NBP Narodowy Bank Polski

Polityka Certyfikacji Narodowego Centrum Certyfikacji

OID: 1.3.6.1.4.1.31995.3.3.0
wersja 3.0

Departament Bezpieczeństwa NBP
Warszawa, 2016

Spis treści

Uwaga dla Strony ufającej

Przed zaufaniem podpisowi elektronicznemu lub pieczęci elektronicznej weryfikowanej z wykorzystaniem certyfikatu dostawcy usług zaufania wydanego zgodnie z niniejszą Polityką Certyfikacji Narodowego Centrum 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. Wstęp

1.1 Wprowadzenie

Narodowe Centrum Certyfikacji to system informatyczny Narodowego Banku Polskiego, zwanego dalej „NBP", zbudowany w celu realizacji zadań powierzonych NBP przez ministra właściwego do spraw informatyzacji zgodnie z art. 11 ust.1 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. 2016 poz. 1579) zwanej dalej „ustawą o usługach zaufania". Narodowe Centrum Certyfikacji nie jest kwalifikowanym dostawcą usług zaufania.

Funkcjonowanie Narodowego Centrum Certyfikacji regulowane jest prawem obowiązującym na terytorium Rzeczpospolitej Polskiej, w szczególności ustawą o usługach zaufania oraz odpowiednimi przepisami wykonawczymi.

Postanowienia niniejszej Polityki Certyfikacji Narodowego Centrum Certyfikacji, zwanej dalej „Polityką", są wiążące dla NBP, Subskrybentów oraz Strony ufającej. Polityka znajduje zastosowanie w procesie wytwarzania i zarządzania certyfikatami dostawcy usług zaufania wydanymi przez Narodowe Centrum Certyfikacji. Polityka określa w szczególności: typy i zakres stosowania wydawanych certyfikatów dostawcy usług zaufania, zasady ich wydawania, uczestników procesu wydawania certyfikatów dostawcy usług zaufania, ich odpowiedzialność i obowiązki oraz zasady unieważniania wydanych certyfikatów dostawcy usług zaufania.

1.2 Nazwa dokumentu i jego identyfikacja

Nazwa dokumentu	Polityka Certyfikacji Narodowego Centrum Certyfikacji
Wersja dokumentu	3.0
Status dokumentu	Obowiązujący
Data wprowadzenia	22 grudnia 2016 r.
OID	1.3.6.1.4.1.31995.3.3.0
Lokalizacja	http://www.nccert.pl/files/PC_NCCert.pdf

1.3 Definicje

Na użytek Polityki przyjmuje się następujące pojęcia:

1) **Certyfikat** – certyfikat podpisu elektronicznego, certyfikat pieczęci elektronicznej, lub certyfikat uwierzytelniania witryn internetowych.

2) **Certyfikat podpisu elektronicznego** - poświadczenie elektroniczne, które przyporządkowuje dane służące do walidacji podpisu elektronicznego do osoby fizycznej i potwierdza co najmniej imię i nazwisko lub pseudonim tej osoby.

3) **Certyfikat pieczęci elektronicznej** - poświadczenie elektroniczne, które łączy dane służące do walidacji pieczęci elektronicznej z osobą prawną i potwierdza nazwę tej osoby.

4) **Certyfikat dostawcy usług zaufania** – certyfikat służący do weryfikacji zaawansowanych podpisów elektronicznych lub pieczęci elektronicznych, o których mowa w Załączniku I lit. g eIDAS, Załączniku III lit. g eIDAS, Załączniku IV lit. h eIDAS lub certyfikat służący do weryfikacji innych usług zaufania świadczonych przez kwalifikowanych dostawców usług zaufania.

5) **Certyfikat Narodowego Centrum Certyfikacji** – certyfikat do weryfikacji pieczęci elektronicznych, którymi Narodowe Centrum Certyfikacji opatruje certyfikaty dostawcy usług zaufania.

6) **Certyfikat uwierzytelniania witryn internetowych** – to poświadczenie, które umożliwia uwierzytelnianie witryn internetowych i przyporządkowuje witrynę internetową do osoby fizycznej lub prawnej, której wydano certyfikat.

7) **Dane służące do składania pieczęci elektronicznej** - niepowtarzalne dane, które podmiot składający pieczęć wykorzystuje do złożenia pieczęci elektronicznej

8) **Dane służące do składania podpisu elektronicznego** – unikalne dane, których podpisujący używa do składania podpisu elektronicznego.

9) **Dane służące do walidacji** - dane używane do walidacji podpisu elektronicznego lub pieczęci elektronicznej

10) **Dostawca usług zaufania** – osoba fizyczna lub prawna, która świadczy przynajmniej jedną usługę zaufania, jako kwalifikowany lub niekwalifikowany dostawca usług zaufania.

11) **eIDAS** – Rozporządzenie Parlamentu Europejskiego i Rady Unii Europejskiej Nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.

12) **Elektroniczny znacznik czasu** - dane w postaci elektronicznej, które wiążą inne dane w postaci elektronicznej z określonym czasem, stanowiąc dowód na to, że te inne dane istniały w danym czasie.

13) **Jednostka oceniająca zgodność** - jednostka określona w art. 2 pkt 13 rozporządzenia (WE) nr 765/2008, która jest akredytowana zgodnie z tym rozporządzeniem jako właściwa do przeprowadzania oceny zgodności kwalifikowanego dostawcy usługi zaufania i świadczonych przez niego kwalifikowanych usług zaufania

14) **Kwalifikowany certyfikat pieczęci elektronicznej** - certyfikat pieczęci elektronicznej, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku III do eIDAS.

15) **Kwalifikowany certyfikat podpisu elektronicznego** - certyfikat podpisu elektronicznego, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku I do eIDAS.

16) **Kwalifikowany certyfikat uwierzytelniania witryn internetowych** - certyfikat uwierzytelniania witryn internetowych, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku IV do eIDAS

17) **Kwalifikowany dostawca usług zaufania** - dostawca usług zaufania, który świadczy przynajmniej jedną kwalifikowaną usługę zaufania i któremu status kwalifikowany nadał organ nadzoru.

18) **Kwalifikowany elektroniczny znacznik czasu** - elektroniczny znacznik czasu, który spełnia następujące wymogi:

    a. wiąże on datę i czas z danymi tak, aby w wystarczający sposób wykluczyć możliwość niewykrywalnej zmiany danych;

    b. oparty jest na precyzyjnym źródle czasu powiązanym z uniwersalnym czasem koordynowanym;

    c. jest podpisany przy użyciu zaawansowanego podpisu elektronicznego lub opatrzony zaawansowaną pieczęcią elektroniczną kwalifikowanego dostawcy usług zaufania lub w inny równoważny sposób.

19) **Kwalifikowana pieczęć elektroniczna** - zaawansowana pieczęć elektroniczną, która została złożona za pomocą kwalifikowanego urządzenia do składania pieczęci elektronicznej i która opiera się na kwalifikowanym certyfikacie pieczęci elektronicznej.

20) **Kwalifikowany podpis elektroniczny** - zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego.

21) **Kwalifikowane urządzenie do składania pieczęci elektronicznej** - urządzenie do składania pieczęci elektronicznej, które spełnia odpowiednio wymogi określone w załączniku II do eIDAS;

22) **Kwalifikowane urządzenie do składania podpisu elektronicznego** - urządzenie do składania podpisu elektronicznego, które spełnia wymogi określone w załączniku II do eIDAS.

23) **Kwalifikowana usługa rejestrowanego doręczenia elektronicznego** - usługa rejestrowanego doręczenia elektronicznego, która spełnia następujące wymogi:

    a. jest świadczona przez co najmniej jednego kwalifikowanego dostawcę usług zaufania;

    b. z dużą dozą pewności zapewnia identyfikację nadawcy;

    c. zapewnia identyfikację adresata przed dostarczeniem danych;

    d. wysłanie i otrzymanie danych jest zabezpieczone zaawansowanym podpisem elektronicznym lub zaawansowaną pieczęcią elektroniczną kwalifikowanego dostawcy usług zaufania w taki sposób, by wykluczyć możliwość niewykrywalnej zmiany danych;

    e. każda zmiana danych niezbędna do celów wysłania lub otrzymania danych jest wyraźnie wskazana nadawcy i adresatowi danych;

    f. data i czas wysłania, otrzymania i wszelkiej zmiany danych są wskazane za pomocą kwalifikowanego elektronicznego znacznika czasu.

24) **Kwalifikowana usługa zaufania** - usługa zaufania, która spełnia stosowne wymogi określone w eIDAS.

25) **Lista CRL** – lista unieważnionych certyfikatów dostawcy usług zaufania.

26) **Narodowe Centrum Certyfikacji** - system informatyczny NBP zbudowany w celu realizacji zadań powierzonych NBP przez ministra właściwego do spraw informatyzacji, zgodnie z ustawą o usługach zaufania oraz identyfikacji elektronicznej.

27) **Organ nadzoru** – minister właściwy do spraw informatyzacji.

28) **Pieczęć elektroniczna** – dane w postaci elektronicznej dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, aby zapewnić autentyczność pochodzenia oraz integralność powiązanych danych.

29) **Podmiot składający pieczęć** - osoba prawna, która składa pieczęć elektroniczną;

30) **Podpis elektroniczny** – dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej, i które użyte są przez podpisującego jako podpis.

31) **Podpisujący** - osoba fizyczna, która składa podpis elektroniczny.

32) **Polityka świadczenia usług** - nazwany zestaw reguł, w szczególności takich jak polityka certyfikacji, mający zastosowanie do określonego kręgu podmiotów lub zastosowań, o wspólnych dla tego kręgu wymaganiach bezpieczeństwa.

33) **Produkt** - sprzęt lub oprogramowanie lub odpowiednie komponenty sprzętu lub oprogramowania, które są przeznaczone do wykorzystania w świadczeniu usług zaufania.

34) **Przepisy o usługach zaufania** – eIDAS wraz z aktami wykonawczymi oraz ustawa o usługach zaufania wraz z aktami wykonawczymi.

35) **Rejestr** – rejestr dostawców usług zaufania, o którym mowa w art. 3 ustawy o usługach zaufania.

36) **Repozytorium** – strona internetowa www.nccert.pl, na której publikowane są w szczególności certyfikaty dostawcy usług zaufania, listy unieważnionych certyfikatów dostawcy usług zaufania, krajowa zaufana lista oraz „Polityka Certyfikacji Narodowego Centrum Certyfikacji".

37) **Rozporządzenie** – Rozporządzenie Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie krajowej infrastruktury zaufania.

38) **Strona ufająca** - to osoba fizyczna lub prawna, która polega na identyfikacji elektronicznej lub usłudze zaufania.

39) **Subskrybent** – kwalifikowany dostawca usług zaufania.

40) **Urządzenie do składania pieczęci elektronicznej** - skonfigurowane oprogramowanie lub skonfigurowany sprzęt, które wykorzystuje się do składania pieczęci elektronicznej.

41) **Urządzenie do składania podpisu elektronicznego** - skonfigurowane oprogramowanie lub skonfigurowany sprzęt, które wykorzystuje się do składania podpisu elektronicznego.

42) **Usługa rejestrowanego doręczenia elektronicznego** - usługa umożliwiająca przesłanie danych między stronami trzecimi drogą elektroniczną i zapewniająca dowody związane z posługiwaniem się przesyłanymi danymi, w tym dowód wysłania i otrzymania

danych, oraz chroniącą przesyłane dane przed ryzykiem utraty, kradzieży, uszkodzenia lub jakiejkolwiek nieupoważnionej zmiany.

43) **Usługa zaufania** - usługa elektroniczna zazwyczaj świadczona za wynagrodzeniem i obejmująca:

   a. tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami; lub

   b. tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych; lub

   c. konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami

44) **Walidacja** - proces weryfikacji i potwierdzenia ważności podpisu elektronicznego lub pieczęci.

45) **Zaawansowana pieczęć elektroniczna** - pieczęć elektroniczna, która spełnia następujące wymogi:

   a. jest unikalnie przyporządkowana podmiotowi składającemu pieczęć;

   b. umożliwia ustalenie tożsamości podmiotu składającego pieczęć;

   c. jest składana przy użyciu danych służących do składania pieczęci elektronicznej, które podmiot składający pieczęć może, mając je z dużą dozą pewności pod swoją kontrolą, użyć do złożenia pieczęci elektronicznej;

   d. jest powiązana z danymi, do których się odnosi, w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna.

46) **Zaawansowany podpis elektroniczny** - podpis elektroniczny, który spełnia następujące wymogi:

   a. jest unikalnie przyporządkowany podpisującemu;

   b. umożliwia ustalenie tożsamości podpisującego;

   c. jest składany przy użyciu danych służących do składania podpisu elektronicznego, których podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą;

d. jest powiązany z danymi podpisanymi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna.

47) **Zaufana lista** – lista dostawców usług zaufania, o której mowa w art. 22 ust.1 eIDAS.

48) **Żądanie certyfikacyjne** – plik w formacie PKCS#10 zawierający między innymi nazwę wyróżniającą Subskrybenta oraz dane służące do walidacji.

1.4 Strony Polityki Certyfikacji

1.4.1 Narodowy Bank Polski

Na podstawie art. 11 ust. 1 ustawy o usługach zaufania, na wniosek Prezesa NBP, Minister Cyfryzacji powierzył w dniu 27 października 2016 r. NBP wykonywanie następujących zadań:

1. tworzenie i wydawanie kwalifikowanym dostawcom usług zaufania certyfikatów dostawcy usług zaufania;
2. publikacja danych służących do weryfikacji podpisów elektronicznych i pieczęci elektronicznych, o których mowa pkt 1;
3. publikacja listy unieważnionych certyfikatów, o których mowa w pkt 1;
4. tworzenie danych do opatrywania pieczęcią certyfikatów, o których mowa w pkt 1 oraz certyfikatów narodowego centrum certyfikacji usług zaufania;
5. prowadzenie Rejestru;
6. prowadzenie Zaufanej listy.

1.4.2 Narodowe Centrum Certyfikacji

Narodowe Centrum Certyfikacji to system informatyczny NBP zbudowany w celu realizacji zadań wymienionych w punkcie 1.4.1.

1.4.3 Punkt Rejestracji Użytkowników

Punkt rejestracji Narodowego Centrum Certyfikacji, prowadzony przez NBP w siedzibie Centrali NBP, jest odpowiedzialny za odbieranie i realizację wniosków ministra właściwego do spraw informatyzacji, w tym decyzji dotyczących unieważnienia certyfikatu dostawcy usług zaufania, a także za wymianę dokumentów oraz informacji pomiędzy Subskrybentem oraz ministrem właściwym do spraw informatyzacji, a Narodowym Centrum Certyfikacji.

1.4.4 Subskrybent

Subskrybentem jest kwalifikowany dostawca usług zaufania, któremu wydany został certyfikat dostawcy usług zaufania.

1.4.5 Strony ufające

Strona ufająca to to osoba fizyczna lub prawna, która polega na usłudze zaufania.

1.5 Zakres stosowania certyfikatów

Certyfikaty dostawcy usług zaufania wydawane Subskrybentowi przez Narodowe Centrum Certyfikacji służą do weryfikacji zaawansowanych podpisów elektronicznych lub pieczęci elektronicznych, o których mowa w Załączniku I lit. g eIDAS, Załączniku III lit. g eIDAS, Załączniku IV lit. h eIDAS, oraz do weryfikacji innych usług zaufania świadczonych przez Subskrybenta.

Zakres zastosowania certyfikatu dostawcy usług zaufania wydanego przez Narodowe Centrum Certyfikacji nie jest przez Narodowe Centrum Certyfikacji ograniczany i wynika z przepisów o usługach zaufania.

Zgodnie z art 16 ustawy o usługach zaufania zaawansowany podpis elektroniczny lub zaawansowana pieczęć elektroniczna weryfikowane przy pomocy certyfikatu dostawcy usług zaufania, służą do opatrywania podpisem elektronicznym lub pieczęcią elektroniczną:

1. certyfikatów kwalifikowanych, o których mowa w załączniku I lit. g eIDAS, załączniku III lit. g eIDAS, załączniku IV lit. h eIDAS;
2. informacji o statusie certyfikatów kwalifikowanych, w tym listy zawieszonych lub unieważnionych certyfikatów;
3. innych certyfikatów związanych ze świadczeniem kwalifikowanych usług zaufania.

Dodatkowo, patrz rozdział 6.1.7

1.6 Zarządzanie Polityką

1.6.1 Organizacja odpowiedzialna za zarządzaniem dokumentem

Autorem i podmiotem odpowiedzialnym za zarządzanie Polityką jest:

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

1.6.2 Kontakt

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

Narodowy Bank Polski
Departament Bezpieczeństwa
ul. Świętokrzyska 11/21
00-919 Warszawa
Polska
tel.: (+48 22) 185 15 13 fax: (+48 22) 185 23 36

https://www.nccert.pl e-mail: nccert@nccert.pl

1.6.3 Procedura zatwierdzania dokumentu

Ogólne zasady świadczenia usług zaufania przez NBP określone są w Uchwale nr 53/2016 Zarządu NBP. Polityka powstała na bazie załącznika nr 1 do ww. uchwały i jest zatwierdzana przez Dyrektora Departamentu Bezpieczeństwa w NBP.

Każda z wersji Polityki obowiązuje do czasu zatwierdzenia i opublikowania nowej wersji. Nowa wersja opracowywana jest przez pracowników NBP i ze statusem „do uzgodnienia" jest przekazywana do ministra właściwego do spraw informatyzacji oraz kwalifikowanych dostawców usług zaufania. Po uzgodnieniu dokumentu, nowa wersja Polityki zatwierdzana jest przez Dyrektora Departamentu Bezpieczeństwa w NBP.

Jedyne zmiany, które można wprowadzić do Polityki bez uzgadniania z ministrem właściwym do spraw informatyzacji i kwalifikowanych dostawców usług zaufania to poprawki błędów edytorskich oraz zmiana danych kontaktowych.

Dowolny zapis w Polityce może być zmieniony z uwzględnieniem 20-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 strony Polityki, będą zamieszczane w Repozytorium. Podmioty, których interesów dotyczy proponowana zmiana, mogą zgłaszać do Dyrektora Departamentu Bezpieczeństwa w NBP komentarze dotyczące proponowanych zmian. Działania podjęte jako skutek zgłoszonych komentarzy są niezawisłą decyzją NBP.

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.

W uzasadnionych przypadkach, w szczególności, gdy zmiany lub terminy ich wprowadzenia wynikają z przepisów prawa ww. terminy zgłaszania uwag lub zawiadamiania o modyfikacji zmian na skutek zgłoszonego komentarza mogą ulec dodatkowo skróceniu.

Aktualna i poprzednie wersje Polityki są dostępne w Repozytorium.

W przypadku, gdy zmiana zapisów Polityki pociąga za sobą konieczność zmiany Uchwały Zarządu NBP - przed opracowaniem nowej wersji Polityki konieczne jest dokonanie zmiany Uchwały Zarządu NBP. Zmiana uchwały odbywa się na zasadach obowiązujących w NBP.

2. Odpowiedzialność za publikację i repozytorium

2.1 Repozytorium

Repozytorium Narodowego Centrum Certyfikacji znajduje się na stronie internetowej www.nccert.pl .

2.2 Informacje publikowane w repozytorium

W Repozytorium publikowane są:

- Certyfikat Narodowego Centrum Certyfikacji (wystawiony w 2009 r.) – https://www.nccert.pl/files/nccert.crt ;
- Certyfikat Narodowego Centrum Certyfikacji (wystawiony w 2016 r.) – https://www.nccert.pl/files/nccert2016.crt
- Certyfikaty dostawców usług zaufania – https://www.nccert.pl/zaswiadczenia.htm ;
- Aktualna lista wydanych certyfikatów dostawców usług zaufania – https://www.nccert.pl/zaswiadczenia.htm ;
- Aktualna lista unieważnionych certyfikatów dostawców usług zaufania (odpowiadająca certyfikatowi wystawionemu w 2009 r.) – http://www.nccert.pl/arl/nccert-n.crl ;
- Aktualna lista unieważnionych certyfikatów dostawców usług zaufania – (odpowiadająca certyfikatowi wydanemu w 2016 r.) - http://www.nccert.pl/arl/nccert2016.crl ;
- Aktualna krajowa zaufana lista – https://www.nccert.pl/tsl/PL_TSL.xml ;
- Aktualny Rejestr - https://www.nccert.pl/podmioty.htm ;
- Aktualna wersja Polityki – https://www.nccert.pl/policies/PC_NCCert.pdf ;
- Wersje archiwalne Polityk - https://www.nccert.pl/archiwum.htm ;
- Informacje dodatkowe, np. ogłoszenia oraz informacje o proponowanych zmianach w Polityce – https://www.nccert.pl/komunikaty.htm .

2.3 Częstotliwość publikacji

- Certyfikaty Narodowego Centrum Certyfikacji – niezwłocznie po ich wytworzeniu;
- Certyfikaty dostawców usług zaufania – niezwłocznie po ich wytworzeniu i wydaniu;
- Aktualna lista wydanych certyfikatów dostawców usług zaufania – niezwłocznie po wytworzeniu i wydaniu certyfikatu kwalifikowanego dostawcy usług zaufania;
- Aktualna lista unieważnionych certyfikatów dostawców usług zaufania – nie rzadziej niż raz dziennie (z wyłączeniem sobót, niedziel oraz wszystkich dni ustawowo wolnych od pracy) oraz każdorazowo, niezwłocznie po unieważnieniu certyfikatu

dostawcy usług zaufania – nie później niż w ciągu 1 godziny od otrzymania przez Narodowe Centrum Certyfikacji, od ministra właściwego do spraw informatyzacji, decyzji o unieważnienie certyfikatu dostawcy usług zaufania;

- Aktualna Zaufana lista – co najmniej raz na 3 miesiące oraz niezwłocznie po wydaniu lub unieważnieniu certyfikatu kwalifikowanego dostawcy usług zaufania przez Narodowe Centrum Certyfikacji lub po każdej aktualizacji rejestru dostawców usług zaufania, o ile ta zmiana pociąga za sobą konieczność dokonania aktualizacji krajowej zaufanej listy;
- Aktualny Rejestr - modyfikowany każdorazowo, niezwłocznie po otrzymaniu polecenia dokonania wpisu do Rejestru od ministra właściwego do spraw informatyzacji;
- Polityka – wersję aktualnie obowiązującą, po każdorazowej zmianie dokumentu, niezwłocznie po zatwierdzeniu zmian, wraz z informacją o dacie wejścia w życie uchwalonych zmian;
- Informacje dodatkowe, np. ogłoszenia oraz informacje o proponowanych zmianach w Polityce – w razie takiej potrzeby.

2.4 Kontrola dostępu do repozytorium

Informacje publikowane w Repozytorium są publicznie dostępne do odczytu. Publikacja tych informacji dokonywana jest wyłącznie przez uprawnionych pracowników NBP.

3. Identyfikacja i uwierzytelnianie

Poniżej przedstawiono ogólne zasady przyjmowania przez Narodowe Centrum Certyfikacji decyzji ministra właściwego do spraw informatyzacji.

Polityka wyróżnia:

- Przyjęcie decyzji o wytworzeniu certyfikatu dostawcy usług zaufania oraz jego odbiór przez Subskrybenta;
- Przyjęcie decyzji o unieważnieniu certyfikatu dostawcy usług zaufania.

Nie przewiduje się przyjmowania decyzji związanych z zawieszaniem certyfikatów dostawcy usług zaufania.

Wydanie kwalifikowanemu dostawcy usług zaufania certyfikatu usług zaufania odbywa się na podstawie decyzji ministra właściwego do spraw informatyzacji, o której mowa w art. 4 ust. 6 ustawy o usługach zaufania. Decyzję minister przekazuje do NBP. Dane niezbędne do wystawienia certyfikatu dostawcy usług zaufania (żądanie certyfikacyjne) do NBP dostarcza dostawca usług zaufania. NBP wystawia certyfikat dostawcy usług zaufania niezwłocznie, nie później niż w terminie 3 dni roboczych od dnia otrzymania decyzji i poprawnych danych do wystawienia certyfikatu dostawcy usług zaufania.

3.1 Nadawanie nazw

Certyfikaty dostawcy usług zaufania wydawane przez Narodowe Centrum Certyfikacji są zgodne z normą X.509 v3. W szczególności oznacza to, że Narodowe Centrum Certyfikacji akceptuje tylko takie nazwy Subskrybentów, które są zgodne ze standardem X.509 (z powołaniem się na zalecenia serii X.500).

Dane umieszczane w certyfikacie dostawcy usług zaufania dostarczane są do Narodowego Centrum Certyfikacji w postaci żądania certyfikacyjnego.

Dane zawarte w żądaniu certyfikacyjnym muszą identyfikować w sposób jednoznaczny Subskrybenta i muszą być identyczne z danymi podanymi przez Subskrybenta we wniosku o dokonanie wpisu do Rejestru. W szczególności, w polu „Organizacja" znajdować się powinna nazwa Subskrybenta zgodna z nazwą firmy uwidocznioną w rejestrach publicznych (np. KRS, CEIDG).

3.1.1 Typy nazw

Nazwa zawarta w certyfikacie Narodowego Centrum Certyfikacji wystawionym w 2009 r. się z trzech następujących pól:

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

Nazwa zawarta w certyfikacie Narodowego Centrum Certyfikacji wystawionym w 2016 r. się z czterech następujących pól:

Nazwa pola	Zawartość
Kraj	PL
Organizacja	Narodowy Bank Polski
Nazwa powszechna	Narodowe Centrum Certyfikacji
Identyfikator Organizacji	VATPL-5250008198

Nazwa Subskrybenta zawarta w certyfikacie dostawcy usług zaufania, weryfikowanym certyfikatem Narodowego Centrum Certyfikacji wystawionym w 2009 r., składa się z czterech następujących pól:

Nazwa pola	Zawartość
Kraj	PL
Organizacja	*nazwa Subskrybenta*
Nazwa powszechna	*Nazwa podana przez Subskrybenta i związana z daną usługą zaufania*
Numer seryjny	*Numer wpisu w Rejestrze*

Nazwa Subskrybenta zawarta w certyfikacie dostawcy usług zaufania, weryfikowanym certyfikatem Narodowego Centrum Certyfikacji wystawionym w 2016 r., składa się z czterech następujących pól:

Nazwa pola	Zawartość
Kraj	PL
Organizacja	*nazwa Subskrybenta*
Nazwa powszechna	*Nazwa podana przez Subskrybenta i związana z daną usługą zaufania*
Identyfikator organizacji	VATPL – *numer NIP Subskrybenta*

3.1.2 Konieczność używania nazw znaczących

Nazwy umieszczone w certyfikacie dostawcy usług zaufania muszą umożliwiać jednoznaczną identyfikację Subskrybenta oraz Narodowego Centrum Certyfikacji.

3.1.3 Zasady interpretacji różnych form nazw

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

3.1.4 Unikalność nazw

Nazwa wyróżniająca Subskrybenta musi zapewnić jednoznaczne wskazanie Subskrybenta.

3.1.5 Rozpoznawanie, uwierzytelnianie oraz rola znaków towarowych

Nie ma zastosowania.

3.2 Początkowa walidacja tożsamości

3.2.1 Dowód posiadania danych do składania pieczęci elektronicznych

Dowodem posiadania danych służących do składania pieczęci elektronicznej skojarzonych z danymi służącymi do walidacji znajdującymi się w żądaniu certyfikacyjnym, jest weryfikacja pieczęci elektronicznej złożonej pod tym żądaniem, dokonana przy pomocy danych służących do walidacji znajdujących się w żądaniu. Narodowe Centrum Certyfikacji dokonuje dodatkowo porównania danych służących do walidacji znajdujących się w żądaniu certyfikacyjnym z danymi służącymi do walidacji, które zostały już wcześniej przyporządkowane do innego Subskrybenta w wydanych certyfikatach dostawcy usług zaufania. W przypadku powtórzenia się tych danych Narodowe Centrum Certyfikacji powiadamia o tym ministra właściwego do spraw informatyzacji.

3.2.2 Uwierzytelnienie tożsamości osób prawnych

Nie dotyczy.

3.2.3 Uwierzytelnienie tożsamości osób fizycznych

Nie dotyczy.

3.2.4 Dane Subskrybenta niepodlegające weryfikacji

Wszystkie dane Subskrybenta umieszczane w certyfikacie dostawcy usług zaufania podlegają weryfikacji w Narodowym Centrum Certyfikacji.

3.2.5 Walidacja urzędów i organizacji

Nie dotyczy.

3.2.6 Kryteria interoperacyjności

Nie dotyczy.

3.3 Identyfikacja i uwierzytelnienie w przypadku żądania aktualizacji danych do składania pieczęci elektronicznych

Identycznie jak w przypadku wydawania pierwszego certyfikatu dostawcy usług zaufania – patrz rozdział 3.2.

4. Wymagania funkcjonalne

4.1 Składanie wniosków

Narodowe Centrum Certyfikacji nie przyjmuje wniosków bezpośrednio od Subskrybenta. Wszystkie wnioski Subskrybentów muszą być kierowane do ministra właściwego do spraw informatyzacji. Narodowe Centrum Certyfikacji wytwarza i wydaje lub unieważnia certyfikaty dostawcy usług zaufania po otrzymaniu stosownej decyzji administracyjnej ministra właściwego do spraw informatyzacji.

W celu wytworzenia certyfikatu dostawcy usług zaufania Subskrybent przygotowuje żądanie certyfikacyjne, zgodne z profilem określonym w załączniku A do Polityki i przekazuje je do Narodowego Centrum Certyfikacji, wraz z informacją czy wystawiony certyfikat ma być opatrzony pieczęcią elektroniczną weryfikowaną certyfikatem Narodowego Centrum Certyfikacji wystawionym w 2009 r. czy certyfikatem wystawionym w 2016 r.

4.1.1 Kto może złożyć wniosek o wydanie certyfikatu ?

Wniosek o wydanie certyfikatu dostawcy usług zaufania, w formie decyzji administracyjnej ministra właściwego do spraw informatyzacji złożyć może tylko minister właściwy do spraw informatyzacji.

4.1.2 Proces składania wniosków i związane z tym obowiązki

Minister właściwy do spraw informatyzacji przekazuje wniosek na adres: Departament Bezpieczeństwa Narodowy Bank Polski, ul. Świętokrzyska 11/21, 00-919 Warszawa. W przypadku wniosku w postaci elektronicznej, minister właściwy do spraw informatyzacji przesyła wniosek, opatrzony kwalifikowanym podpisem elektronicznym na adresy mailowe sekretariat.DB@nbp.pl oraz nccert@nccert.pl .

Pracownik NBP pełniący funkcję Operatora Systemu w Narodowym Centrum Certyfikacji weryfikuje:

1. kwalifikowany podpis elektroniczny, którym opatrzony jest wniosek,
2. uprawnienia osoby, która opatrzyła decyzję kwalifikowanym podpisem elektronicznym,
3. poprawność i kompletność wniosku.

Po dokonaniu weryfikacji potwierdza otrzymanie wniosku drogą mailową na adres wskazany przez ministra właściwego do spraw informatyzacji.

W celu wytworzenia certyfikatu dostawcy usług zaufania Subskrybent przekazuje do Narodowego Centrum Certyfikacji żądanie certyfikacyjne, zgodne z profilem określonym w

załączniku A do Polityki. Żądanie może zostać przekazane, w formie pliku zapisanego na płycie CD, na adres: Departament Bezpieczeństwa Narodowy Bank Polski, ul. Świętokrzyska 11/21, 00-919 Warszawa, lub drogą mailową na adresy mailowe sekretariat.DB@nbp.pl oraz nccert@nccert.pl. W przypadku przesyłania żądania certyfikacyjnego drogą mailową, musi ono być opatrzone kwalifikowanym podpisem elektronicznym uprawnionego pracownika Subskrybenta.

4.2 Przetwarzanie wniosków

4.2.1 Realizacja funkcji identyfikacji i uwierzytelniania

Funkcje identyfikacji i uwierzytelniania są realizowane przez Narodowe Centrum Certyfikacji zgodnie z warunkami określonymi w rozdziale 3.2.

4.2.2 Przyjęcie lub odrzucenie wniosku

Wniosek przesłany przez ministra właściwego do spraw informatyzacji zostaje przyjęty przez Narodowe Centrum Certyfikacji tylko w przypadku, gdy wszystkie etapy weryfikacji opisane w punkcie 4.1.2 zostaną zakończone z wynikiem pozytywnym. W przypadku, gdy chociaż jeden z etapów zakończy się wynikiem negatywnym, wniosek zostaje odrzucony. Informacja o odrzuceniu wniosku jest przesyłana drogą mailową na adres wskazany przez ministra właściwego do spraw informatyzacji.

4.2.3 Okres oczekiwania na przetworzenie wniosku

Narodowe Centrum Certyfikacji wystawia certyfikat dostawcy usług zaufania niezwłocznie, nie później niż w terminie 3 dni roboczych od dnia otrzymania poprawnego wniosku od ministra właściwego do spraw informatyzacji i poprawnego żądania certyfikacyjnego.

Decyzje o unieważnieniu certyfikatu dostawcy usług zaufania Narodowe Centrum Certyfikacji realizuje w ciągu 1 godziny od momentu otrzymania od ministra właściwego do spraw gospodarki poprawnego wniosku.

4.3 Wydanie certyfikatu

4.3.1 Czynności wykonywane podczas wydawania certyfikatu

Procedura wydawania certyfikatu dostawcy usług zaufania przebiega następująco:

1. Operator Systemu sprawdza czy Subskrybent, dla którego wydawany będzie certyfikat, jest zarejestrowany w bazie danych Narodowego Centrum Certyfikacji i w razie potrzeby dokonuje rejestracji.
2. Operator Systemu wczytuje przekazane przez Subskrybenta żądanie certyfikacyjne i zatwierdza jego realizację.

3. Po wygenerowaniu certyfikatu dostawcy usług zaufania, przekazuje ten certyfikat do Subskrybenta w celu jego weryfikacji.
4. Po otrzymaniu od Subskrybenta potwierdzenia poprawności certyfikatu dostawcy usług zaufania (Subskrybent ma obowiązek przesłać informację o poprawności wydanego certyfikatu lub zauważonych błędach najpóźniej w następnym dniu roboczym do godziny 12:00) publikuje certyfikat w Repozytorium, aktualizuje Zaufaną listę, a także informuje o wydaniu certyfikatu ministra właściwego do spraw informatyzacji oraz kwalifikowanych dostawców usług zaufania.

4.3.2 Informowanie Subskrybenta o wydaniu certyfikatu

Informacja o wydaniu nowego certyfikatu dostawcy usług zaufania jest przekazywana Subskrybentowi drogą mailową, a po potwierdzeniu przez Subskrybenta poprawności certyfikatu, jest on publikowany w Repozytorium i umieszczany na Zaufanej liście.

4.4 Akceptacja certyfikatu

4.4.1 Potwierdzenie akceptacji certyfikatu

Subskrybent zobowiązany jest do sprawdzenia poprawności wydanego certyfikatu dostawcy usług zaufania. Subskrybent ma obowiązek przesłać informację o poprawności wydanego certyfikatu lub zauważonych błędach najpóźniej w następnym dniu roboczym do godziny 12:00.

W przypadku zauważeniu błędów w wydanym certyfikacie dostawcy usług zaufania, Narodowe Centrum Certyfikacji powiadamia o tym fakcie ministra właściwego do spraw informatyzacji, a następnie unieważnia błędny certyfikat i wydaje nowy. W takiej sytuacji nie mają zastosowania zapisy rozdziału 4.9 dotyczące unieważniania certyfikatów.

4.4.2 Publikowanie certyfikatu przez Narodowe Centrum Certyfikacji

Po potwierdzeniu przez Subskrybenta poprawności certyfikatu, jest on publikowany w Repozytorium i umieszczany na Zaufanej liście.

4.4.3 Informowanie innych podmiotów o wydaniu certyfikatu

Podstawową metodą informowania innych podmiotów o wydaniu certyfikatu dostawcy usług zaufania jest jego publikacja w Repozytorium oraz umieszczenie na Zaufanej liście. Dodatkowo, informacja o wydaniu nowego certyfikatu dostawcy usług zaufania jest wysyłana drogą mailową do ministra właściwego do spraw informatyzacji oraz do kwalifikowanych dostawców usług zaufania.

4.5 Stosowanie kluczy kryptograficznych oraz certyfikatów

4.5.1 Stosowanie kluczy i certyfikatówprzez Subskrybentów

Patrz rozdziały 1.5 i 6.1.7.

4.5.2 Stosowanie certyfikatów przez stronę ufającą

Strona ufająca musi używać certyfikatów:

- zgodnie z treścią certyfikatu dostawcy usług zaufania (pola keyUsage oraz extendedKeyUsage),
- tylko po zweryfikowaniu ich statusu (patrz rozdział 4.9) oraz wiarygodności pieczęci elektronicznej złożonej przez Narodowe Centrum Certyfikacji.

4.6 Recertyfikacja

Nie dotyczy.

4.7 Odnowienie certyfikatu

Identycznie jak w przypadku wydania pierwszego certyfikatu dostawcy usług zaufania – patrz rozdziały 4.1 – 4.4.

4.8 Modyfikacja certyfikatu

Identycznie jak w przypadku wydania pierwszego certyfikatu dostawcy usług zaufania – patrz rozdziały 4.1 – 4.4.

4.9 Unieważnienie certyfikatu

Z zastrzeżeniem przypadku opisanego w punkcie 4.4.1, Narodowe Centrum Certyfikacji unieważnia certyfikat dostawcy usług zaufania jedynie na podstawie decyzji administracyjnej ministra właściwego do spraw informatyzacji. Żądanie unieważnienia certyfikatu dostawcy usług zaufania należy kierować bezpośrednio do ministra właściwego do spraw informatyzacji.

4.9.1 Okoliczności unieważnienia certyfikatu

Decyzję o unieważnieniu certyfikatu dostawcy usług zaufania podjąć może jedynie minister właściwy do spraw informatyzacji. Polityka nie określa okoliczności wydania tej decyzji.

4.9.2 Kto może żądać unieważnienia certyfikatu

Unieważnienia certyfikatu dostawcy usług zaufania może zażądać jedynie minister właściwy do spraw informatyzacji.

4.9.3 Procedura unieważniania certyfikatu

Po odebraniu decyzji o unieważnieniu certyfikatu dostawcy usług zaufania od ministra właściwego do spraw informatyzacji osoba pełniąca funkcję Operatora Systemu unieważnia certyfikat oraz publikuje w Repozytorium nową listę unieważnionych certyfikatów. Następnie modyfikowany jest Rejestr oraz Zaufana lista.

Po opublikowaniu listy unieważnionych certyfikatów Narodowe Centrum Certyfikacji przekazuje ministrowi właściwemu do spraw informatyzacji oraz Subskrybentom potwierdzenie dokonania unieważnienia.

Operacje związane z unieważnieniem certyfikatu dostawcy usług zaufania oraz wytworzeniem i publikacją aktualnej listy unieważnionych certyfikatów zapisywane są w rejestrze zdarzeń.

4.9.4 Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu

Narodowe Centrum Certyfikacji publikuje aktualną listę unieważnionych certyfikatów w ciągu 1 godziny od momentu otrzymania poprawnej decyzji o unieważnieniu certyfikatu dostawcy usług zaufania od ministra właściwego do spraw informatyzacji.

Lista unieważnionych certyfikatów zapewnia określenie czasu unieważnienia certyfikatu dostawcy usług zaufania z dokładnością do jednej sekundy. Czas ten jest zapisywany automatycznie przez oprogramowanie stosowane do unieważniania certyfikatów. Narodowe Centrum Certyfikacji zapewnia przyjmowanie i weryfikację pod względem formalnym wniosków o unieważnie certyfikatu dostawcy usług zaufania przez całą dobę.

4.9.5 Maksymalny dopuszczalny czas przetwarzania wniosku o unieważnienie

Narodowe Centrum Certyfikacji publikuje aktualną listę unieważnionych certyfikatów w ciągu 1 godziny od momentu otrzymania poprawnej decyzji o unieważnieniu certyfikatu dostawcy usług zaufania od ministra właściwego do spraw informatyzacji.

4.9.6 Obowiązek sprawdzania list unieważnionych certyfikatów przez stronę ufającą

Przed akceptacją pieczęci elektronicznej weryfikowanej z wykorzystaniem certyfikatu dostawcy usług zaufania wydanego przez Narodowe Centrum Certyfikacji Strona ufająca powinna sprawdzić, czy certyfikat dostawcy usług zaufania nie znajduje się na liście unieważnionych certyfikatów publikowanej pod na stronie internetowej www.nccert.pl.

Należy jednak zwrócić uwagę, że publikacja listy unieważnionych certyfikatów, podobnie jak listy unieważnionych i zawieszonych certyfikatów publikowanej przez Subskrybenta, następuje później niż unieważnienie certyfikatu dostawcy usług zaufania. Narodowe Centrum Certyfikacji gwarantuje, że czas od odebrania decyzji o unieważnieniu certyfikatu do publikacji listy nie przekroczy 1 godziny.

4.9.7 Częstotliwość publikowania list unieważnionych certyfikatów

Aktualne listy unieważnionych certyfikatów publikowane są w następujących sytuacjach:

- niezwłocznie po dokonaniu unieważnienia, w terminie do 1 godziny od otrzymania od ministra właściwego do spraw informatyzacji decyzji o unieważnieniu certyfikatu dostawcy usług zaufania;
- co najmniej raz dziennie (z wyłączeniem sobót, niedziel oraz wszystkich dni ustawowo wolnych od pracy) .

4.9.8 Maksymalne opóźnienie w publikowaniu list unieważnionych certyfikatów

Narodowe Centrum Certyfikacji publikuje aktualną listę unieważnionych certyfikatów bez zbędnej zwłoki natychmiast po jej wytworzeniu.

4.9.9 Dostępność usługi OCSP

Narodowe Centrum Certyfikacji nie udostępnia usługi weryfikacji statusu certyfikatu w trybie on-line.

4.9.10 Obowiązek sprawdzania unieważnień w trybie on-line

Nie dotyczy.

4.9.11 Inne dostępne formy ogłaszania unieważnień certyfikatów

Informacja o unieważnieniu certyfikatu dostawcy usług zaufania jest umieszczana Rejestrze, a także na zaufanej liście.

4.9.12 Specjalne obowiązki w przypadku naruszenia ochrony klucza

W przypadku naruszenia bezpieczeństwa lub podejrzenia naruszenia bezpieczeństwa danych służących do składania pieczęci elektronicznej Subskrybent zobowiązany jest do niezwłocznego powiadomienia o zdarzeniu ministra właściwego do spraw informatyzacji.

W przypadku naruszenia bezpieczeństwa lub podejrzenia naruszenia bezpieczeństwa danych do składania pieczęci elektronicznej przez Narodowe Centrum Certyfikacji, NBP zobowiązany jest do niezwłocznego powiadomienia o zdarzeniu ministra właściwego do spraw informatyzacji.

4.10 Usługi weryfikacji statusu certyfikatu

4.10.1 Charakterystyki operacyjne

Informację o statusie certyfikatów wydanych przez Narodowe Centrum Certyfikacji można uzyskać w oparciu o listy unieważnionych certyfikatów publikowane na stronie internetowej www.nccert.pl .

4.10.2 Dostępność usługi

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

4.10.3 Cechy opcjonalne

Nie dotyczy.

4.11 Zakończenie subskrypcji

Zakończenie przez Subskrybenta korzystania z usług zaufania świadczonych przez Narodowe Centrum Certyfikacji jest równoznaczne z zaprzestaniem działalności jako kwalifikowany dostawca usług zaufania.

4.12 Deponowanie i odtwarzanie klucza

Nie dotyczy.

5. Zabezpieczenia techniczne, organizacyjne i operacyjne

W niniejszym rozdziale zawarto najważniejsze informacje dotyczące zabezpieczeń fizycznych, organizacyjnych oraz operacyjnych stosowanych w NBP w związku z realizacją zadań powierzonych przez ministra właściwego do spraw informatyzacji.

5.1 Zabezpieczenia fizyczne

5.1.1 Lokalizacja i budynki

Narodowe Centrum Certyfikacji jest zlokalizowane w dwóch różnych ośrodkach obliczeniowych znajdujących się w oddalonych od siebie obiektach NBP, zabezpieczonych systemami ochrony fizycznej zgodnie z przepisami obowiązującymi w NBP. Ośrodek zapasowy, zapewniający możliwość pełnego odtworzenia funkcjonalności systemu z ośrodka podstawowego oraz przechowywanie kopii zapasowych i archiwalnych, jest dostępny dla upoważnionych osób w trybie: 24 godziny na dobę, 7 dni w tygodniu.

5.1.2 Dostęp fizyczny

Zapewnia się kontrolę dostępu do pomieszczeń, w których zlokalizowane jest Narodowe Centrum Certyfikacji. Dostęp do elementów systemu mają wyłącznie osoby uprawnione. Dopuszcza się pracę w systemie osób niebędących pracownikami NBP, w związku z realizacją zadań określonych w umowach, zawartych przez NBP. Umowy te zawierają zapisy zapewniające właściwy poziom bezpieczeństwa wykonywanych prac serwisowych i konserwacyjnych, które są wykonywane wyłącznie pod nadzorem osób pełniących role w Narodowym Centrum Certyfikacji.

5.1.3 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.

5.1.4 Zagrożenie powodziowe

Krytyczne elementy Narodowego Centrum Certyfikacji, są rozmieszczone w pomieszczeniach o małym ryzyku zalania, w tym w wyniku uszkodzenia instalacji budynku. W przypadku wystąpienia zagrożenia zalaniem, postępuje się zgodnie z procedurami obowiązującymi w NBP oraz uruchamia się procedury zapewnienia ciągłości działania Narodowego Centrum Certyfikacji.

5.1.5 Ochrona przeciwpożarowa

Pomieszczenia zajmowane przez Narodowe Centrum Certyfikacji są chronione przez automatyczną instalację przeciwpożarową. W przypadku wystąpienia zagrożenia pożarowego postępuje się zgodnie z procedurami obowiązującymi w NBP oraz uruchamia się procedury zapewnienia ciągłości działania Narodowego Centrum Certyfikacji.

5.1.6 Nośniki informacji

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

Dostęp do nośników informacji jest ograniczony, a nośniki przechowywane są w nadzorowanych pomieszczeniach. Dane wprowadzane do systemu z zewnętrznych elektronicznych nośników informacji są, przed ich wprowadzaniem do systemu, badane na obecność wirusów komputerowych lub innego złośliwego oprogramowania.

5.1.7 Niszczenie zbędnych nośników informacji

Zbędne dokumenty papierowe, dokumenty w formie elektronicznej oraz inne nośniki informacji używane w Narodowym Centrum Certyfikacji są niszczone w bezpieczny sposób, zgodnie z procedurami obowiązującymi w NBP.

5.1.8 Przechowywanie kopii bezpieczeństwa

Kopie bezpieczeństwa są przechowywane w zamkniętych pomieszczeniach w różnych lokalizacjach. Ośrodek zapasowy, zapewniający możliwość pełnego odtworzenia funkcjonalności systemu z ośrodka podstawowego, jest dostępny dla upoważnionych osób w trybie: 24 godziny na dobę, 7 dni w tygodniu. Ośrodek zapasowy jest chroniony przy zastosowaniu analogicznych środków, jak ośrodek podstawowy.

5.2 Zabezpieczenia organizacyjne

5.2.1 Zaufane role

W Narodowym Centrum Certyfikacji funkcjonują następujące role:

1. **Inspektor Bezpieczeństwa Systemu**, który nadzoruje wdrożenie i stosowanie wszystkich procedur bezpiecznej eksploatacji systemu teleinformatycznego Narodowego Centrum Certyfikacji;
2. **Administrator Systemu**, który instaluje, konfiguruje i zarządza systemem teleinformatycznym oraz odtwarza dane z kopii zapasowej;
3. **Operator Systemu** wykonujący codzienną obsługę systemu, w tym wykonuje kopie zapasowe;

4. **Inspektor ds. Audytu** analizujący zapisy rejestrów zdarzeń mających miejsce w Narodowym Centrum Certyfikacji;.

5.2.2 Lista osób wymaganych podczas realizacji zadania

Zgodnie z procedurami Narodowego Centrum Certyfikacji część zadań wymaga obecności więcej niż jednego pracownika NBP pełniącego rolę w Narodowym Centrum Certyfikacji.

Lp.	Nazwa zadania	Lista osób wymaganych
1.	Uruchomienie systemu	Operator Systemu, Administrator Systemu, IBS
2.	Wczytanie danych do składania pieczęci elektronicznych	dwóch Operatorów Systemu, IBS
3.	Wystawienie certyfikatu dostawcy usług zaufania	dwóch Operatorów Systemu
4.	Unieważnienie certyfikatu dostawcy usług zaufania	dwóch Operatorów Systemu
5.	Odtworzenie kopii zapasowej systemu	Operator Systemu, Administrator Systemu, IBS
6.	Zamknięcie systemu	Operator Systemu, IBS
7.	Wykonanie kopii zapasowej	Operator Systemu, IBS
8.	Wygenerowanie danych do składania pieczęci elektronicznej	Dwóch Operatorów Systemu, IBS

5.2.3 Identyfikacja oraz uwierzytelnianie każdej roli

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

1. kontrolę i ograniczenie dostępu do poszczególnych pomieszczeń zajmowanych przez Narodowe Centrum Certyfikacji;
2. przydział indywidualnych imiennych kont w systemie i określony zakres uprawnień uzasadniony zakresem wykonywanych obowiązków;
3. zastosowanie kart elektronicznych do uaktywniania elementów systemu.

5.2.4 Role, które nie mogą być łączone

Żadne role w Narodowym Centrum Certyfikacji nie mogą być łączone.

5.3 Nadzorowanie personelu

5.3.1 Kwalifikacje, doświadczenie oraz upoważnienia

NBP gwarantuje, że pracownicy NBP wykonujący zadania w ramach Narodowego Centrum Certyfikacji:

1. posiadają pełną zdolność do czynności prawnych;
2. posiadają niezbędną wiedzę i umiejętności w zakresie technologii tworzenia certyfikatów i świadczenia innych usług związanych z podpisem elektronicznym

i pieczęcią elektroniczną, sprzętu i oprogramowania stosowanego do elektronicznego przetwarzania danych oraz automatycznego przetwarzania danych w sieciach i systemach teleinformatycznych;
3. posiadają dostęp do dokumentacji w zakresie uzasadnionym zajmowanym stanowiskiem oraz powierzonymi obowiązkami, w tym do niezbędnych procedur, polityk i regulaminów.

5.3.2 Procedury weryfikacji przygotowania

Osoby pełniące role w Narodowym Centrum Certyfikacji są dobierane zgodnie z kwalifikacjami oraz na zasadach zatrudniania obowiązujących w NBP.

5.3.3 Szkolenie

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

1. technologii tworzenia certyfikatów i świadczenia innych usług związanych z podpisem elektronicznym i pieczęcią elektroniczną;
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.

5.3.4 Częstotliwość powtarzania szkoleń oraz wymagania

Szkolenia obejmują zakres wiedzy wymagany na danym stanowisku pracy. Osoby pełniące role w Narodowym Centrum Certyfikacji przechodzą szkolenia udoskonalające, zgodnie z zasadami szkoleń obowiązującymi w NBP. W przypadku zmiany w funkcjonowaniu Narodowego Centrum Certyfikacji, pracownicy NBP przechodzić będą szkolenia dodatkowe.

5.3.5 Częstotliwość rotacji stanowisk i jej kolejność

Nie dotyczy.

5.3.6 Sankcje z tytułu nieuprawnionych działań

Wszystkie czynności wykonywane w ramach obowiązków związanych z funkcjonowaniem Narodowego Centrum Certyfikacji są dokumentowane i nadzorowane. Umożliwia to w szczególności wykrycie ewentualnych nieuprawnionych działań osób pełniących role w Narodowym Centrum Certyfikacji.

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

5.3.7 Pracownicy kontraktowi

Nie dotyczy.

5.3.8 Dokumentacja przekazana pracownikom

Osoby pełniące role w Narodowym Centrum Certyfikacji otrzymują opis obowiązków dotyczący zajmowanego stanowiska pracy wraz z niezbędnymi procedurami, na zasadach obowiązujących w NBP.

5.4 Procedury rejestrowania zdarzeń oraz audytu

W celu zapewnienia właściwego poziomu bezpieczeństwa funkcjonowania Narodowego Centrum Certyfikacji opracowano i wdrożono 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 role 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 wykorzystywanego systemu,
2. nieuprawnionych prób uzyskania dostępu do wykorzystywanych i przetwarzanych danych,
3. nieuprawnionych prób uzyskania dostępu do pomieszczeń Narodowego Centrum Certyfikacji,
4. prób zakłócenia działalności wykorzystywanego systemu,
5. prób uniemożliwienia realizacji zadań Narodowego Centrum Certyfikacji.

5.4.1 Typy rejestrowanych zdarzeń

Rejestry zdarzeń tworzone są w czasie bieżącej pracy Narodowego Centrum Certyfikacji. Rejestry zdarzeń zawierają zapisy dotyczące operacji wykonywanych w związku z realizacją zadań Narodowego Centrum Certyfikacji, 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, certyfikatami dostawcy usług zaufania oraz danymi służącymi do składania pieczęci elektronicznej przez Narodowe Centrum Certyfikacji, np. tworzenie kont użytkowników i rodzaj przydzielanych uprawnień,
3. instalacja 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, uruchamianie 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 certyfikatu dostawcy usług zaufania oraz wszystkie wiadomości z tym związane, a w szczególności wysłane i odebrane komunikaty przesyłane w relacjach ministra właściwego do spraw informatyzacji z NBP.

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.

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.

5.4.2 Częstotliwość przetwarzania zapisów rejestrowanych zdarzeń

Rejestry zdarzeń są przeglądane co najmniej raz dziennie (z wyłączeniem sobót, niedziel oraz wszystkich dni ustawowo wolnych od pracy). Zasady kontroli i analizy rejestrów zdarzeń określają procedury Narodowego Centrum Certyfikacji.

5.4.3 Okres przechowywania zapisów rejestrowanych zdarzeń

Rejestry zdarzeń są przechowywane przez minimum 3 lata w sposób umożliwiający elektroniczne ich przeszukiwanie. Po upływie okresu przechowywania rejestry zdarzeń są niszczone w bezpieczny sposób lub są przenoszone do archiwum zgodnie zaktualnie obowiązującymi przepisami prawa, normami i standardami.

5.4.4 Ochrona zapisów rejestrowanych zdarzeń

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

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 rozdziale 5.2.1 niniejszej Polityki. Czynności polegające na tworzeniu kopii zapasowych nadzoruje bezpośrednio Inspektor Bezpieczeństwa Systemu.

5.4.5 Procedury tworzenia kopii zapisów rejestrowanych zdarzeń

Kopie rejestrów zdarzeń są tworzone wraz z kopiami bezpieczeństwa systemu. Identyczne kopie rejestrów zdarzeń przechowywane są w dwóch różnych lokalizacjach. 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 rozdziale 5.2.1 niniejszej Polityki. Czynności polegające na tworzeniu kopii zapasowych nadzoruje bezpośrednio Inspektor Bezpieczeństwa Systemu.

5.4.6 System gromadzenia zapisów rejestrowanych zdarzeń (wewnętrzny a zewnętrzny)

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

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

Lp.	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
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 certyfikatów dostawcy usług zaufania.	automatyczny	Oprogramowanie
7.	Udane i nieudane operacje związane z publikacją certyfikatów dostawcy usług zaufania oraz informacji o unieważnieniach certyfikatów dostawcy usług zaufania.	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/ manualny	System operacyjny i personel
10.	Zmiany konfiguracji systemu.	manualny	Personel
11.	Uaktualnienia oprogramowania i zmiany w sprzęcie komputerowym.	manualny	Personel
12.	Czynności związane z serwisem systemu.	manualny	Personel
13.	Zmiany w personelu.	manualny	Personel

5.4.7 Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenie

Osoby pełniące role w Narodowym Centrum Certyfikacji powiadamiają Inspektora Bezpieczeństwa Systemu o wszystkich wydarzeniach mających wpływ na bezpieczeństwo systemu oraz wszystkich wydarzeniach wskazujących na możliwe naruszenie bezpieczeństwa. W przypadku wystąpienia incydentu, o którym mowa w art.19 eIDAS, informacja o wystąpieniu incydentu jest przekazywana do ministra właściwego do spraw informatyzacji.

5.4.8 Oszacowanie podatności na zagrożenia

Dokonuje się okresowej oceny poziomu ryzyka systemu, w celu identyfikacji zagrożeń, oszacowania prawdopodobieństwa ich wystąpienia oraz podatności na nie. Na podstawie

wyników analizy ryzyka wprowadzone zostają rozwiązania mające na celu eliminację lub zmniejszenie podatności systemu na zagrożenia.

5.5 Zapisy archiwalne

5.5.1 Rodzaje archiwizowanych danych

Narodowe Centrum Certyfikacji archiwizuje i przechowuje następujące informacje:

1. certyfikaty Narodowego Centrum Certyfikacji,
2. certyfikaty dostawców usług zaufania,
3. listy unieważnionych certyfikatów,
4. Zaufane listy,
5. Rejestr,
6. przyjęte żądania certyfikacji,
7. kopie bezpieczeństwa elementów systemu,
8. kopie bezpieczeństwa baz danych,
9. kopie korespondencji NBP prowadzonej w związku z funkcjonowaniem Narodowego Centrum Certyfikacji;
10. rejestry zdarzeń,
11. inne informacje publikowane przez Narodowe Centrum Certyfikacji.

5.5.2 Okres przechowywania archiwum

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.

NBP przechowuje wszystkie dokumenty oraz dane elektroniczne wymienione w rozdziale 5.5.1, z wyłączeniem rejestrów zdarzeń, przez okres 20 lat od chwili powstania danego dokumentu lub danych. W przypadku certyfikatów Narodowego Centrum Certyfikacji oraz certyfikatów dostawcy usług zaufania, okres 20 lat liczony jest od chwili wygaśnięcia danego certyfikatu.

5.5.3 Ochrona archiwum

Wszystkie dokumenty oraz dane elektroniczne bezpośrednio związane z realizacją zadań Narodowego Centrum Certyfikacji są przechowywane w sposób zapewniający bezpieczeństwo przechowywanych dokumentów oraz danych. W szczególności:

1. zasoby archiwalne zabezpieczone są środkami ochrony fizycznej;
2. dostęp do archiwum jest ograniczony jedynie do upoważnionych osób pełniących role w Narodowym Centrum Certyfikacji;

3. pomieszczenia archiwum są monitorowane.

5.5.4 Procedury tworzenia kopii archiwalnych

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.

5.5.5 Wymaganie znakowania czasem kopii archiwalnych

Znakowanie czasem zasobów archiwalnych nie jest wymagane.

5.5.6 Kopie archiwalne rejestrów zdarzeń (system wewnętrzny i zewnętrzny)

Kopie achiwalne są wykonywane ręcznie przez Operatorów Systemu i zapisywane na zewnętrznych nośnikach danych.

5.5.7 Procedury dostępu oraz weryfikacji zarchiwizowanej informacji

Informacje są udostępniane jedynie uprawnionym podmiotom. Informacje mogą być dodawane i usuwane do/z archiwum jedynie przez upoważnione osoby pełniące role w Narodowym Centrum Certyfikacji. W regularnych odstępach czasu sprawdzana jest możliwość odczytania informacji z archiwizowanych kopii bezpieczeństwa. W razie stwierdzenia problemów z odczytaniem danych archiwalnych zasobów są one odtwarzane na podstawie informacji istniejącej w systemie bądź kopii zasobów archiwalnych. Szczegółowy opis ww. czynności znajduje się w procedurach Narodowego Centrum Certyfikacji.

5.6 Zmiana klucza

Okresy ważności certyfikatów Narodowego Centrum Certyfikacji oraz certyfikatów dostawcy usług zaufania, wynoszą nie dłużej niż:

- 23 lata dla certyfikatu Narodowego Centrum Certyfikacji;
- 11 lat dla certyfikatu dostawcy usług zaufania.

Dane służące do składania pieczęci elektronicznej i dane służące do walidacji są ważne tak długo, jak długo ważny jest certyfikat Narodowego Centrum Certyfikacji lub certyfikat dostawcy usług zaufania powiązany z tymi danymi. Czas początku ważności certyfikatu

Narodowego Centrum Certyfikacji i certyfikatu dostawcy usług zaufania nie może być wcześniejszy niż moment ich wytworzenia.

Wymiana danych służących do składania pieczęci elektronicznej przez Narodowe Centrum Certyfikacji wymaga wytworzenia nowego certyfikatu Narodowego Centrum Certyfikacji. Ze względu na stopień skomplikowania operacji wymiany certyfikatu Narodowego Centrum Certyfikacji, sposób realizacji tej wymiany jest każdorazowo uzgadniany z ministrem właściwym do spraw informatyzacji oraz z Subskrybentami. Zależnie od decyzji możliwy jest jeden z następujących scenariuszy:

1. Wymiana danych do składania pieczęci elektronicznych odbywa się w ramach tego samego urzędu certyfikacji tzn. nie jest powiązana ze zmianą identyfikatora wyróżniającego zawartego w certyfikacie Narodowego Centrum Certyfikacji.
2. Wymiana danych do składania pieczęci elektronicznych jest powiązana z uruchomieniem w ramach Narodowego Centrum Certyfikacji nowego urzędu certyfikacji z nowym identyfikatorem wyróżniającym. W takim przypadku do czasu wygaśnięcia poprzedniego certyfikatu Narodowego Centrum Certyfikacji funkcjonują dwa urzędy certyfikacji z zastrzeżeniem, iż wszystkie nowe certyfikaty dostawcy usług zaufania wydawane są w ramach nowego urzędu. Urząd certyfikacji powiązany z poprzednim certyfikatem Narodowego Centrum Certyfikacji służy jedynie do publikacji list unieważnionych certyfikatów oraz ewentualnego unieważniania wydanych przez siebie certyfikatów dostawcy usług zaufania.

Zasady wymiany danych służących do składania pieczęci elektronicznych lub podpisów elektronicznych przez Subskrybenta określane są przez Subskrybenta.

5.7 Naruszenie ochrony klucza i uruchamianie po awariach oraz klęskach żywiołowych

Narodowe Centrum Certyfikacji posiada opracowane i przetestowane procedury, które:

1. obejmują informacje dotyczące ustawień oraz sposobu konfiguracji sprzętu oraz oprogramowania;
2. określają środki oraz szczegółowe procedury odtwarzania a także przewidywany czas ich wykonywania;
3. wskazują osoby odpowiedzialne za uruchomienie procedur mających ograniczyć skutki zdarzenia lub klęski żywiołowej, przywrócić wymagany poziom bezpieczeństwa systemu oraz właściwy poziom świadczonych usług;

4. identyfikują osoby odpowiedzialne za opracowanie i utrzymanie procedur, w tym odpowiedzialne za regularne przeprowadzanie testów opisanych w tych procedurach;
5. określają priorytety podejmowania poszczególnych działań.

NBP posiada ośrodek zapasowy zapewniający możliwość realizacji zadań Narodowego Centrum Certyfikacji w przypadku zakłócenia działalności ośrodka podstawowego. Procedury określają okoliczności i zasady uruchamiania systemu w ośrodku zapasowym.

5.7.1 Procedury obsługi incydentów i reagowania na nie

Zgodnie z obowiązującymi w NBP wewnętrznymi przepisami dotyczącymi obsługi incydentów oraz z odpowiednimi zapisami w umowach zawartych przez NBP z firmami zewnętrznymi świadczącymi usługi wsparcia i serwisu oprogramowania oraz sprzętu wykorzystywanego w Narodowym Centrum Certyfikacji.

W przypadku wystąpienia incydentu, o którym mowa w art.19.2 eIDAS, informacja o incydencie może być zgłaszana przez dostawcę na adres nccert@nccert.pl. Wszelkie informacje o wystąpieniu incydentu są przekazywane przez NBP do ministra właściwego do spraw informatyzacji.

5.7.2 Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych

Procedury Narodowego Centrum Certyfikacji obejmują postępowanie w przypadku awarii sprzętu, oprogramowania oraz uszkodzenia przetwarzanych i przechowywanych danych. Zawierają opis bazowej konfiguracji systemu, procedury instalacji i konfiguracji oraz procedury odtwarzania elementów systemu z kopii zapasowych. Określają także okoliczności, w jakich następuje uruchomienie systemu w ośrodku zapasowym.

5.7.3 Ujawnienie lub podejrzenie ujawnienia danych do składania pieczęci elektronicznej

Procedury Narodowego Centrum Certyfikacji obejmują postępowanie w przypadku naruszenia bezpieczeństwa danych służących do składania pieczęci elektronicznej, wykorzystywanych przez Narodowe Centrum Certyfikacji. Procedury określają sposób powiadamiania ministra właściwego do spraw informatyzacji oraz Subskrybentów.

5.7.4 Zapewnienie ciągłości działania po katastrofach

Procedury Narodowego Centrum Certyfikacji obejmują działania konieczne do przywrócenia odpowiedniego poziomu bezpieczeństwa oraz właściwego poziomu świadczenia usług zaufania, w przypadku wystąpienia klęski żywiołowej, ataku terrorystycznego, aktu sabotażu lub wystąpienia innych zagrożeń mogących naruszyć ciągłość działania Narodowego Centrum Certyfikacji.

5.8 Zakończenie działalności Narodowego Centrum Certyfikacji

1. W przypadku:

1) zamiaru zaprzestania pełnienia roli podmiotu upoważnionego, albo
2) niemożności pełnienia roli podmiotu upoważnionego, albo
3) poinformowania NBP przez ministra właściwego do spraw informatyzacji o zamiarze cofnięcia upoważnienia, o którym mowa w art. 11 ust. 1 ustawy o usługach zaufania

- NBP zobowiązuje się do zapewnienia ciągłości pełnienia roli podmiotu upoważnionego, do czasu wyłonienia przez ministra właściwego do spraw informatyzacji nowego podmiotu, który przejąłby jego obowiązki.

2. NBP zapewnia ciągłość pełnienie roli podmiotu upoważnionego nie dłużej niż:

1) 6 miesięcy od dnia poinformowania ministra właściwego do spraw informatyzacji o okolicznościach, o których mowa w pkt 1 i 2 powyżej;
2) 4 miesięcy od dnia poinformowania NBP o okoliczności, o której mowa w pkt 3 powyżej.

3. W przypadku cofnięcia przez ministra właściwego do spraw informatyzacji upoważnienia, o którym mowa w art. 11 ust. 1 ustawy o usługach zaufania, NBP zaprzestaje pełnienia roli podmiotu upoważnionego ze skutkiem natychmiastowym.

4. NBP, w przypadku zaprzestania pełnienia roli podmiotu upoważnionego, zobowiązuje się do umożliwienia przejęcia i kontynuacji pełnienia tej roli przez inny podmiot, w tym ministra właściwego do spraw informatyzacji, oraz przekazania podmiotowi przejmującemu pełnienie tej roli – na żądanie ministra właściwego do spraw informatyzacji – wszelkich informacji i danych, które umożliwią wykonywanie tej roli przez nowy podmiot.

6 Procedury bezpieczeństwa technicznego

6.1 Generowanie danych do składania i walidacji pieczęci elektronicznej i ich instalowanie

6.1.1 Generowanie danych do składania i walidacji pieczęci elektronicznej

Dane do składania i walidacji pieczęci elektronicznej Narodowego Centrum Certyfikacji generowane są bezpośrednio w module kryptograficznym będącym urządzeniem do składania pieczęci elektronicznej, a następnie zapisywane są (w postaci sekretu współdzielonego) na kartach elektronicznych. Generowanie odbywa się w ośrodku podstawowym, w pomieszczeniach Narodowego Centrum Certyfikacji w obecności przynajmniej dwóch Operatorów Systemu oraz Inspektora Bezpieczeństwa Systemu. Po wygenerowaniu danych, karty elektroniczne przeznaczone do ośrodka zapasowego są do niego przewożone.

6.1.2 Przekazywanie danych do składania podpisu elektronicznego lub pieczęci elektronicznej Subskrybentowi

Nie dotyczy. Dane do składania podpisu elektronicznego lub pieczęci elektronicznej Subskrybenta są generowane przez Subskrybenta.

6.1.3 Dostarczanie danych do walidacji do Narodowego Centrum Certyfikacji

Subskrybent przekazuje Narodowemu Centrum Certyfikacji dane służące do walidacji za pośrednictwem ministra właściwego do spraw informatyzacji, w postaci żądania certyfikacji.

6.1.4 Przekazywanie danych do walidacji pieczęci elektronicznej Narodowego Centrum Certyfikacji

Dane służące do walidacji pieczęci elektronicznej Narodowego Centrum Certyfikacji wydawane są Subskrybentowi w formie certyfikatu Narodowego Centrum Certyfikacji. Certyfikat Narodowego Centrum Certyfikacji jest także publikowany w Repozytorium.

6.1.5 Długości danych do składania i walidacji podpisu elektronicznego lub pieczęci elektronicznej

Dane do składania i walidacji pieczęci elektronicznej Narodowego Centrum Certyfikacji, mają długość 4096 bitów (w przypadku certyfikatu wystawionego w 2016 r.) lub 2048 bitów (w przypadku certyfikatu wystawionego w 2009 r.).

Dane do składania i walidacji podpisu elektronicznego lub pieczęci elektronicznej Subskrybenta mają długość 4096 bitów (w przypadku certyfikatów wystawianych od dnia 9 grudnia 2016 r.) lub 2048 bitów (w przypadku certyfikatów wystawianych do dnia 9 grudnia 2009 r.).

6.1.6 Parametry generowania danych do składania i walidacji pieczęci elektronicznej oraz weryfikacja jakości

O ile przepisy prawa nie stanowią inaczej, wygenerowane dane do składania i walidacji pieczęci elektronicznej muszą spełniać minimalne wymagania określone w dokumencie ETSI TS 119 312 „Electronic Signatures and Infrastructures; Cryptographic Suites".

Odpowiednia jakość danych do składania i walidacji pieczęci elektronicznej zapewniona jest przez urządzenie do składania pieczęci elektronicznej wykorzystywane przez Narodowe Centrum Certyfikacji. Po wygenerowaniu Narodowe Centrum Certyfikacji weryfikuje długość oraz algorytm wygenerowanych danych.

6.1.7 Akceptowane zastosowanie danych do składania podpisu elektronicznego lub pieczęci elektronicznej

Zakres zastosowania danych do składania pieczęci elektronicznej przez Narodowe Centrum Certyfikacji określony jest przez dwa atrybuty certyfikatu Narodowego Centrum Certyfikacji: keyUsage oraz basicConstraints. Dopuszcza się wykorzystanie tych danych jedynie do:

1. opatrywania pieczęcią elektroniczną wydawanych certyfikatów dostawcy usług zaufania,
2. opatrywania pieczęcią elektroniczną list unieważnionych certyfikatów.

Zakres zastosowania danych do składania podpisu elektronicznego lub pieczęci elektronicznej przez Subskrybenta określony jest przez trzy atrybuty certyfikatu dostawcy usług zaufania: keyUsage, extKeyUsage oraz basicConstraints. Dopuszcza się wykorzystanie tych danych jedynie do opatrywania podpisem elektronicznym lub pieczęcią elektroniczną:

1. certyfikatów kwalifikowanych, o których mowa w załączniku I lit. g eIDAS, załączniku III lit. g eIDAS, załączniku IV lit. h eIDAS;
2. informacji o statusie certyfikatów kwalifikowanych, w tym listy zawieszonych lub unieważnionych certyfikatów;
3. innych certyfikatów związanych ze świadczeniem kwalifikowanych usług zaufania.

Wykorzystanie danych służących do do składania podpisu elektronicznego lub pieczęci elektronicznej przez Subskrybenta musi być zgodne z polityką certyfikacji wyspecyfikowaną Rejestrze.

6.2 Ochrona danych do składania pieczęci elektronicznej oraz nadzorowanie mechanizmów modułu kryptograficznego

Dane do składania pieczęci elektronicznej przez Narodowe Centrum Certyfikacji, tworzone są bezpośrednio w modułach kryptograficznych, a następnie zapisywane są (w postaci

sekretu współdzielonego) na kartach elektronicznych. Generowanie odbywa się w ośrodku podstawowym, w pomieszczeniach Narodowego Centrum Certyfikacji w obecności przynajmniej dwóch Operatorów Systemu oraz Inspektora Bezpieczeństwa Systemu. Moduły kryptograficzne nie opuszczają pomieszczeń Narodowego Centrum Certyfikacji i znajdują się w pomieszczeniach zabezpieczonych systemem alarmowym. Karty elektroniczne zawierające sekret współdzielony zabezpieczone są kodami PIN i są przechowywane w sposób zabezpieczający przed nieupoważnionym dostępem.

6.2.1 Standardy modułów kryptograficznych

Moduły kryptograficzne wykorzystywane w Narodowym Centrum Certyfikacji są zgodne z wymaganiami normy FIPS 140-2 Level 3.

6.2.2 Podział danych do składania pieczęci elektronicznej na części

Dane do składania pieczęci elektronicznej w przypadku eksportu poza urządzenie do składania pieczęci elektronicznej przenoszone są w postaci sekretu współdzielonego. Utworzonych jest dziewięć kart elektronicznych zawierających sekret współdzielony, a odtworzenie danych do składania pieczęci elektronicznej wymaga użycia dwóch kart.

6.2.3 Deponowanie danych do składania pieczęci elektronicznej

Dane do składania pieczęci elektronicznej nie są składowane ani deponowane, z wyjątkiem sytuacji o której mowa w punkcie 6.2.2.

6.2.4 Kopie zapasowe danych do składania pieczęci elektronicznej

Dane do składania pieczęci elektronicznej występują jedynie w urządzeniach do składania pieczęci elektronicznej znajdujących się w ośrodku podstawowym i zapasowym oraz na kartach elektronicznych, o których mowa w punkcie 6.2.2. Nie tworzy się dodatkowych kopii zapasowych danych do składania pieczęci elektronicznej.

6.2.5 Archiwizowanie danych do składania pieczęci elektronicznej

Dane do składania pieczęci elektronicznej nie są archiwizowane. Po upływie okresu ważności certyfikatu Narodowego Centrum Certyfikacji powiązanego z tymi danymi, są one niszczone zgodnie z procedurami obowiązującymi w NBP.

6.2.6 Wprowadzenie lub pobieranie danych do składania pieczęci elektronicznej do/z modułu kryptograficznego

W przypadku zaistnienia takiej potrzeby, dane do składania pieczęci elektronicznej są wprowadzane do modułu kryptograficznego za pomocą kart elektronicznych, o których mowa w punkcie 6.2.2. Wprowadzenie tych danych odbywa się w obecności przynajmniej dwóch Operatorów Sytemu oraz Inspektora Bezpieczeństwa Systemu.

Dane do składnia pieczęci elektronicznej są pobierane z modułu kryptograficznego jedynie w dwóch przypadkach:

1. bezpośrednio po ich wygenerowaniu w celu zapisania na kartach elektronicznych oraz przeniesienia do ośrodka zapasowego;
2. gdy zachodzi konieczność utworzenia nowego kompletu kart elektronicznych, o których mowa w punkcie 6.2.2 tzn. w przypadku uszkodzenia kart elektronicznych wchodzących w skład kompletu utworzonego w momencie generowania danych do składania pieczęci elektronicznych. Po wygenerowaniu nowego kompletu kart elektronicznych, poprzedni komplet jest niszczony.

6.2.7 Przechowywanie danych do składania pieczęci elektronicznej w module kryptograficznym

Dane do składania pieczęci elektronicznej są przechowywane są w module kryptograficznym w formie jawnej. Nie są one jednak dostępne dla nieuprawnionych osób.

6.2.8 Metoda aktywacji danych do składania pieczęci elektronicznej

Dane do składania pieczęci elektronicznej można aktywować dopiero po ich wprowadzeniu do modułu kryptograficznego. Aktywacja danych wymaga podania hasła dostępowego do tego modułu.

6.2.9 Metoda dezaktywacji danych do składania pieczęci elektronicznej

Dane do składania pieczęci elektronicznej mogą być dezaktywowane poprzez ich usunięcie z modułu kryptograficznego lub poprzez zatrzymanie aplikacji korzystającej z tych danych.

6.2.10 Metoda niszczenia danych do składania pieczęci elektronicznej

Dane do składania pieczęci elektronicznej zapisane w module kryptograficznym są niszczone poprzez ich usunięcie z tego modułu za pomocą oprogramowania do zarządzania tym modułem.

Niszczenie danych do składania pieczęci elektronicznej zapisanych na kartach elektronicznych (w postaci sekretu współdzielonego) polega na fizycznym zniszczeniu tych kart elektronicznych.

6.2.11 Ocena modułu kryptograficznego

Patrz pkt 6.2.1

6.3 Inne aspekty zarządzania danymi do składania pieczęci elektronicznej

6.3.1 Archiwizowanie danych do walidacji pieczęci elektronicznej

Dane do walidacji pieczęci elektronicznej Narodowego Centrum Certyfikacji oraz Subskrybenta są archiwizowane i przechowywane przez okres co najmniej 20 lat od momentu upłynięcia okresu ich ważności.

6.3.2 Okresy stosowania danych do składania i weryfikacji pieczęci elektronicznej

Długość okresu ważności danych do składania pieczęci elektronicznej i danych służących do walidacji pieczęci elektronicznej jest równa okresowi ważności certyfikatu powiązanemu z tymi danymi, okeślonemu w rozdziale 5.6

6.4 Dane aktywujące

Dane aktywujące stosowane są do uaktywniania danych do składania pieczęci elektronicznej przez Narodowe Centrum Ceryfikacji oraz do uaktywniania danych do składania podpisu elektronicznego przez Operatorów Systemu.

W skład danych aktywujących dane do składania pieczęci elektronicznej wchodzą, zapisane na kartach elektronicznych, elementy sekretu współdzielonego, które po wczytaniu umożliwiają odtworzenie danych do składania pieczęci elektronicznej oraz kody PINy zabezpieczające te karty elektroniczne.

Dane aktywujące dane do składania podpisu elektronicznego przez Operatora Systemu mają postać kodu PIN zabezpieczającego kartę elektroniczną Operatora.

6.4.1 Generowanie danych aktywujących i ich instalowanie

Dane aktywujące w postaci elementów sekretu współdzielonego zapisanych na kartach elektronicznych generowane są w sposób opisany w punkcie 6.1.1.

Dane aktywujące w postaci kodów PIN są ustalane przez Operatorów Systemu.

6.4.2 Ochrona danych aktywujących

Dane aktywujące dane do składania pieczęci elektronicznej podlegają szczególnej ochronie. Karty elektroniczne zawierające elementy sekretu współdzielonego są przechowywane w Narodowym Centrum Certyfikacji w sposób zapewniający odpowiedni poziom bezpieczeństwa, pod nadzorem Inspektora Bezpieczeństwa Systemu. Kody PIN do tych kart są znane jedynie ich właścicielom. Dodatkowo, opracowane są procedury udostępniania w sytuacjach awaryjnych kodów PIN do kart innym upoważnionym osobom.

6.4.3 Inne problemy związane z danymi aktywującymi

Nie dotyczy.

6.5 Nadzorowanie bezpieczeństwa systemu komputerowego

6.5.1 Wymagania techniczne dotyczące specyficznych zabezpieczeń systemów komputerowych

Elementy Narodowego Centrum Certyfikacji zabezpieczone są w następujący sposób:

1. fizyczne odseparowanie elementów systemu od innych systemów informatycznych,
2. kontrola dostępu zarówno w zakresie dostępu do pomieszczeń jak i poszczególnych elementów systemu (np. imienne konta w systemie operacyjnym i aplikacjach),
3. prowadzenie audytu zabezpieczeń,
4. separacja ról w systemie operacyjnym i w aplikacjach,
5. identyfikacja i uwierzytelnianie ról,
6. kryptograficzna ochrona komunikacji pomiędzy poszczególnymi elementami systemu,
7. mechanizm odtwarzania danych do składania pieczęci elektronicznej,
8. wykonywanie kopii zapasowych i archiwalnych,
9. utrzymywanie ośrodka zapasowego gotowego na przejęcie pracy w dowolnym momencie,
10. monitorowanie i alarmowanie w przypadku nieautoryzowanego dostępu do systemu teleinformatycznego.

6.5.2 Ocena bezpieczeństwa systemów komputerowych

Narodowe Centrum Certyfikacji wykorzystuje system informatyczny zapewniający poziom bezpieczeństwa wymagany przepisami o usługach zaufania i wewnętrznymi regulacjami NBP.

6.6 Cykl życia zabezpieczeń technicznych

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

6.6.1 Nadzorowanie rozwoju systemu

Rozwój aplikacji odbywa się w wydzielonym środowisku testowym, przy zastosowaniu odpowiednich środków kontroli jakości. Praca nad rozwojem aplikacji odbywa się w wydzielonym środowisku testowym.

6.6.2 Nadzorowanie zarządzania bezpieczeństwem

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

6.6.3 Nadzorowanie cyklu życia zabezpieczeń

Niniejsza Polityka nie określa żadnych wymagań w tym zakresie.

6.7 Nadzorowanie zabezpieczeń sieci komputerowej

Elementy Narodowego Centrum Certyfikacji nie są dołączone do sieci zewnętrznej. Komunikacja ze światem zewnętrznym odbywa się za pomocą nośników danych.

6.8 Znakowanie czasem

Nie dotyczy.

7. Profile certyfikatów oraz list CRL

Patrz załączniki C i D.

8. Audyt zgodności i inne oceny

8.1 Częstotliwość i okoliczności oceny

Narodowe Centrum Certyfikacji podlega kontroli zgodności funkcjonowania z przepisami ustawy o usługach zaufania. Kontrola zgodności dokonywana jest w miarę bieżących potrzeb lub w przypadku dokonywania znaczących zmian w Narodowym Centrum Certyfikacji

Dodatkowo, funkcjonowanie Narodowego Centrum Certyfikacji w ramach NBP może podlegać audytom wewnętrznym i kontrolom wewnętrznym zgodnie z przepisami obowiązującymi w NBP.

8.2 Tożsamość i kwalifikacje audytora

Osoby wykonujące kontrole zgodności powinny posiadać wystarczającą wiedzę i kwalifikacje, aby dokonać wiarygodnej oceny badanego zagadnienia.

8.3 Związek audytora z audytowaną jednostką

Kontroli zgodności nie mogą dokonywać pracownicy bezpośrednio związani z funkcjonowaniem Narodowego Centrum Certyfikacji.

8.4 Zagadnienia objęte audytem

Termin i zakres kontroli zgodności określany jest przez dyrektora Departamentu Bezpieczeństwa.

8.5 Działania podejmowane w celu usunięcia usterek wykrytych podczas audytu

Wyniki kontroli zgodności przekazywane są Prezesowi NBP. W przypadku stwierdzenia przez kontrolerów nieprawidłowości, dyrektor Departamentu Bezpieczeństwa podejmuje niezwłocznie działania mające na celu realizację zaleceń pokontrolnych.

8.6 Informowanie o wynikach audytu

Wybrane fragmenty raportu z kontroli mogą, za zgodą ministra właściwego do spraw informatyzacji, zostać opublikowane w Repozytorium.

9. Inne kwestie biznesowe i prawne

9.1 Opłaty

Narodowe Centrum Certyfikacji nieodpłatnie:

1. wytwarza, wydaje i publikuje certyfikaty dostawcy usług zaufania;
2. umożliwia dostęp do danych umieszczonych w Repozytorium;
3. umożliwia pobieranie certyfikatów dostawcy usług zaufania;
4. publikuje informacje o unieważnieniu certyfikatu dostawcy usług zaufania;
5. umożliwia dostęp do list unieważnionych certyfikatów dostawcy usług zaufania umieszczonych w Repozytorium;
6. umożliwia dostęp do Zaufanej listy umieszczonej w Repozytorium.

Dokument „Polityka Certyfikacji Narodowego Centrum Certyfikacji" jest dostępny nieodpłatnie na stronie internetowej Narodowego Centrum Certyfikacji wyłącznie w wersji elektronicznej.

9.2 Odpowiedzialność finansowa

Nie dotyczy.

9.3 Poufność informacji biznesowej

NBP stosuje przepisy ustawy o usługach zaufania oraz ustawy o ochronie danych osobowych, w odniesieniu do informacji gromadzonych w związku z funkcjonowaniem Narodowego Centrum Certyfikacji.

9.3.1 Zakres poufności informacji

Informacje związane z funkcjonowaniem Narodowego Centrum Certyfikacji, których nieuprawnione ujawnienie mogłoby narazić na szkodę NBP, Narodowe Centrum Certyfikacji, subskrybenta lub stronę ufającą są objęte tajemnicą. W szczególności tajemnicą są objęte dane służące do składania pieczęci elektronicznej przez Narodowe Centrum Certyfikacji.

Tajemnicą nie są objęte informacje o naruszeniu przepisów o usługach zaufania przez subskrybenta oraz informacje o naruszeniach bezpieczeństwa i utracie integralności, o których mowa w art. 19 ust. 2 eIDAS.

Obowiązek zachowania tajemnicy, o której mowa w art. 15 ust. 1 ustawy o usługach zaufania, trwa przez 10 lat od ustania stosunku prawnego, o którym mowa w art. 15 ust. 3 tej ustawy. Obowiązek zachowania tajemnicy danych służących do składania pieczęci elektronicznej przez Narodowe Centrum Certyfikacji jest bezterminowy.

9.3.2 Informacje znajdujące się poza zakresem poufności informacji

Do informacji publicznie dostępnych zaliczane są w szczególności:

1) certyfikaty Narodowego Centrum Certyfikacji;
2) wydane certyfikaty dostawców usług zaufania;
3) listy wydanych certyfikatów dostawcy usług zaufania;
4) listy unieważnionych certyfikatów;
5) Zaufana lista;
6) Rejestr;
7) Polityka;
8) informacje o proponowanych zmianach w Polityce;
9) ogłoszenia dotyczące bieżącej działalności.

9.3.3 Obowiązek ochrony poufności informacji

Wszyscy pracownicy NBP, wykonujący zadania związane ze świadczeniem usług zaufania, są zobowiązani do zachowania poufności informacji opisanych w rozdziale 9.3.1. Obowiązek ochrony poufności informacji przez pracowników firm zewnętrznych, wykonujących zadania na rzecz NBP, jest regulowany w umowach zawartych przez NBP z tymi firmami.

NBP ujawnia dane związane z funkcjonowaniem Narodowego Centrum Certyfikacji i objęte tajemnicą wyłącznie następującym podmiotom:

1) sądom i prokuraturze – w związku z toczącym się postępowaniem;
2) ministrowi właściwemu do spraw informatyzacji – w związku ze sprawowaniem przez niego nadzoru nad działalnością dostawców usług zaufania;
3) innym upoważnionym organom – w związku z prowadzonym przez te organy postępowaniem.

Zgodnie z art. 15 ust. 4 ustawy o usługach zaufania nie udostępnia się danych wykorzystywanych przez Narodowe Centrum Certyfikacji służących do składania pieczęci elektronicznej.

9.4 Zobowiązania i gwarancje

9.4.1 Obowiązki NBP

NBP jest obowiązany w szczególności do:

1) wytwarzania certyfikatów Narodowego Centrum Certyfikacji;
2) wytwarzania i wydawania certyfikatów dostawcy usług zaufania na podstawie decyzji ministra właściwego do spraw informatyzacji;
3) publikacji certyfikatów Narodowego Centrum Certyfikacji;
4) publikacji wydanych certyfikatów dostawcy usług zaufania;

5) publikacji list wydanych certyfikatów dostawcy usług zaufania;
6) prowadzenia Rejestru;
7) publikacji zaufanej listy;
8) zapewnienia aktualności zaufanej listy;
9) publikacji danych służących do weryfikacji zaufanej listy;
10) terminowej publikacji aktualnych list unieważnionych certyfikatów;
11) zapewnienia należytego poziomu bezpieczeństwa prowadzenia działalności;
12) zapewnienia ochrony danych osobowych stosownie do postanowień ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r. poz. 922), zwanej dalej „ustawą o ochronie danych osobowych", o ile przepisy ustawy o usługach zaufania nie stanowią inaczej;
13) używania danych służących do składania pieczęci elektronicznej zgodnie z ustawą o usługach zaufania;
14) wykorzystywania przy pełnieniu roli podmiotu upoważnionego, w szczególności przy tworzeniu rejestrów zdarzeń oraz tworzeniu listy unieważnionych certyfikatów dostawcy usług zaufania, rozwiązań zapewniających synchronizację z Międzynarodowym Wzorcem Czasu (Coordinated Universal Time) z dokładnością do 1 sekundy.

9.4.2 Obowiązki Punktu Rejestracji

Punkt Rejestracji Narodowego Centrum Certyfikacji w siedzibie Centrali NBP jest odpowiedzialny za odbieranie i realizację wniosków ministra właściwego do spraw informatyzacji, a także za wymianę dokumentów oraz informacji pomiędzy Subskrybentem oraz ministrem właściwym do spraw informatyzacji a NBP.

9.4.3 Obowiązki Subskrybenta

Subskrybent jest obowiązany w szczególności do:

1) przestrzegania przepisów ustawy o usługach zaufania oraz innych aktów prawnych obowiązujących na terytorium Rzeczypospolitej Polskiej;
2) przestrzegania zasad określonych w Polityce;
3) spełniania wymogów bezpieczeństwa, nakładanych przez ustawę o usługach zaufania oraz normy i obowiązujące standardy, w tym do prawidłowego i bezpiecznego wytworzenia danych powiązanych z certyfikatem dostawcy usług zaufania i służących do składania pieczęci elektronicznych i podpisów elektronicznych oraz ochrony tych danych przed utratą, kradzieżą, ujawnieniem, modyfikacją oraz nieautoryzowanym dostępem i użyciem;
4) niezwłocznego powiadomienia ministra właściwego do spraw informatyzacji o naruszeniu bezpieczeństwa lub o podejrzeniu naruszenia bezpieczeństwa danych

powiązanych z certyfikatem dostawcy usług zaufania i służących do składania pieczęci elektronicznych lub podpisów elektronicznych;
5) sprawdzenia i potwierdzenia poprawności danych zawartych w wydanym certyfikacie dostawcy usług zaufania;
6) zapoznawania się z treścią korespondencji przesyłanej przez NBP;
7) niezwłocznego zawiadomienia ministra właściwego do spraw informatyzacji, nie później niż w terminie 14 dni od zmiany stanu faktycznego lub prawnego, o każdej zmianie danych zawartych we wniosku, o którym mowa w art. 7 ustawy o usługach zaufania.

9.4.4 Obowiązki strony ufającej

Strona ufająca powinna dokonać weryfikacji każdego podpisu elektronicznego i pieczęci elektronicznej, którym zamierza zaufać, ze szczególnym uwzględnieniem informacji zawartych w Polityce.

9.5 Wyłączenia odpowiedzialności z tytułu gwarancji

Wydanie certyfikatu dostawcy usług zaufania nie czyni z NBP agenta, powiernika czy reprezentanta podmiotu, któremu wydany zostaje certyfikat dostawcy usług zaufania.

9.6 Ograniczenia odpowiedzialności

NBP nie ponosi wobec Strony ufającej odpowiedzialności za szkody powstałe na skutek niedopełnienia przez nią swoich obowiązków oraz niedopełnienia obowiązków przez Subskrybenta lub inną Stronę ufającą, w tym za:

1) zaniedbanie obowiązku weryfikacji podpisu elektronicznego lub pieczęci elektronicznej;
2) zaufanie zweryfikowanemu niekompletnie lub negatywnie podpisowi elektronicznemu bądź pieczęci elektronicznej;
3) zaufanie opatrzonym podpisem elektronicznym lub pieczęcią elektroniczną dokumentom zawierającym nieprawdziwe dane;
4) opatrzenie podpisem elektronicznym lub pieczęcią elektroniczną nieprawdziwych danych przez Subskrybenta;
5) niedopełnienie obowiązku ochrony danych służących do składania podpisu elektronicznego lub pieczęci elektronicznej.

NBP nie odpowiada za procesy związane ze świadczeniem usług zaufania przez Subskrybenta.

9.7 Interpretacja i wykonywanie aktów prawnych

Działalność Narodowego Centrum Certyfikacji zgodna jest z obowiązującymi na terytorium Rzeczypospolitej Polskiej aktami prawnymi, w szczególności ustawą o usługach zaufania oraz aktami wykonawczymi wydanymi do niej.

Jeśli jakiekolwiek postanowienie Polityki stałoby się nieważne lub niewykonalne, nie wpłynie to w żaden sposób na ważność i wykonalność pozostałych postanowień. Każde postanowienie Polityki dotyczące ograniczenia odpowiedzialności jest wiążące i niezależne od pozostałych postanowień.

10. Publikacja Zaufanej listy

Zgodnie z art. 11 ust. 1 ustawy o usługach zaufania oraz identyfikacji elektronicznej NBP tworzy, prowadzi i publikuje zaufaną listę, o której mowa w *Decyzji Wykonawczej Komisji (UE) z 2015/1505 z dnia 8 września 2015 r. ustanawiającej specyfikacje techniczne i formaty dotyczące zaufanych list zgodnie z art. 22 ust. 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym*.

Zaufana lista zawiera informacje dotyczące kwalifikowanych dostawców usług zaufania, którzy są objęci nadzorem przez Rzeczpospolitą Polską, wraz z informacjami dotyczącymi świadczonych przez nich kwalifikowanych usług zaufania, zgodnie z odpowiednimi przepisami *Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE*.

Transgraniczne stosowanie podpisów elektronicznych zostało ułatwione poprzez decyzję Komisji 2009/767/WE z dnia 16 października 2009 r., w której nałożono na państwa członkowskie obowiązek tworzenia, prowadzenia i publikowania zaufanych list zawierających informacje dotyczące nadzorowanych/akredytowanych przez państwa członkowskie podmiotów świadczących usługi certyfikacyjne i powszechnie wystawiających kwalifikowane certyfikaty zgodnie z dyrektywą Parlamentu Europejskiego i Rady 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych. Publikowana przez Narodowe Centrum Certyfikacji zaufana lista jest kontynuacją zaufanej listy ustanowionej decyzją 2009/767/WE". Zaufane listy są podstawowym elementem procesu budowania zaufania wśród operatorów rynku elektronicznego, ponieważ umożliwiają użytkownikom ustalenie statusu kwalifikowanego i historii statusu dostawców usług zaufania oraz ich usług.

Certyfikaty służące do weryfikacji pieczęci elektronicznej, którą opatrzono zaufaną listę, są publikowane na stronie www.nccert.pl oraz znajdują się na europejskiej „liście list" publikowanej przez Komisję Europejską. Identyfikator wyróżniający tych certyfikatów ma postać:

Nazwa pola	Wartość
Kraj	PL
Organizacja	National Bank of Poland
Nazwa powszechna	Polish TSL Operator

10.1 Częstotliwość publikacji Zaufanej listy

Aktualna zaufana lista jest publikowana co najmniej raz na 3 miesiące oraz niezwłocznie po:

- wydaniu lub unieważnieniu certyfikatu dostawcy usług zaufania
- każdej aktualizacji Rejestru, o ile aktualizacja ta powoduje konieczność zmiany danych zawartych na zaufanej liście.

Operacje związane z wytworzeniem i publikacją aktualnej zaufanej listy zapisywane są w rejestrze zdarzeń.

Aktualna zaufana lista jest publikowana pod adresem https://www.nccert.pl/tsl/PL_TSL.xml

Dodatkowo, na stronie https://www.nccert.pl znajdują się:

1. certyfikaty służące do weryfikacji pieczęci elektronicznej którą opatrzono zaufaną listę,
2. plik zawierający skrót (sha256) z aktualnej zaufanej listy,
3. link do europejskiej „listy list" będącej zbiorem odnośników do list publikowanych przez poszczególne państwa członkowskie, a także zawierającej certyfikaty służące do weryfikacji podpisów elektronicznych i pieczęci elektronicznych, którymi opatrzono te listy.
4. Decyzja Komisji z dnia 8 września 2015 r. ustanawiająca specyfikacje techniczne i formaty dotyczące zaufanych list zgodnie z art. 22 ust. 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.

Załącznik A – Certyfikaty Narodowego Centrum Certyfikacji

Data wystawienia	26 października 2009 roku
Data wygaśnięcia	27 października 2020 roku
Identyfikator klucza podmiotu	59 34 0c fb 7d e7 45 01 6f c9 70 96 c2 4e 06 f8 0f 81 43 f6
Certyfikat w formacie base64	-----BEGIN CERTIFICATE----- MIIDzTCCArWgAwIBAgIUYqcNBMMkuNQnVsw/gWvy6zLvBxkwDQYJKoZIhvcNAQEF BQAwbjELMAkGA1UEBhMCUEwxLjAsBgNVBAoMJU1pbmlzdGVyIHdsYXNjaXd5IGRv IHNwcmF3IGdvc3BvZGFya2kxLzAtBgNVBAMMJk5hcm9kb3dlIENlbnRydW0gQ2Vy dHlmaWthY2ppIChOQ0NlcnQpMB4XDTA5MTAyNjA2NTcwMVoXDTIwMTAyNjIzNTk1 OVowbjELMAkGA1UEBhMCUEwxLjAsBgNVBAoMJU1pbmlzdGVyIHdsYXNjaXd5IGRv IHNwcmF3IGdvc3BvZGFya2kxLzAtBgNVBAMMJk5hcm9kb3dlIENlbnRydW0gQ2Vy dHlmaWthY2ppIChOQ0NlcnQpMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC AQEA47WXqJ/BLdHdOOh7Stj8NMUVYlmwmpfr8KUOoJA4AEYp+KZaK58wgaknV7a/ v1y+4OXSGCRtvDP7YiLbqlC3TmkKaUFxeizygmo07PtUEIyAXhA72yfe/RI8ZyW9 +jv8tY6aNPK7FTpBP6T2WngLdNMN9iwd7AhCZoZCYL3auA/xqKJUmJC8F/9+tkzk B8PEV6LIzuyE8cF+225VTHJtMkqNhwJSn35BKlAm+d4j/ra58Bh/KYicqLibDKV0 TKPG/3MIFNXLmW9ia/7GkGkGXmjHwlNrWwwpgaPHLTeUMOghD9ve/dyD1afEdjyi Q1BNGcfUCZ8qXKF0ROZaDoy7PQIDAQABo2MwYTAOBgNVHQ8BAf8EBAMCAQYwDwYD VR0TAQH/BAUwAwEB/zAfBgNVHSMEGDAWgBRZNAz7fedFAW/JcJbCTgb4D4FD9jAd BgNVHQ4EFgQUWTQM+33nRQFvyXCWwk4G+A+BQ/YwDQYJKoZIhvcNAQEFBQADggEB ALt95q4lwfjnsFsENeoq8xhYOz/y7veagxLM6f7t0nTPn4GVihXdVZUWQ3IpvRHu h0x1X3etV2IcuEWQw4oNsdWk2ydZwxbMdxebnrVIk7tteyTRjSg3FCjtCyPfHRga y505/bxiWVph64uClZA/1D5cC+IzN3h2xxU2faX1A4Bq2m52s9XzNqZe6SwJBqn2 YE9oDER0MFXhpgZOOSK5owveLBb4MdFKqno96CD9V8u/fD16v7lSwJE+fSub+ih+ DlUEMBM3kJ0SA7pClHl3fOlGCw7rzVjX67QlYbr1vMFuWYx0fv65YD9UrNX5THkT 2kq8e5JRDuHq4X17XtGHlU4= -----END CERTIFICATE-----

Data wystawienia	9 grudnia 2016 roku
Data wygaśnięcia	10 grudnia 2039 roku
Identyfikator klucza podmiotu	29 b3 c8 c4 df a3 87 f8 66 05 12 58 fd 46 2a b8 98 0d 79 87
Certyfikat w formacie base64	-----BEGIN CERTIFICATE----- MIIFzzCCA7egAwIBAgIUQPj3irDjZBBWkcjZ4Cz4wcZACkYwDQYJKoZIhvcNAQEN BQAwbzELMAkGA1UEBhMCUEwxHTAbBgNVBAoMFE5hcm9kb3d5IEJhbmsgUG9sc2tp MSYwJAYDVQQDDB1OYXJvZG93ZSBDZW50cnVtIENlcnR5ZmlrYWNqaTEZMBcGA1UE YQwQVkFUUEwtNTI1MDAwODE5ODAeFw0xNjEyMDkwODUyNDFaFw0zOTEyMDkyMzU5 NTlaMG8xCzAJBgNVBAYTAlBMMR0wGwYDVQQKDBROYXJvZG93eSBCYW5rIFBvbHNr aTEmMCQGA1UEAwwdTmFyb2Rvd2UgQ2VudHJ1bSBDZXJ0eWZpa2FjamkxGTAXBgNV BGEMEFZBVFBMLTUyNTAwMDgxOTgwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIK AoICAQDuyaDrULBW0PLYMfDwG1cZ6qWlTCzhb+vffSNd6AvF/4uTwCpNNcbHH3WH st1FD1ZygGBFyWjb6QpGwW58JSd+6+UuvsVTzYSilhrd4afmNGyKg945e4z1vY91 bzivNPQ+LcXPMFx+GLcncrYzyQLsK5fqNOuVQDXPhrFG3o4gDxhUWsHjpBKWvFwI n1VzNcP17/MML5pYAnOGnlNQpjqexbzSEsDF3b1mTi50kkfHD/NN4zSaJMJGvsFj aIFhakEuLA6GeI7OO+do3oh5U8osUYOznbB1BtC3NGAE9NU1JeSHQH3speUX8iH7 0UjNdhyf96HY/ZDMRJF4bfWLdBCxCAmWJEYADbciUxus6TUjrjEzKSceMEmjg2Or DMUISSmsH44Usx6S367WmGVpsuMh39X0GQRLz+ntwqJi1yvRttcdrhrNo7jOEG2R Elm113+GDo1mmtMB6TrKU42kEQsR1yH7FAO0/zsvnnVjUtFEHH45SQWS43fuZXO1 ioS0SFNO/7wKZS+cYOzzGlMvv+eW6jVYouXupM/Fa5+vkhYnw6v/LTWIYylw9XbZ Xpgf+aSa8ZWiaTKfHhEHFmhVPjqUF4bkACVUknu+5UZKUTE1+69PgpEe0uhyzJ/z QIwZ6+MHpzDx2cfi6qU2sKGS8M99upjMm7GQ4LqHlG/lYrterwIDAQABo2MwYTAO BgNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/BAUwAwEB/zAfBgNVHSMEGDAWgBQps8jE 36OH+GYFElj9Riq4mA15hzAdBgNVHQ4EFgQUKbPIxN+jh/hmBRJY/UYquJgNeYcw DQYJKoZIhvcNAQENBQADggIBAK+GzchsHQruy9sCZ2QDtF6kveZT5JVfpfJ7Aspw VR3+VrH50aiGlSid4va1EBHWxD1uw7t3FMYvlvU/KAk+TA5+0GSrJFalO5nYNma9 dYcgiD8tBQdB3tOU27wTrSD0VXsolXnRYNerNyeo5TWzqcy5InfZAT95XtmTE9me l1cu4yYwdT1/+m0ws9YZLdvaDK9tIJzkOn4CFTCvMUcGMOg1ncE1X07LH26ibsiV zgbVBoK6Qe+O4w533pTta9rOoudOqL44F/+YPSSfBNvRD49OpQNYsf2umgS2WTsk

```
wcSEM/gJoelE0Avp4c1rz0/6VQsX+JNOnHadKZQl1GUrUxEAiAy4A5hpz6qyTNtu
DSc3tdbjaddLr7jESAaU3Zbi/s+vDeYqgO5jsR6RX1iyBpUTdciTnZOGSyRE5ek2
g6IERpmnhP4bKL2ylJK+OchYFL/HFPFiAuRXBhiv5o8AOQGvWVY8bCvzliI869IS
w4kdpmxnyx9GKxcuTTmvr3TMIbEpCuG+vCsmjvl+JtP/bGWSNjSpzxO4NEABnAjM
BI4m+SGQy2wxJ3dEONZvjk1ph0bYE/cQRlgoxAlk8JuGt0XTw03Ar2EklhN8IeBk
8e6KDeKxSNX60z3XTChCgTPj+ErwdNzX8tcRo5FrQ68VwTF27+pYYAEfAs2hqHZ2
KHW0
-----END CERTIFICATE-----
```

Załącznik B – Profil żądania certyfikacyjnego

Pole (typ pola)	Uwagi
CertificationRequest (*CertificationRequest*)	Żądanie certyfikacyjne PKCS#10.
certificationRequestInfo (*CertificationRequestInfo*)	Właściwa treść żądania certyfikacyjnego.
version (*Version*)	Wersja żądania certyfikacji, wartość pola: 0 (wersja v1)
subject (*Name*)	Unikalna nazwa wyróżniająca kwalifikowanego dostawcy usług zaufania, zgodna z wymaganiami określonymi w punkcie 3.1.1
subjectPKInfo (*SubjectPublicKeyInfo*)	Wartość danych służące do walidacji wraz z identyfikatorem algorytmu, z którym stowarzyszone są te dane.
algorithm (*AlgorithmIdentifier*)	Identyfikator algorytmu, z którym stowarzyszone są dane służące do walidacji.
Algorithm(1) (*OBJECT IDENTIFIER*)	Identyfikator obiektu przypisany algorytmowi, z którym stowarzyszone są dane służące do walidacji.
parameters	Atrybut zgodny z polem **Algorithm(1)** i określany przez kwalifikowanego dostawcę usług zauufania.
subjectPublicKey (*BIT STRING*)	Dane służące do walidacji.
attributes (*Attributes*)	Atrybuty żądania certyfikacyjnego do umieszczenia w certyfikacie dostawcy usług zaufania.
subjectKeyIdentifier (*SubjectKeyIdentifier*)	Pole opcjonalne – Identyfikator danych służących do walidacji.
keyUsage (*KeyUsage*)	Zamierzony sposób wykorzystania danych służących do składania pieczęci elektronicznej lub podpisu elektronicznego.
extKeyUsage (*ExtendedKeyUsage*)	Zamierzone rozszerzone zastosowanie danych służących do składania pieczęci elektronicznej lub podpisu elektronicznego. **Pole nie występuje** w

	przypadku usługi polegającej na wydawaniu kwalifikowanych certyfikatów.
signatureAlgorithm (*AlgorithmIdentifier*)	Identyfikator algorytmu z którym stowarzyszone są dane służące pieczęci elektronicznej lub popisu elektronicznego składanego przez kwalifikowanego dostawcę usług zaufania.
Algorithm(2) (*OBJECT IDENTIFIER*)	Identyfikator obiektu przypisany algorytmowi, z którym stowarzyszone są dane służące pieczęci elektronicznej lub popisu elektronicznego składanego przez kwalifikowanego dostawcę usług zaufania.
parameters	Atrybut zgodny z polem **Algorithm(2)** i określany przez kwalifikowanego dostawcę usług zaufania.
signatureValue (*BIT STRING*)	Wartość pieczęci elektronicznej lub popisu elektronicznego złożonego przez kwalifikowanego dostawcę usług zaufania.

Załącznik C – Profil certyfikatu dostawcy usług zaufania

Pole (typ pola)	Uwagi
tbsCertificate (*TBSCertificate*)	Właściwa treść certyfikatu.
version (*Version*)	Wersja certyfikatu, wartość pola: 2 (wersja v3).
serialNumber (*CertificateSerialNumber*)	Unikalny numer seryjny.
signature (*AlgorithmIdentifier*)	Identyfikator algorytmu pieczęci elektronicznej składanej przez Narodowe Centrum Certyfikacji.
algorithm (*OBJECT IDENTIFIER*)	Identyfikator obiektu: { iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }[1] { iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 13 }[2]
parameters	**null**
issuer (*Name*)	Identyfikator wyróżniający Narodowego Centrum Certyfikacji, opisany w punkcie 3.1.1.
validity (*Validity*)	Oznaczenie okresu ważności certyfikatu.
notBefore (*Time*)	Początek okresu ważności certyfikatu.
notAfter (*Time*)	Koniec okresu ważności certyfikatu.
subject (*Name*)	Identyfikator wyróżniający Subskrybenta opisany w punkcie 3.1.1.
subjectPublicKeyInfo (*SubjectPublicKeyInfo*)	Wartość danych służących do walidacji wraz z identyfikatorem algorytmu, z którym stowarzyszone są te dane.

[1] Dla certyfikatów weryfikowanych certyfikatem Narodowego Centrum Certyfikacji wystawionym w 2009 r.
[2] Dla certyfikatów weryfikowanych certyfikatem Narodowego Centrum Certyfikacji wystawionym w 2016 r.

algorithm (*AlgorithmIdentifier*)	Identyfikator algorytmu, z którym stowarzyszone są dane służące do walidacji.
algorithm (*OBJECT IDENTIFIER*)	Identyfikator obiektu przypisany algorytmowi, z którym stowarzyszone są dane służące do walidacji.
parameters	Atrybut zgodny z polem **algorithm** i określany przez kwalifikowanego dostawcę usług zaufania oraz dostarczany do Narodowego Centrum Certyfikacji w żądaniu certyfikacyjnym.
subjectPublicKey (*BIT STRING*)	Dane służące do walidacji.
extensions (*Extensions*)	Rozszerzenia certyfikatu.
authorityKeyIdentifier (*AuthorityKeyIdentifier*)	**Rozszerzenie niekrytyczne** - Identyfikator danych służących do walidacji pieczęci elektronicznej złożonej przez Narodowe Centrum Certyfikacji.
keyIdentifier (*KeyIdentifier*)	Wartość skrótu (algorytm SHA-1) z danych służących do walidacji pieczęci elektronicznej złożonej przez Narodowe Centrum Certyfikacji.
authorityCertIssuer (*GeneralNames*)	Unikalna nazwa wyróżniająca zgodna z polem **issuer**.
authorityCertSerialNumber (*AuthorityCertSerialNumber*)	Numer seryjny certyfikatu Narodowego Centrum Certyfikacji.
subjectKeyIdentifier (*KeyIdentifier)*	**Rozszerzenie niekrytyczne** - Identyfikator – wartość skrótu (algorytm SHA-1) z danych służących do walidacji pieczęci elektronicznej lub podpisu elektronicznego Subskrybenta
KeyUsage (*KeyUsage*)	**Rozszerzenie krytyczne** – sposób wykorzystania danych służących do składania pieczęci elektronicznej lub podpisu elektronicznego przez Subskrybenta.

certificatePolicies (*CertificatePolicies*)	**Rozszerzenie krytyczne** – Polityka certyfikacji Narodowego Centrum Certyfikacji.
policyIdentifier (OBJECT IDENTIFIER)	Identyfikator polityki (anyPolicy) – wartość pola **{ 2 5 29 32 0 }**
policyQualifiers (PolicyQualifierInfo)	Informacja o polityce certyfikacji Narodowego Centrum Certyfikacji.
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 dany certyfikat jest certyfikatem dostawcy usług zaufania wydającym certyfikaty
cA (*BOOLEAN*)	Pole ma wartość: 1. **True** – w przypadku certyfikatu będącego certyfikatem dostawcy usług zaufania wydającym certyfikaty kwalifikowane, 2. **False** – w pozostałych przypadkach.
extKeyUsage (lista pól typu *OBJECT IDENTIFIER*)	Rozszerzenie krytyczne: 1. w przypadku certyfikatu dostawcy usług zaufania świadczącego usługi zaufania polegające na wydawaniu certyfikatów pole nie występuje, **2.** w pozostałych przypadkach pole zawiera identyfikator obiektu wskazujący na rodzaj usługi zaufania określony przez Subskrybenta i dostarczany do Narodowego Centrum Certyfikacji w żądaniu certyfikacyjnym.

SignatureAlgorithm (*AlgorithmIdentifier*)	identyfikator algorytmu pieczęci elektronicznej składanej przez Narodowe Centrum Certyfikacji.
Algorithm (*OBJECT IDENTIFIER*)	Identyfikator obiektu: { iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }[3] { iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 13 }[4]
parameters	**null**
signatureValue (*BIT STRING*)	Wartość pieczęci elektronicznej złożonej przez Narodowe Centrum Certyfikacji.

[3] Dla certyfikatów weryfikowanych certyfikatem Narodowego Centrum Certyfikacji wystawionym w 2009 r.
[4] Dla certyfikatów weryfikowanych certyfikatem Narodowego Centrum Certyfikacji wystawionym w 2016 r.

Załącznik D – Profil listy CRL

Pole (typ pola)	Uwagi
tbsCertList (*TBSCertList*)	Lista CRL
version (*Version*)	Wersja listy CRL – wartość pola: 1 (wersja v2).
signature (*AlgorithmIdentifier*)	Identyfikator algorytmu pieczęci elektronicznej składanej przez Narodowe Centrum Certyfikacji.
algorithm (*OBJECT IDENTIFIER*)	Identyfikator obiektu: { iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }[5] { iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 13 }[6]
parameters	**null**
issuer (*Name*)	Identyfikator wyróżniający Narodowego Centrum Certyfikacji, opisany w punkcie 3.1.1.
thisUpdate (*Time*)	Data wydania listy.
nextUpdate (*Time*)	Przewidywana data wydania następnej listy.
revokedCertificates (*Name*)	Lista unieważnionych certyfikatów.
userCertificate (*CertificateSerialNumber*)	Numer seryjny unieważnionego certyfikatu.
revocationDate (*Time*)	Data i czas unieważnienia.
crlEntryExtensions (*Extensions*)	Rozszerzenia informacji o unieważnieniu dotyczące każdego certyfikatu oddzielnie.
cRLReason (*CRLReason*)	Przyczyna unieważnienia certyfikatu (patrz punkt D.1)

[5] Dla list CRL weryfikowanych certyfikatem Narodowego Centrum Certyfikacji wystawionym w 2009 r.
[6] Dla list CRL weryfikowanych certyfikatem Narodowego Centrum Certyfikacji wystawionym w 2016 r.

crlExtensions (*Extensions*)	Rozszerzenia listy unieważnionych certyfikatów.
authorityKeyIdentifier (*AuthorityKeyIdentifier*)	Identyfikator danych służących do walidacji pieczęci elektronicznej składanej przez Narodowe Centrum Certyfikacji.
keyIdentifier (*KeyIdentifier*)	Wartość skrótu (algorytm SHA-1) z danych służących do walidacji pieczęci elektronicznej składanej przez Narodowe Centrum Certyfikacji.
authorityCertIssuer (*GeneralNames*)	Unikalna nazwa wyróżniająca zgodna z polem **issuer**.
authorityCertSerialNumber (*AuthorityCertSerialNumber*)	Numer seryjny zcertyfikatu Narodowego Centrum Certyfikacji.
cRLNumber (*Integer (0..MAX)*)	Numer kolejny listy unieważnionych certyfikatów.
signatureAlgorithm (*AlgorithmIdentifier*)	Ientyfikator algorytmu algorytmu pieczęci elektronicznej składanej przez Narodowe Centrum Certyfikacji.
algorithm (*OBJECT IDENTIFIER*)	Identyfikator obiektu: { iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }[7] { iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 13 }[8]
parameters	**null**
signatureValue (*BIT STRING*)	Wartość pieczęci elektronicznej złożonej przez Narodowe Centrum Certyfikacji.

[7] Dla list CRL weryfikowanych certyfikatem Narodowego Centrum Certyfikacji wystawionym w 2009 r.
[8] Dla list CRL weryfikowanych certyfikatem Narodowego Centrum Certyfikacji wystawionym w 2016 r.

D.1 Przyczyna unieważnienia certyfikatu

W liście CRL wydawanej przez Narodowe Centrum Certyfikacji w polu CRLReason mogą znaleźć się następujące wartości:

1. **unspecified**: certyfikat został unieważniony, jednak przyczyna unieważnienia jest nieznana; powód unieważnienia nie wyklucza, że ma miejsce kompromitacja lub podejrzenie kompromitacji danych służących do składania podpisu elektronicznego lub pieczęci elektronicznej powiązanych z tym certyfikatem,
2. **keyCompromise**: certyfikat został unieważniony z powodu kompromitacji lub podejrzenia kompromitacji danych służących do składania podpisu elektronicznego lub pieczęci elektronicznej powiązanych z tym certyfikatem,
3. **cACompromise**: certyfikat został unieważniony z powodu kompromitacji danych służących do składania pieczęci elektronicznej przez Narodowe Centrum Certyfikacji,
4. **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 lub pieczęci elektronicznej powiązanych z tym certyfikatem,
5. **superseded**: certyfikat został unieważniony z powodu zastąpienia danych służących do składania podpisu elektronicznego lub pieczęci elektronicznej powiązanych z tym certyfikatem; powód unieważnienia wskazuje, że nie ma miejsca kompromitacja lub podejrzenie kompromitacji danych służących do składania podpisu elektronicznego lub pieczęci elektronicznej powiązanych z tym certyfikatem,
6. **cessationOfOperation**: certyfikat został unieważniony z powodu zaprzestania używania go do celu, dla którego został wydany, i jednocześnie nie ma miejsca sytuacja określona w pkt 4 i 5; wskazany powód unieważnienia wskazuje, że nie ma miejsca kompromitacja lub podejrzenie kompromitacji danych służących do składania podpisu elektronicznego lub pieczęci elektronicznej powiązanych z tym certyfikatem,

Załącznik E – Historia zmian dokumentu

Lp.	Data	Wersja	Osoba	Opis wykonanych prac
1.	22.07.2016	2.51		Dostosowanie dokumentu „Polityka Certyfikacji Narodowego Centrum Certyfikacji wer. 2.5" do przepisów o usługach zaufania
2.	15.09.2016	2.52		Uwzględnienie uwag zgłoszonych przez kwalifikowanych dostawców usług zaufania
3.	1.12.2016	2.53		Dodanie zapisów związanych ze zmianą algorytmów kryptograficznych
4.	8.12.2016	2.6		Zmiana procedury przekazywania żądań certyfikacyjnych do NBP
5.				
6.				
7.				
8.				
9.				

Zatwierdzenie dokumentu

Data	Wersja	Osoba	Podpis
	3.0	Dyrektor Departamentu Bezpieczeństwa	