Ministerstwo
Cyfryzacji

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

1.1 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, Urzędów Wojewódzkich, konsulatów oraz innych pracowników urzędów, którzy do realizacji swoich obowiązków związanych z obsługą spraw obywatelskich potrzebują dostępu do Rejestrów Państwowych.

Udostępnienie danych z SRP 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 dokumentami: Polityka Certyfikacji dla operatorów SRP oraz Polityka Bezpieczeństwa Informacji SRP. O uzyskanie dostępu i otrzymanie certyfikatu wnioskuje każdy użytkownik.

1.2 Wniosek dotyczy następujących sytuacji:

1.2.1 **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://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 3810/930nc** 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 3810/930nc** 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 3810/930nc** jest aplikacja Chiron. Jeżeli użytkownik wykorzystuje kartę kryptograficzną inną niż **Athena IDProtect Duo v1** lub **Gemalto ID Prime 3810/930nc** musi wypełnić wniosek, wraz z którym należy dostarczyć kartę kryptograficzną i sterowniki zawierające bibliotekę PKCS#11.
- W przypadku braku możliwości zdalnej recertyfikacji przez aplikację Chiron 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 np. 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 pieczątek) 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/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 aplikacji Chiron;
- 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 terytorialny w przypadku Urzędów Gmin i Urzędów Stanu Cywilnego należy podać siedmiocyfrowy kod TERYT, w przypadku Urzędów Wojewódzkich dwucyfrowy kod Województwa. Podpunkt d) kod organu wypełnia Urząd Wojewódzki oraz konsulat. Należy w nim wpisaćć czerocyfrowy kod organu paszportowego. W podpunkcie e) 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.

1.3.3 **W punkcie 3**

należy wybrać odpowiedni rodzaj jednostki, która składa wniosek o dostęp do SRP. W przypadku:

- urzędu wojewódzkiego dokonać wyboru zakresu przysługujących użytkownikowi uprawnień
- urzędu gminy dokonać wyboru zakresu przysługujących uprawnień.
- rola UKR uprawnia do dostępu do rejestru zakwaterowania obywateli Ukrainy (wniosków o świadczenie na pokrycie kosztów zakwaterowania i wyżywienia). W przypadku urzędów wojewódzkich dotyczy tylko przeglądania tego rejestru.

Dla urzędu gminy, jeżeli wniosek dotyczy pracownika jednocześnie ewidencji ludności i dowodów osobistych lub UKR jak i obsługi mobilnej RDO należy wypełnić 2 oddzielne wnioski.

1.3.4 **W punkcie 4**

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

1.3.5 **W punkcie 5**

należy wypełnić tylko w przypadku odbioru osobistego certyfikatu w Centrum Certyfikacji. 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.

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 5, 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 pieczątką 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 pieczątki kierownika danej jednostki. Użytkownicy, którzy utracili (zagubili lub zniszczyli) kartę kryptograficzną zobowiązani są do dostarczenia wraz z wnioskiem nową kartę kryptograficzną.

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

Centralny Ośrodek Informatyki
ul. Gdańska 47/49
90-729 Łódź