NBP Narodowy Bank Polski

Informacja o zasadach świadczenia usług zaufania w systemie DOCert

Wersja 1.0

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 .

Departament Bezpieczeństwa NBP
Warszawa, 2017

1. Dane adresowe

Departament Bezpieczeństwa Narodowego Banku Polskiego
ul. Świętokrzyska 11/21, 00-919 Warszawa
tel. +48221851414 fax: +48221852336 mail: 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[1] 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. poz 1579) zwanej dalej „ustawą o usługach zaufania".

Podstawą do wystawienia certyfikatu w systemie DOCert jest „Zamówienie na usługę kryptograficzną" przygotowane przez właściwą jednostkę organizacyjną NBP[2]. 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. 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.

System DOCert umożliwia zdalne odnawianie certyfikatów, bez konieczności składania wizyty w NBP, za pomocą dostępnego na stronie www.docert.nbp.pl Systemu Zdalnej

[1] 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
[2] Jednostka organizacyjna NBP to departament Centrali lub oddział okręgowy NBP.

Obsługi Certyfikatów (SZOC). Przeprowadzenie tej operacji wymaga posiadania kluczy kryptograficznych i ważnego certyfikatu (oraz znajomość 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[3], któremu wydany został certyfikat.

NBP nie ponosi odpowiedzialności za niedokonanie przez Stronę ufającą[4] 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 polityk certyfikacji oraz umów zawartych pomiędzy NBP a Klientami;
4) zapewnić należytą ochronę klucza prywatnego oraz hasła do niego;
5) wykorzystywać klucze kryptograficzne i certyfikaty systemu DOCert tylko w zakresie określonym w certyfikacie oraz opisanym w umowach zawartych pomiędzy NBP a Klientami;
6) natychmiast żądać unieważnienia certyfikatu w przypadku kompromitacji odpowiadającego mu klucza prywatnego;
7) terminowo wymieniać klucze kryptograficzne;
8) zapewnić aktualność posiadanego pakietu ochrony kryptograficznej;

[3] Uczestnik to Klient, przedstawiciel Klienta, jednostka organizacyjna NBP lub obiekt (np. serwer) posiadający certyfikat wydany w systemie DOCert.

[4] Strona ufająca to osoba lub podmiot, inna niż Uczestnik, która akceptuje i ufa certyfikatowi wydanemu w systemie DOCert.

9) w przypadku zakończenia uczestnictwa – zwrócić wszystkie otrzymane z NBP elementy pakietu ochrony kryptograficznej, z wyłączeniem kluczy kryptograficznych zapisanych na płycie CD.

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 polityk certyfikacji oraz umów zawartych pomiędzy NBP a Klientami;
2) chronić klucze prywatne Centrum Certyfikacji Kluczy i zapewnić bezpieczeństwo procesu generowania kluczy kryptograficznych Uczestników;
3) generować i zarządzać certyfikatami zgodnie 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 polityk certyfikacji;
7) świadczyć usługi zaufania zgodnie z obowiązującym prawem 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 .

8. Ochrona danych osobowych

NBP jest administratorem danych osobowych przetwarzanych w ramach systemu DOCert. Dane osobowe w systemie DOCert przetwarzane są zarówno w postaci papierowej, jak i elektronicznej, i nie są publicznie dostępne. Dane osobowe związane z usługą zaufania są przetwarzane w ramach zbioru danych osobowych o nazwie „Baza certyfikatów". Nadzór nad prawidłowym przestrzeganiem zasad przetwarzania danych osobowych w NBP pełni Administrator Bezpieczeństwa Informacji. NBP do ochrony danych osobowych stosuje środki zabezpieczeń zgodne z przepisami o ochronie danych osobowych.

Zakres danych osobowych Użytkownika, przetwarzanych w systemie DOCert, w zależności od umów zawartych pomiędzy NBP a Klientami, to:

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

Dokumenty zawierające dane osobowe, po osiągnięciu celu, dla którego zostały zgromadzone, są archiwizowane zgodnie z przepisami powszechnie obowiązującymi oraz wewnętrznymi regulacjami NBP.

Czas przechowywania certyfikatów zawierających dane osobowe jest ściśle związany z czasem przechowywania dokumentów weryfikowanych za pomocą tych certyfikatów. Po tym okresie certyfikaty są usuwane z bazy systemu DOCert, a kopie archiwalne, zawierające te certyfikaty, są niszczone.

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 .

NBP **pobiera opłaty** w przypadku :

- Zniszczenia[5] lub zagubienia karty elektronicznej wydanej przez NBP,
- Zagubienia licencji oprogramowania kryptograficznego, przekazanego przez NBP,
- Zagubienia lub zniszczenia czytnika kart elektronicznych, przekazanego przez NBP.

[5] Za zniszczenie uważa się także trwałe zablokowanie karty elektronicznej oraz brak kodu PUK w przypadku zmiany kodu 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 ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 poz 922 z późn. zm.), oraz ustawą o usługach zaufania.

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.

12. Punkty Rejestracji Użytkowników

W systemie DOCert funkcjonuje 17 Punktów Rejestracji Użytkowników, jeden w Centrali NBP oraz szesnaście w oddziałach okręgowych NBP. Dane adresowe poszczególnych Punktów Rejestracji Użytkowników dostępne są na stronie www.docert.nbp.pl .

13. Identyfikacja dokumentu

Nazwa dokumentu	Informacja o zasadach świadczenia usług zaufania w systemie DOCert
Wersja dokumentu	1.0
Data zatwierdzenia	26.04.2017
Osoba zatwierdzająca	Dyrektor Departamentu Bezpieczeństwa NBP
Lokalizacja	http://www.DOCert.nbp.pl/Certyfikaty/PDS_DOCert.pdf