



Kancelaria Prezesa
Rady Ministrów

Instrukcja wypełniania wniosku o dostęp do Systemu Rejestrów Państwowych (SRP) - Użytkownicy instytucjonalni (wniosek C)

1.1 Informacje

Niniejsza instrukcja zawiera ogólne zasady wypełniania wniosku o dostęp do Systemu Rejestrów Państwowych (SRP) – Użytkownicy instytucjonalni. Na jego podstawie zapewniany jest dostęp do aplikacji ŹRÓDŁO Systemu Rejestrów Państwowych dla pracowników Instytucji Zewnętrznych, które posiadają stosowne uprawnienie wynikające z decyzji Ministra Spraw Wewnętrznych i Administracji lub Ministra Cyfryzacji.

Przed wypełnieniem wniosku o dostęp do Systemu Rejestrów Państwowych użytkownik jest zobowiązany do zapoznania się z dokumentami: Polityka Certyfikacji dla operatorów SRP oraz Polityka Bezpieczeństwa Informacji SRP. O uzyskanie dostępu i otrzymanie certyfikatu wnioskuje osobiście każdy użytkownik.

UWAGA. Certyfikaty dla użytkowników wydawane są na kartach mikroprocesorowych, dlatego wraz z wnioskiem o dostęp do SRP należy przesłać kartę o specyfikacji zgodnej z dokumentem Specyfikacja kart kryptograficznych dla SRP, dostępnej na stronie <https://www.gov.pl/cyfryzacja/jak-uzyskac-dostep-do-srp>. Wraz z kartą należy dostarczyć sterowniki zawierające bibliotekę PKCS#11. Karta w formacie ID1 musi posiadać interfejs stykowy (lub dualny). Ponadto musi być pozbawiona nadruków i posiadać możliwość generowania kluczy kryptograficznych RSA 2048 bit oraz funkcji skrótu SHA-512. Centrum Certyfikacji wykorzystuje następujące karty:

- **Athena IDProtect Duo v1**
- **Gemalto ID Prime 3810**

Dostarczenie jednej z w/w kart nie wymaga przesłania bibliotek PKCS#11.

Instytucja użytkownika odpowiada dodatkowo za przygotowanie odpowiedniej infrastruktury (m.in. czytniki kart), umożliwiającej dostęp do rejestrów z użyciem kart kryptograficznych.

1.2 Wniosek dotyczy następujących sytuacji:

1.2.1 Wydania certyfikatu dla użytkowników instytucjonalnych

Wraz z wnioskiem należy dostarczyć kartę kryptograficzną o specyfikacji zgodnej z dokumentem Specyfikacja kart kryptograficznych dla SRP, dostępnej na stronie <https://www.gov.pl/cyfryzacja/jak-uzyskac-dostep-do-srp>

1.2.2 Zmiany danych

np. nazwiska. Jeżeli użytkownik wykorzystuje kartę kryptograficzną **Athena IDProtect Duo v1** lub **Gemalto ID Prime 3810**, nie przesyła karty do Centrum Certyfikacji. Na podstawie wniosku zostaną zmienione dane w Centrum Certyfikacji. Po zmianie danych użytkownik zostanie poinformowany, że należy dokonać recertyfikacji. Jeżeli użytkownik wykorzystuje kartę kryptograficzną inną niż Athena IDProtect Duo v1 lub Gemalto ID Prime 3810, musi

wraz z wnioskiem dostarczyć kartę kryptograficzną i sterowniki zawierające bibliotekę PKCS#11.

1.2.3 Recertyfikacji – odnowienia certyfikatu

- Podstawowym narzędziem do odnowienia certyfikatu, zapisanego na karcie kryptograficznej **Athena IDProtect Duo v1** lub **Gemalto ID Prime 3810**, jest strona do recertyfikacji - <https://cc.obywatel.gov.pl/>. Jeżeli użytkownik wykorzystuje kartę kryptograficzną inną niż **Athena IDProtect Duo v1** lub **Gemalto ID Prime 3810**, musi wypełnić wniosek wraz, z którym należy dostarczyć kartę kryptograficzną i sterowniki zawierające bibliotekę PKCS#11.
- W przypadku braku możliwości zdalnej recertyfikacji przez stronę <https://cc.obywatel.gov.pl/>, wraz z wnioskiem o recertyfikację należy dostarczyć użytkowaną kartę kryptograficzną.
- W przypadku uszkodzenia karty, wraz z wnioskiem o recertyfikację należy dostarczyć nową kartę kryptograficzną o specyfikacji zgodnej z dokumentem Specyfikacja kart kryptograficznych dla SRP, dostępnej na stronie <https://www.gov.pl/cyfryzacja/jak-uzyskac-dostep-do-srp>.

1.2.4 Usunięcia użytkownika

w przypadku, gdy wnioskujący zaprzestaje korzystania z rejestrów, do których wcześniej uzyskał dostęp. Usunięcie konta wiąże się również z unieważnieniem certyfikatów oraz koniecznością zwrotu karty kryptograficznej udostępnionej przez MSW/MSWiA, MC lub KPRM.

1.2.5 Unieważnienia certyfikatu

jeżeli użytkownik zagubi kartę kryptograficzną do Sytemu Rejestrów Państwowych lub istnieje uzasadnione podejrzenie ujawnienia lub udostępnienia osobom nieupoważnionym klucza prywatnego zapisanego na karcie kryptograficznej.

1.3 Zasady dotyczące wypełniania wniosku

Wniosek należy wypełniać drukowanymi literami. Niedopuszczalne jest dokonywanie jakichkolwiek zmian w szacie graficznej lub w treści wniosku. Wprowadzenie zmian lub niekompletne wypełnienie wniosku będzie skutkowało brakiem realizacji wniosku. Wniosek należy wypełnić w formie elektronicznej (z wyłączeniem podpisów i pieczętek) w celu uniknięcia pomyłek w zapisie.

1.3.1 W punkcie 1 należy wskazać cel złożenia wniosku:

- a) **zapewnienie dostępu dla nowego użytkownika** - w przypadku, gdy wnioskujący składa wniosek po raz pierwszy

- b) **zmiana danych** - przeznaczony dla osób, które posiadają kartę kryptograficzną, ale ich dane uległy zmianie
- c) **recertyfikacja**
 - w przypadku, gdy zbliża się koniec ważności aktualnie używanego certyfikatu, a użytkownik nie ma możliwości przeprowadzenia recertyfikacji za pośrednictwem strony <https://cc.obywatel.gov.pl/>;
 - w przypadku uszkodzenia karty
- d) **usunięcie użytkownika** - w przypadku, gdy wnioskujący zaprzestaje korzystania z rejestrów, do których wcześniej uzyskał dostęp. Usunięcie konta wiąże się również z unieważnieniem certyfikatów oraz koniecznością zwrotu karty kryptograficznej, udostępnionej przez MSW/MSWiA, MC lub KPRM.
- e) **unieważnienie certyfikatu** – np. w przypadku zagubienia karty lub podejrzenia ujawnienia klucza prywatnego zapisanego na karcie kryptograficznej osobom nieupoważnionym

1.3.2 W punkcie 2

należy wpisać dane jednostki organizacyjnej (wraz z ulicą i numerem domu/lokalu) wnioskującej o dostęp. W podpunkcie c) kod konsulatu należy podać czterocyfrowy kod konsulatu. Pole c) kod konsulatu wypełnia tylko organ konsularny.

1.3.3 W punkcie 3

należy wpisać dane użytkownika, który występuje o dostęp do rejestrów.

1.3.4 W punkcie 4

należy wybrać rejestry, do których dostęp zamierza posiadać wnioskujący. Dopuszcza się możliwość wyboru więcej niż jednego rejestru spośród dostępnych. Dopuszcza się możliwość wyboru następujących rejestrów:

- a) PESEL - Powszechny Elektroniczny System Ewidencji Ludności;
- b) RDO - Rejestr Dowodów Osobistych;
- c) BUSC - Baza Usług Stanu Cywilnego;
- d) RDK - Rejestr Danych Kontaktowych;
- e) RDP - Rejestr Danych Paszportowych.

W przypadku rejestrów PESEL, RDO, BUSC i RDP będzie to dostęp w trybie przeglądania, natomiast w przypadku rejestru RDK - w trybie przeglądania i aktualizacji.

1.3.5 W punkcie 5

należy podać numer upoważnienia do przetwarzania danych osobowych, zgromadzonych w rejestrze PESEL, RDO, BUSC, RDK i/lub RDP. Jeżeli do poszczególnych rejestrów zostały wystawione różne upoważnienia, należy podać kolejno ich numery.

1.3.6 W punkcie 6

należy wypełnić w przypadku odbioru osobistego certyfikatu w Centrum Certyfikacji.

Podpunkty a) Rodzaj dokumentu tożsamości i b) Seria i numer dokumentu należy wypełnić, gdy wnioskujący (lub osoba przez niego wyznaczona) zamierza osobiście odebrać kartę kryptograficzną wraz z kodem PIN w Centrum Certyfikacji. Podpunkty c) Imię i d) Nazwisko należy wypełnić w przypadku, kiedy kartę kryptograficzną i PIN odbiera osoba wyznaczona przez wnioskującego. Odbiór osobisty wymaga wcześniejszego uzgodnienia terminu. W przypadku pozostawienia pustych pól w punkcie 6, karta kryptograficzna oraz kod PIN zostaną przesłane pocztą w dwóch oddzielnych przesyłkach na adres jednostki podany przez wnioskującego w punkcie 2 wniosku.

1.4 Informacje końcowe

Wydrukowany wniosek o uzyskanie dostępu należy opatrzyć podpisem osoby składającej wniosek (użytkownika) oraz podpisem i pieczętką kierownika danej jednostki – tj. osoby (organu lub podmiotu) wskazanej w decyzji administracyjnej (piastun organu, kierownik jednostki podmiotu wymienionego w decyzji administracyjnej) lub osoby posiadającej upoważnienie do występowania z wnioskami w imieniu kierownika jednostki (w tym przypadku należy również dołączyć upoważnienie). Do wniosku należy dołączyć kopię decyzji administracyjnej wyrażającej zgodę na uzyskanie dostępu do wybranego rejestru. Dostęp do rejestrów, na które nie zostanie przedłożona pisemna zgoda, nie zostanie udzielony. Wnioski o zapewnienie dostępu dla nowego użytkownika, zmianę danych i recertyfikację muszą zawierać obydwa wymagane podpisy. W przypadku wniosku o usunięcie użytkownika – jego podpis nie jest wymagany. Za ważność posiadanego certyfikatu odpowiada użytkownik.

Poprawnie wypełniony wniosek wraz z niezbędnymi podpisami należy przesłać na adres:

Centralny Ośrodek Informatyki

ul. Gdańska 47/49

90-729 Łódź