Ministerstwo Cyfryzacji

Centrum Certyfikacji
Ministerstwo Cyfryzacji

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

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.

Dodatkowo przed wypełnieniem wniosku o dostęp do Systemu Rejestrów Państwowych użytkownik ma obowiązek zapoznać się z dokumentem „Polityka Certyfikacji dla operatorów 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 z interfejsem stykowym (lub dualnym), na której zostanie umieszczony certyfikat. Użytkownicy instytucjonalni zobowiązani są do dostarczenia wraz z wnioskami kart kryptograficznych, o specyfikacji zgodnej z dokumentem Specyfikacja kart kryptograficznych dla SRP, dostępnej na stronie https://mc.gov.pl/files/specyfikacja_kart_srp.pdf. Wraz z kartą należy dostarczyć sterowniki zawierające bibliotekę PKCS#11. Karta w formacie ID1 musi być pozbawiona nadruków i posiadać możliwość generowania kluczy kryptograficznych RSA 2048 bit oraz funkcji skrótu SHA-512. Centrum Certyfikacji wykorzystuje następujące karty:

1. Athena IDProtect Duo v1
2. 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.

Wniosek dotyczy następujących sytuacji:

1. Wydania certyfikatu na karcie kryptograficznej dla użytkowników instytucjonalnych, którzy będą korzystać z SRP za pomocą aplikacji ŹRÓDŁO.
2. Zmiany danych np. nazwiska. Jeżeli użytkownik wykorzystuje kartę kryptograficzną Athena IDProtect Duo v1 lub Gemalto ID Prime 3810 nie przesyła karty do MC. 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.
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.

4. Usunięcia użytkownika.

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

Ministerstwo Cyfryzacji
Departament Utrzymania i Rozwoju Systemów
ul. Królewska 27
00-060 Warszawa

Zasady dotyczące wypełniania wniosku

W punkcie 1 wniosku należy zaznaczyć tylko jedno pole z możliwych do wyboru:

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

b) *zmiana danych/uprawnień* – w przypadku, gdy wnioskujący składa wniosek o zmianę danych lub aktualnie posiadanych uprawnień;

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/;

d) *usunięcie konta* – w przypadku, gdy wnioskujący zaprzestaje korzystania z rejestrów, do których wcześniej uzyskał dostęp. Usunięcie konta wiąże się również z unieważnieniem certyfikatu.

W punkcie 2 należy wpisać dane jednostki organizacyjnej (wraz z ulicą i numerem domu/lokalu) wnioskującej o dostęp.

W punkcie 3 należy wpisać dane użytkownika, który występuje o dostęp do rejestrów.

W punkcie 4 należy wybrać rejestry, do których dostęp w trybie przeglądania 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.

W punkcie 5 należy podać numer upoważnienia do przetwarzania danych osobowych zgromadzonych w rejestrze PESEL i/lub RDO. Jeżeli jedno upoważnienie zostało wystawione zarówno do PESEL jak i RDO należy podać numer w polu *a) upoważnienie PESEL* i *b) upoważnienie RDO*.

Punkt 6 należy wypełnić w przypadku odbioru osobistego certyfikatu w MC. Podpunkty *a) Rodzaj dokumentu tożsamości* i *b) Seria dokumentu tożsamości* należy wypełnić, gdy wnioskujący (lub osoba przez niego wyznaczona) zamierza osobiście odebrać kartę kryptograficzną wraz z kodem PIN

w Centrum Certyfikacji MC. Podpunkty *c) Imię* i *d) Nazwisko* należy wypełnić w przypadku, jeżeli 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.

Wydrukowany wniosek o uzyskanie dostępu należy opatrzyć podpisem osoby składającej wniosek (użytkownika) oraz podpisem i pieczątką 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. W przypadku zbliżania się końca terminu ważności certyfikatu użytkownik musi wypełnić wniosek z zaznaczeniem pola recertyfikacja i przesłać do MC.