



NARODOWY  
BANK POLSKI

---

## Informacja o zasadach świadczenia usług zaufania w systemie DOCert

Wersja 4.0

Niniejszy dokument zawiera najważniejsze informacje dotyczące zasad świadczenia usług zaufania w systemie DOCert. Pełna informacja nt. tych zasad znajduje się w dokumencie „System DOCert – Polityka certyfikacji dla certyfikatów użytkowych”, dostępnej pod adresem [http://www.DOCert.nbp.pl/Certyfikaty/PC\\_DOCert.pdf](http://www.DOCert.nbp.pl/Certyfikaty/PC_DOCert.pdf).

## 1. Dane adresowe

Departament Cyberbezpieczeństwa Narodowego Banku Polskiego

ul. Świętokrzyska 11/21, 00-919 Warszawa

tel. +48221851433      mail: [cck@nbp.pl](mailto:cck@nbp.pl)

## 2. Rodzaje i zastosowanie certyfikatów, procedury weryfikacji

Certyfikaty wydawane w systemie DOCert mogą być wykorzystywane:

- zgodnie z informacją zawartą w certyfikacie dotyczącą użycia certyfikatu,
- w systemach informatycznych NBP do wymiany informacji wewnątrz NBP oraz pomiędzy NBP a Klientami<sup>1</sup> w zakresie zapewnienia integralności, poufności i niezaprzeczalności,
- w należącym do Ministerstwa Finansów systemie obsługi budżetu państwa TREZOR, do zapewnienia integralności oraz niezaprzeczalności.

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

Certyfikaty wydawane w systemie DOCert nie są certyfikatami kwalifikowanymi w rozumieniu ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. 2021 poz. 1797) zwanej dalej „ustawą o usługach zaufania”.

Podstawą do wystawienia certyfikatu w systemie DOCert jest „Zamówienie na usługę kryptograficzną” przygotowane przez właściwą jednostkę organizacyjną NBP<sup>2</sup>. „Zamówienie na usługę kryptograficzną” powinno zawierać dane pozwalające na weryfikację tożsamości użytkowników, którzy zgłoszą się po odbiór kluczy kryptograficznych i certyfikatów: imię, nazwisko, PESEL lub serię i numer dokumentu tożsamości. „Zamówienie na usługę kryptograficzną” jest ważne przez 3 miesiące od daty wystawienia. Przed przystąpieniem do generowania kluczy kryptograficznych i certyfikatów pracownik NBP dokonuje weryfikacji tożsamości użytkownika. Weryfikacja ta polega na porównaniu numeru PESEL lub serii i numeru dokumentu tożsamości, wskazanego w „Zamówieniu na usługę kryptograficzną”, z informacją zawartą w dokumencie tożsamości, który użytkownik powinien posiadać podczas wizyty w NBP. Użytkownik osobiście generuje klucze kryptograficzne oraz ustala hasła dostępu do nich.

---

<sup>1</sup> Klient to osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która na podstawie umowy lub przepisów powszechnie obowiązujących korzysta z certyfikatów systemu DOCert

<sup>2</sup> Jednostka organizacyjna NBP to departament Centrali lub oddział okręgowy NBP.

System DOCert umożliwia zdalne odnawianie certyfikatów, bez konieczności składania wizyty w NBP, za pomocą dostępnego na stronie [www.docert.nbp.pl](http://www.docert.nbp.pl) Systemu Zdalnej Obsługi Certyfikatów (SZOC). Przeprowadzenie tej operacji wymaga posiadania kluczy kryptograficznych i ważnego certyfikatu (oraz znajomości hasła chroniącego klucz prywatny) lub posiadania ważnego kodu jednorazowego, otrzymanego z NBP. Na podstawie tych danych dokonywane jest uwierzytelnienie użytkownika dokonującego generowania kluczy kryptograficznych i certyfikatów za pomocą SZOC.

### 3. Ograniczenia odpowiedzialności

Wydanie certyfikatu w systemie DOCert nie czyni z NBP agenta, powiernika czy reprezentanta Uczestnika<sup>3</sup>, któremu wydany został certyfikat.

NBP nie ponosi odpowiedzialności za niedokonanie przez Stronę ufającą<sup>4</sup> poprawnej i rzetelnej weryfikacji każdego podpisu i /lub certyfikatu, któremu zamierza zaufać. Zaufanie niekompletnie lub negatywnie zweryfikowanemu podpisowi lub certyfikatowi następuje na wyłączną odpowiedzialność Strony ufającej.

NBP nie ponosi odpowiedzialności za użycie przez użytkownika kluczy kryptograficznych i certyfikatów niezgodnie z ich przeznaczeniem określonym w umowach oraz dokumencie „System DOCert – polityka certyfikacji dla certyfikatów użytkowych”.

NBP, jako właściciel systemu DOCert, nie ponosi odpowiedzialności za zawartość dokumentów lub innych danych podpisanych lub zaszyfrowanych przy użyciu kluczy kryptograficznych i certyfikatów wygenerowanych w systemie DOCert.

### 4. Zobowiązania Uczestnika

Uczestnik ma obowiązek:

- 1) dostarczyć wszystkie dane wymagane do wystawienia certyfikatu w systemie DOCert i zapewnić ich prawdziwość;
- 2) niezwłocznie informować NBP o wszelkich zmianach danych, o których mowa w pkt 1;
- 3) przestrzegać przepisów polityki certyfikacji oraz umów zawartych pomiędzy NBP a Klientami;
- 4) zapewnić należytą ochronę klucza prywatnego oraz hasła do niego;
- 5) wykorzystywać klucze kryptograficzne i certyfikaty systemu DOCert tylko w zakresie określonym w certyfikacie oraz opisanym w umowach zawartych pomiędzy NBP a Klientami;
- 6) natychmiast żądać unieważnienia certyfikatu w przypadku kompromitacji odpowiadającego mu klucza prywatnego;
- 7) terminowo wymieniać klucze kryptograficzne;

---

<sup>3</sup> Uczestnik to Klient, przedstawiciel Klienta, jednostka organizacyjna NBP lub obiekt (np. serwer) posiadający certyfikat wydany w systemie DOCert.

<sup>4</sup> Strona ufająca to osoba lub podmiot, inna niż Uczestnik, która akceptuje i ufa certyfikatowi wydanemu w systemie DOCert.

- 8) zapewnić aktualność posiadanego pakietu ochrony kryptograficznej;
- 9) w przypadku zakończenia uczestnictwa – zwrócić wszystkie otrzymane z NBP elementy pakietu ochrony kryptograficznej, z wyłączeniem kluczy kryptograficznych zapisanych na nośnikach innych niż karta elektroniczna.

## **5. Zobowiązania stron ufających**

Strona ufająca wykorzystująca certyfikaty systemu DOCert, ma obowiązek:

- 1) korzystać z certyfikatów tylko w zakresie w nich opisanym;
- 2) dokonywać pełnej weryfikacji certyfikatu Uczestnika przed jego wykorzystaniem;
- 3) informować NBP o każdym użyciu certyfikatu przez osobę nieupoważnioną lub w sposób niezgodny z jego przeznaczeniem.

## **6. Zobowiązania NBP**

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

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

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

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

## 7. Polityka certyfikacji

NBP publikuje dokument „System DOCert – Polityka certyfikacji dla certyfikatów użytkowych” na stronie [www.docert.nbp.pl](http://www.docert.nbp.pl).

## 8. Ochrona danych osobowych

NBP jest administratorem danych osobowych przetwarzanych w ramach systemu DOCert z wyłączeniem danych osobowych powierzonych NBP przez Ministerstwo Finansów w ramach porozumienia o współpracy w zakresie świadczenia usług certyfikacyjnych dla Systemu TREZOR. Świadczenie usług zaufania w systemie DOCert odbywa się zgodnie z obowiązującymi przepisami, a w szczególności zgodnie z przepisami o ochronie danych osobowych.

Dane osobowe w systemie DOCert przetwarzane są zarówno w postaci papierowej, jak i elektronicznej i nie są publicznie dostępne.

W systemie DOCert przetwarza się następujące dane osobowe pracowników NBP oraz użytkowników zewnętrznych korzystających z certyfikatów systemu:

- imię i nazwisko ;
- seria i numer dokumentu stwierdzającego tożsamość;
- data urodzenia;
- PESEL i/lub NIP;
- miejsce pracy;
- adres e-mail;
- numer telefonu ;
- certyfikat;
- podpis.

Dokumenty w formie papierowej i elektronicznej, zawierające dane osobowe związane z systemem DOCert, podlegają zabezpieczeniom zapobiegającym nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu, zgodnie z przepisami prawa. Dokumenty w postaci papierowej zawierające dane osobowe związane z systemem DOCert, z wyłączeniem protokołów przekazania pakietu ochrony kryptograficznej, przechowywane są przez okres ważności certyfikatu, którego dotyczą jednak nie dłużej niż przez 7 lat po jego wygaśnięciu lub unieważnieniu. Po tym okresie dokumenty są niszczone zgodnie z procedurami obowiązującymi w NBP.

## 9. Opłaty

NBP nie pobiera opłat za wydanie pakietu ochrony kryptograficznej, kluczy kryptograficznych czy certyfikatów, ani za dostęp do repozytorium, znajdującego się na stronie [www.docert.nbp.pl](http://www.docert.nbp.pl).

NBP **pobiera opłaty** w przypadku :

- Zniszczenia<sup>5</sup> lub zagubienia karty elektronicznej wydanej przez NBP,
- Zagubienia licencji oprogramowania kryptograficznego, przekazanego przez NBP,
- Zagubienia lub zniszczenia czytnika kart elektronicznych, przekazanego przez NBP.

Zasady odpowiedzialności finansowej podmiotów określają umowy zawierane pomiędzy NBP a Klientami korzystającymi z systemów informatycznych NBP, akty normatywne powszechnie obowiązujące oraz akty prawne organów NBP, na podstawie których NBP świadczy dla Klienta usługi zaufania.

## 10. Kwestie prawne

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

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

## 11. Audyt

System DOCert może być objęty kontrolą wewnętrzną lub zadaniem audytowym zgodnie z przepisami odrębnymi. Dodatkowo, z częstotliwością określoną w przepisach odrębnych, Inspektor Bezpieczeństwa Systemu przeprowadza analizę ryzyka systemu DOCert. Celem przeprowadzenia analizy ryzyka systemu DOCert jest ocena poziomu ryzyka bezpieczeństwa systemu. Analizę ryzyka przeprowadza się zgodnie z obowiązującą w NBP metodyką.

---

<sup>5</sup> Za zniszczenie uważa się także trwałe zablokowanie karty elektronicznej oraz brak kodu PUK w przypadku zmiany kodu przekazanego przez NBP.

## 12. Punkty Rejestracji Użytkowników

W systemie DOCert funkcjonuje siedemnaście Punktów Rejestracji Użytkowników - jeden w Centrali NBP oraz szesnaście w oddziałach okręgowych NBP. Dane adresowe Centrali NBP oraz oddziałów okręgowych NBP dostępne są na stronie [www.nbp.pl](http://www.nbp.pl).

## 13. Zatwierdzenie dokumentu

Lp.	Stanowisko / Departament	Data/ Podpis
1.	Dyrektor Departamentu Cyberbezpieczeństwa	

---

[www.nbp.pl](http://www.nbp.pl)