



Ministerstwo
Cyfryzacji

Centrum Certyfikacji
Ministerstwo Cyfryzacji

Instrukcja wypełniania wniosku o dostęp do Systemu Rejestrów Państwowych (SRP) - Użytkownicy aplikacji „Źródło” (wniosek A)

Informacje

Instrukcja zawiera ogólne zasady wypełniania wniosku o dostęp do Systemu Rejestrów Państwowych (SRP) - Użytkownicy aplikacji „Źródło”. Na podstawie wniosku zapewniany jest dostęp do Systemu Rejestrów Państwowych dla pracowników Urzędów Gmin, Urzędów Stanu Cywilnego oraz innych pracowników urzędów, którzy do realizacji swoich obowiązków związanych z obsługą spraw obywatelskich potrzebują dostępu do Rejestrów Państwowych.

Udostępnienie danych z Rejestru PESEL oraz Rejestru Dowodów osobistych następuje na podstawie odpowiedniej ustawy, upoważnienia wydanego przez Ministra Spraw Wewnętrznych i Administracji, Ministra Cyfryzacji lub innych szczególnych przepisów.

Przed wypełnieniem wniosku o dostęp do Systemu Rejestrów Państwowych użytkownik jest zobowiązany do zapoznania się z dokumentem „Polityka Certyfikacji dla operatorów SRP”. O uzyskanie dostępu i otrzymanie certyfikatu wnioskuje każdy użytkownik.

Wniosek dotyczy następujących sytuacji:

1. Wydania certyfikatu na karcie kryptograficznej dla urzędników. Wraz z wnioskiem należy dostarczyć kartę kryptograficzną o specyfikacji zgodnej z dokumentem *Specyfikacja kart kryptograficznych dla SRP*, dostępnej na stronie https://mc.gov.pl/files/specyfikacja_kart_srp.pdf.
2. Zmiany danych np. nazwiska. Jeżeli użytkownik wykorzystuje kartę kryptograficzną **Athena IDProtect Duo v1** lub **Gemalto ID Prime 3810** nie przysyła karty do Ministerstwa Cyfryzacji (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. Jeżeli użytkownik wykorzystywał kartę kryptograficzną **Athena IDProtect Duo v1** lub **Gemalto ID Prime 3810**, która została przekazana przez MSW/MSWiA lub MC, wraz z wnioskiem musi dostarczyć kartę kryptograficzną.

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

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

Zasady dotyczące wypełniania wniosku

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/>;

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 lub MC.

W punkcie 2 należy wpisać dane jednostki organizacyjnej (wraz z ulicą i numerem domu/lokalu) wnioskującej o dostęp. W podpunkcie *c) kod terytorialny* w przypadku Urzędów Gmin i Urzędów Stanu Cywilnego należy podać siedmiocyfrowy kod TERYT, w przypadku Urzędów Wojewódzkich dwucyfrowy kod Województwa. W podpunkcie *d) kod lokalizacji* w przypadku Urzędów Gmin i Urzędów Stanu Cywilnego domyślną wartością jest 01. Jeżeli Gmina lub USC posiada więcej niż jedną lokalizację, należy wpisywać kolejne wartości, np. jeżeli są trzy lokalizacje, pierwsza ma kod 01, druga kod 02, a trzecia kod 03. W przypadku Urzędów Wojewódzkich w polu *d) kod lokalizacji* należy podać wartość 00.

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

Punkt 4 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 4, 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 pieczętą kierownika danej jednostki wnioskującej. Wnioski o zapewnienie dostępu dla nowego użytkownika, zmianę danych i recertyfikację mają zawierać obydwa wymagane podpisy. Wniosek o usunięcie użytkownika wymaga tylko podpisu i pieczętki kierownika danej jednostki. Użytkownicy, którzy utracili (zagubili lub zniszczyli) kartę kryptograficzną zobowiązani są do dostarczenia wraz z wnioskiem kartę kryptograficzną.