                         [2]     IA5String,
     x400Address                     [3]     ORAddress,
     directoryName                   [4]     Name,
     ediPartyName                    [5]     EDIPartyName,
     uniformResourceIdentifier       [6]     IA5String,
     iPAddress                       [7]     OCTET STRING,
     registeredID                    [8]     OBJECT IDENTIFIER }
```

Rozszerzenie jest niekrytyczne.

8 Zaświadczenie certyfikacyjne dla podmiotu kwalifikowanego świadczącego usługi w zakresie wydawania certyfikatów atrybutów.

Profil zaświadczenia certyfikacyjnego dla podmiotu kwalifikowanego świadczącego usługi w zakresie wydawania certyfikatów atrybutów różni się w stosunku do profilu dla zaświadczenia certyfikacyjnego dla podmiotów kwalifikowanych świadczących usługi certyfikacyjne polegające na wydawaniu certyfikatów, jedynie w następującej pozycji:

* właściciel zaświadczenia certyfikacyjnego (subject),

oraz w rozszerzeniu:

* punkty dystrybucji CRL (CRLDistributionPoints),

Pozostałe pola zaświadczenia certyfikacyjnego są takie same jak w przypadku zaświadczenia dla podmiotów kwalifikowanych świadczących usługi certyfikacyjne polegające na wydawaniu certyfikatów.

8.1 Właściciel zaświadczenia certyfikacyjnego (subject)

Nazwy podmiotów, którym Narodowe Centrum Certyfikacji wydaje zaświadczenia certyfikacyjne w zakresie wydawania certyfikatów atrybutów konstruowane są z następujących pól:

* numer seryjny (ang. serialNumber)

* nazwa kraju (ang. countryName) = PL

* organizacja (ang. organizationName)

* nazwa powszechna (ang. commonName)

8.2 Rozszerzenia zaświadczenia certyfikacyjnego

Wymienione zostało tylko to rozszerzenie, które jest inne niż w profilu dla podmiotu kwalifikowanego świadczącego usługi certyfikacyjne polegające na wydawaniu certyfikatów, lub w tym profilu nie występują.

8.2.1 Rozszerzenie określające punkty dystrybucji list CRL (CRLDistributionPoints)

```
|CRLDistributionPoints ::= SEQUENCE SIZE (1..MAX) OF DistributionPoint
|
| DistributionPoint ::= SEQUENCE {
|      distributionPoint       [0]     DistributionPointName OPTIONAL,
|      reasons                 [1]     ReasonFlags OPTIONAL,
|      cRLIssuer               [2]     GeneralNames OPTIONAL }
|
| DistributionPointName ::= CHOICE {
|      fullName                [0]     GeneralNames,
|      nameRelativeToCRLIssuer [1]     RelativeDistinguishedName }
```

```
|
| ReasonFlags ::= BIT STRING {
|       unused                    (0),
|       keyCompromise             (1),
|       cACompromise              (2),
|       affiliationChanged        (3),
|       superseded                (4),
|       cessationOfOperation      (5),
|       certificateHold           (6),
|       privilegeWithdrawn        (7),
|       aACompromise              (8) }
```

9 Podstawowe pola listy CRL

Lista unieważnionych i zawieszonych certyfikatów i zaświadczeń certyfikacyjnych CertificateList jest ciągiem trzech pól, których znaczenie przedstawiono poniżej:

```
| CertificateList ::= SEQUENCE  {
|     tbsCertList         TBSCertList,
|     signatureAlgorithm  Algorithmrdentifier,
|     signatureValue      BIT STRING
| }
```

W skład profilu listy CRL wydanej przez Narodowe Centrum Certyfikacji wchodzą pola: version, signature, issuer, thisUpdate, nextUpdate, signatureAlgorithm, signatureValue oraz rozszerzenia (extension) cRLNumber i authorityKeyIdentifier. Ponadto dla niepustej listy CRL dodatkowo muszą zostać umieszczone, w stosunku do każdego zawieszanego lub unieważnianego zaświadczenia certyfikacyjnego, pola: userCertificate i revocationDate oraz rozszerzenie cRLReason.

9.1 Pole informacyjne (tbsCertList)

Pole to jest sekwencją zawierającą nazwę wydawcy, datę wydania, datę przewidywanego następnego wydania listy, listę unieważnionych i zawieszonych certyfikatów oraz opcjonalnie rozszerzenia. Lista unieważnionych i zawieszonych certyfikatów zawiera z kolei sekwencje definiujące unieważniany lub zawieszany certyfikat: numer seryjny, datę unieważnienia oraz opcjonalnie rozszerzenia listy CRL.

9.1.1 Pole algorytmu podpisu (signatureAlgorithm)

Pole to zawiera identyfikator algorytmu stosowanego do poświadczenia elektronicznego CertificateList. Pole jest typu AlgorithmIdentifier, zdefiniowanym w pkt 1.1.3, i musi zawierać taki sam identyfikator algorytmu, jaki zastosowano w przypadku pola signature sekwencji tbsCertList.

9.1.2 Wartość podpisu (signatureValue)

Pole zawiera poświadczenie elektroniczne sekwencji tbsCertList.

9.2 Poświadczona elektronicznie lista certyfikatów (tBSCertList)

Poświadczana elektronicznie lista zawieszonych i unieważnionych certyfikatów jest sekwencją obligatoryjnych lub opcjonalnych pól. Pola obligatoryjne identyfikują wydawcę CRL, opcjonalne zaś zawierają listy zawieszonych i unieważnionych certyfikatów oraz rozszerzenia CRL.

```
| TBSCertList ::= SEQUENCE  {
|     version              Version OPTIONAL,
|     signature            AlgorithmIdentifier,
|     issuer               Name,
|     thisupdate           Time,
|     nextUpdate           Time OPTIONAL,
|
|     revokedCertificates  SEQUENCE OF SEQUENCE {
|     userCertificate      CertificateSerialNumber,
|         revocationDate      Time,
|         crlEntryExtensions  Extensions OPTIONAL } OPTIONAL,
|     crlEXtensions   [0] EXPLICIT Extensions OPTIONAL }
```

9.2.1 Wersja (version)

Wartość pola wynosi 1, wskazując, że numerem wersji CRL jest v2.

9.2.2 Algorytm podpisu (signature)

Pole identyfikuje algorytm, jaki został użyty do poświadczenia elektronicznego listy CRL. Lista CRL jest poświadczona z użyciem algorytmu określonego w pkt 1.1.3.

9.2.3 Wydawca (issuer)

Pole zawiera identyfikator wyróżniający kwalifikowanego podmiotu świadczącego usługi certyfikacyjne, który wydał listę CRL.

Zawartość pola:

Dla urzędu ***stary Root***

* nazwa kraju (ang. countryName) = ‘PL’

* nazwa organizacji (ang. organizationName) = ‘CZiC Centrast SA w imieniu Ministra Gospodarki’

* nazwa powszechna (ang. commonName) = ‘CZiC Centrast S.A.’

Dla urzędu ***nowy Root***:

* nazwa kraju (ang. countryName) = ‘PL’

* nazwa organizacji (ang. organizationName) = ‘Minister wlasciwy do spraw gospodarki’

* nazwa powszechna (ang. commonName) = ‘Narodowe Centrum Certyfikacji (NCCert)’

9.2.4 Data wydania (thisUpdate)

Pole zawiera datę wydania listy CRL.

Zasady reprezentacji czasu są opisane w pkt 1.1.5.

9.2.5 Data następnego wydania (nextUpdate)

Pole zawiera datę, do której na pewno zostanie wydana następna lista CRL. Publikacja musi nastąpić wcześniej niż deklarowana data, ale w żadnym przypadku później.

Zasady reprezentacji czasu są opisane w pkt 1.1.5.

9.2.6 Certyfikaty unieważnione i zawieszone (revokedCertificates)

Ta część CRL zawiera listę zawieszonych i unieważnionych certyfikatów. Certyfikaty te identyfikowane są na podstawie numerów seryjnych (userCertificate). Określana jest także data zawieszenia lub unieważnienia certyfikatu (revocationDate) definiowana w sposób określony w pkt 1.1.5. Z każdym zawieszonym lub unieważnionym certyfikatem związać należy również przyczynę zawieszenia lub unieważnienia poprzez pole cRLReason,
określone w pkt 9.2.6.1.

Poniżej przedstawiono rozszerzenia crlEntryExtensions, dotyczących każdego z zawieszonych lub unieważnionych zaświadczeń certyfikacyjnych oddzielnie.
Każde z nich jest niekrytyczne.

9.2.6.1 Kod przyczyny unieważnienia/zawieszenia (cRLReason)

Pole jest niekrytycznym rozszerzeniem listy CRL, które umożliwia określenie przyczyny unieważnienia zaświadczenia certyfikacyjnego lub wskazania, że jest ono zawieszone. Kwalifikowany podmiot świadczący usługi certyfikacyjne i wydający zaświadczenia certyfikacyjne musi wskazać, czy zaświadczenie certyfikacyjne znajdujące się na liście CRL jest zawieszone, czy unieważnione. Składnia oraz OID tego rozszerzenia jest następujący:

```
| id-ce-cRLReason OBJECT IDENTIFIER ::= { id-ce 21 }
|
| CRLReason ::= ENUMERATED {
|     unspecified             (0),  -- nieokreślona (nieznana)
|     keyCompromise           (1),  -- kompromitacja klucza
|     cACompromise            (2),  -- kompromitacja klucza CC
|     affiliationChanged      (3),  -- zamiana danych (afiliacji)
|                                      subskrybenta
|     superseded              (4),  -- zastąpienie (odnowienie) klucza
```

```
|     cessationOfOperation     (5),   -- zaprzestanie operacji z
|                                        wykorzystaniem klucza
|     certificateHold          (6),   -- certyfikat zawieszony
|                                        (wstrzymany)
|     removeFromCRL            (8),   -- certyfikat wycofany z listy CRL
|     privilegeWithdrawn       (9),   -- certyfikat klucza publicznego
|                                        (   PKC)lub certyfikat atrybutów
|                                            został unieważniony z powodu
|                                        anulowania zawartych w nich
|                                        uprawnień
|     aaCompromise            (10)    -- kompromitacja atrybutów
|                                        potwierdzanych przez wystawcę
|                                        atrybutów }
```

W liście CRL wydawanej przez Narodowe Centrum Certyfikacji w polu CRLReason mogą znaleźć się następujące wartości:
a) unspecified: zaświadczenie certyfikacyjne zostało unieważnione, jednak przyczyna unieważnienia jest nieznana; powód unieważnienia nie wyklucza, że ma miejsce kompromitacja lub podejrzenie kompromitacji danych służących do poświadczania certyfikatów przez podmiot świadczący usługi certyfikacyjne,

b) keyCompromise: zaświadczenie certyfikacyjne zostało unieważnione z powodu kompromitacji lub podejrzenia kompromitacji danych służących do składania podpisu elektronicznego właściciela,

c) cACompromise: dotyczy tylko zaświadczeń certyfikacyjnych i oznacza, że zostało ono unieważnione z powodu kompromitacji danych służących do składania poświadczenia elektronicznego kwalifikowanego podmiotu świadczącego usługi certyfikacyjne,

d) affiliationChanged: certyfikat został unieważniony z powodu zmiany danych zawartych w certyfikacie; powód unieważnienia wskazuje, że nie ma miejsca kompromitacja lub podejrzenie kompromitacji danych służących do składania podpisu elektronicznego właściciela,

e) superseded: certyfikat został unieważniony z powodu zastąpienia klucza publicznego; powód unieważnienia wskazuje, że nie ma miejsca kompromitacja lub podejrzenie kompromitacji danych służących do składania podpisu elektronicznego właściciela,

f) cessationOfOperation: certyfikat został unieważniony z powodu zaprzestania używania go do celu, dla którego został wydany, i jednocześnie nie ma miejsca sytuacja określona w pkt d i e; wskazany powód unieważnienia wskazuje, że nie ma miejsca kompromitacja lub podejrzenie kompromitacji danych służących do składania podpisu elektronicznego właściciela,

g) certificateHold: certyfikat został zawieszony; ponieważ w Narodowym Centrum Certyfikacji występują wyłącznie zaświadczenia certyfikacyjne oraz certyfikaty infrastruktury, które nie mogą być zawieszane to przyczyna ta nie będzie używana.

9.2.7 Pola rozszerzeń (crlExtensions)

Profil listy CRL wydanej przez kwalifikowany podmiot świadczący usługi certyfikacyjne składa się z następujących rozszerzeń standardowych:

* authorityKeyIdentifier

* cRLNumber

Każde z rozszerzeń jest niekrytyczne.

9.2.7.1 Identyfikator klucza wydawcy (authorityKeyIdentifier)

Pole to umożliwia identyfikację danych służących do weryfikacji poświadczenia elektronicznego, odpowiadającego danym służącym do składania poświadczenia elektronicznego, zastosowanym do poświadczenia elektronicznego listy CRL. Składnia tego rozszerzenia opisana jest w pkt 1.1.10.1.

9.2.7.2 Numer CRL (cRLNumber)

Pole jest niekrytycznym rozszerzeniem CRL i określa monotonicznie zwiększany numer list CRL wydanych przez urząd certyfikacji. Dzięki temu rozszerzeniu użytkownik listy jest w stanie w prosty sposób określić, kiedy określony CRL zastąpił inny CRL. Składnia oraz OID tego rozszerzenia są następujące:

```
| id-ce-cRLNumber OBJECT IDENTIFIER ::= { id-ce 20 }
| cRLNumber ::= INTEGER (0..MAX)
```