Ministerstwo
Spraw Wewnętrznych

Centrum Certyfikacji
Ministerstwa Spraw Wewnętrznych

Instrukcja zdalnej recertyfikacji oraz zdalnego odblokowania karty

Warszawa 2014

Spis treści

1 Cel i zakres dokumentu

Procedura jest instrukcją procesu zdalnej wymiany certyfikatów (zdalna wymiana certyfikatów jest procesem wymiany klucza prywatnego oraz certyfikatu). Dokument zawiera również instrukcję zdalnego odblokowania PIN-u karty.

2 Słownik użytych terminów i zwrotów

W Instrukcji wykorzystywane są nazwy i zwroty, które dla wygody użytkownika zamieszczamy poniżej w formie słownika:

- Karta kryptograficzna – urządzenie przechowujące i zabezpieczające klucze prywatne i certyfikat użytkownika
- System Rejestrów Państwowych (SRP) – w pełni zintegrowany, referencyjny i nowoczesny system mający na celu poprawę jakości danych zgromadzonych w ewidencjach które prowadzi Minister Spraw Wewnętrznych
- Zdalna Recertyfikacja – proces polegający na wystawieniu nowego certyfikatu dla użytkownika, który posiada certyfikat wystawiony przez CC MSW; zdalna recertyfikacja odbywa się za pośrednictwem strony internetowej
- Recertyfikacja (odnowienie, wymiana certyfikatu) – proces polegający na wystawieniu nowego certyfikatu dla użytkownika, który posiada certyfikat wydany przez CC MSW; recertyfikacja odbywa się w Punkcie Rejestracji CC MSW
- Aplikacja ŹRÓDŁO – bezpłatna aplikacja do obsługi rejestrów państwowych służąca do edycji i przetwarzania danych gromadzonych w SRP
- Certyfikat – elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis elektroniczny i które umożliwiają identyfikację tej osoby
- Użytkownik – osoba, dla której wystawiany jest certyfikat w ramach systemu certyfikacji
- Certyfikat przeterminowany – certyfikat, którego termin ważności upłynął oraz nie został on unieważniony
- Certyfikat unieważniony – certyfikat, który został umieszczony na liście certyfikatów unieważnionych (CRL) przed upływem ważności
- Certyfikat ważny (aktualny) – certyfikat, którego termin ważności nie upłynął oraz nie został on unieważniony
- Centrum Certyfikacji MSW (CC MSW) – komórka organizacyjna w MSW, która w ramach swoich obowiązków świadczy usługi certyfikacyjne dla systemów pl.ID oraz SIPR
- Personalizacja (karty kryptograficznej) – czynność składająca się z personalizacji elektronicznej polegającej na wygenerowaniu przez kartę pary kluczy kryptograficznych

i osadzeniu na niej certyfikatu przez CC MSW oraz personalizacji graficznej podczas, której wykonywany jest nadruk na karcie

- Nowa karta (kryptograficzna) – karta, która nie została spersonalizowana
- Java – aplikacja niezbędna do uruchomienia funkcjonalności strony do zdalnej recertyfikacji w przeglądarce Internetowej
- Strona zdalnej recertyfikacji – strona internetowa, na której można przeprowadzić proces zdalnej recertyfikacji, dostępna pod adresem cc.msw.gov.pl

3 Wstęp do procesu recertyfikacji

Karta kryptograficzna umożliwia identyfikację użytkownika w Systemie Rejestrów Państwowych. Oznacza to, że dostęp do gromadzonych w rejestrach informacji można uzyskać tylko po poprawnym przeprowadzeniu autoryzacji z wykorzystaniem właśnie tego narzędzia. Tym samym karta kryptograficzna jest niezbędnym elementem umożliwiającym wzięcie udziału w testach zewnętrznych programu pl.ID, jak również w przyszłym korzystaniu z Systemu Rejestrów Państwowych (SRP) oraz aplikacji ŹRÓDŁO.

Na karcie umieszczony jest certyfikat, wystawiany przez CC MSW na okres nie dłuższy niż 2 lata. Każdy użytkownik chcący korzystać z SRP czy aplikacji ŹRÓDŁO musi posiadać ważny certyfikat na swojej karcie kryptograficznej, dlatego aby móc skorzystać z posiadanej karty niezbędna jest recertyfikacja. Proces ten polega na wystawieniu nowego certyfikatu użytkownika na posiadanej przez niego karcie.

Większość użytkowników posiada karty kryptograficzne, które zostały dostarczone do gmin w ramach projektu pl.ID – polska ID karta w okresie październik 2011 r. – styczeń 2012 r. Karty współpracują z aplikacją ŹRÓDŁO umożliwiając dostęp do Systemu Rejestrów Państwowych (SRP). Posiadacze kart biorący udział w testach i korzystający z zasobów SRP i aplikacji ŹRÓDŁO, będą zobowiązani jedynie do odnowienia certyfikatu, zgodnie z niniejszą instrukcją.

W przypadku osób, których dane osobowe uległy zmianie, CC MSW dopuszcza możliwość zdalnego wydania certyfikatu po przekazaniu poprawnie wypełnionego wniosku zawierającego aktualne dane użytkownika, zgodnie z procedurą z pkt 4.3.

3.1 Wymagania techniczne

Aby procesy realizowane za pomocą strony cc.msw.gov.pl mogły przebiec prawidłowo, użytkownik posiadający kartę kryptograficzną powinien mieć skonfigurowaną przez lokalnego administratora systemu stację roboczą spełniającą poniższe wymagania:

- Stacja PC z systemem operacyjnym Windows XP lub nowszym.
- Jedna z przeglądarek WWW:
    - Internet Explorer,
    - Firefox,
    - Chrome.

- Przeglądarka musi mieć włączoną obsługę Javy.
- W systemie musi być zainstalowana aktualna wersja Javy kompatybilna co do przeglądarki i biblioteki PKCS#11 (32 lub 64 bit). Zaleca się użycie 32 bitowej wersji java jeśli biblioteka PKCS#11 również jest 32 bit.
- W systemie Windows muszą być zainstalowane aktualne sterowniki do obsługi czytnika kart.
- Czytnik kart musi być widoczny w systemie Windows jako rozpoznane i sprawne urządzenie.
- W systemie Windows musi być zainstalowane oprogramowanie producenta kart, zawierające bibliotekę PKCS#11.

3.2 Strona cc.msw.gov.pl

W celu wejścia na stronę zdalnej recertyfikacji, należy w pasku adresu przeglądarki wpisać adres cc.msw.gov.pl. W przypadku pojawienia się monitu związanego z bezpieczeństwem aplikacji Java (poniższy rysunek), należy zezwolić aplikacji na uruchomienie poprzez użycie opcji „Run". Jeżeli użytkownik nie potrzebuje otrzymywać monitu za każdym razem, powinien zaznaczyć opcję „Do not show this again for apps from the publisher and location above".

Rysunek nr 1 - Monit związany z bezpieczeństwem aplikacji Java

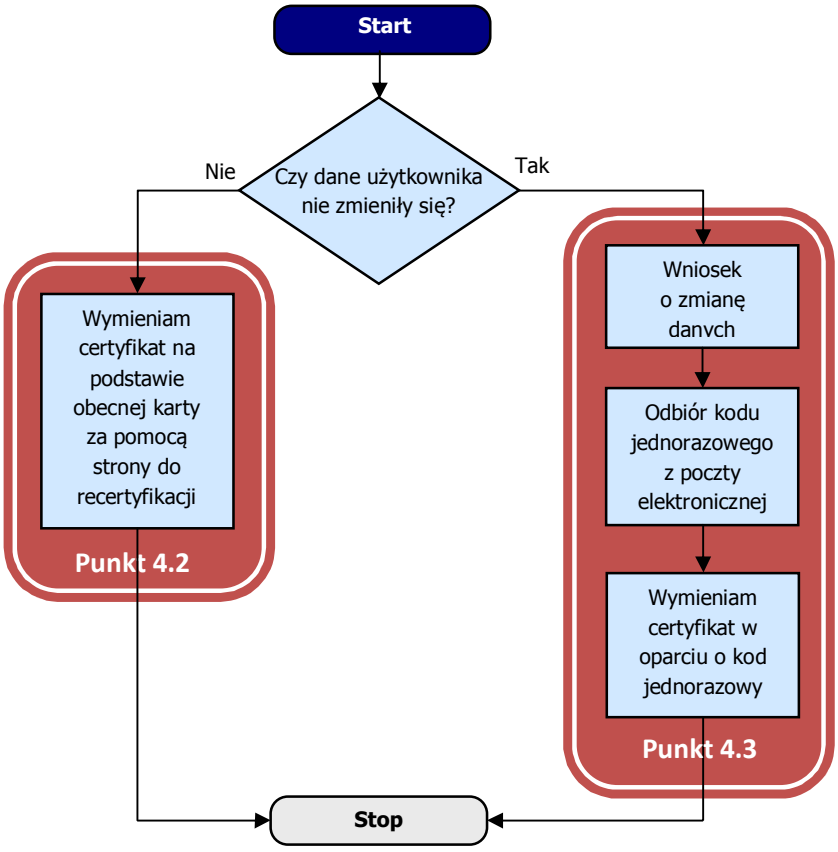
Przed wykonaniem kolejnych kroków należy umieścić posiadaną kartę w czytniku. Czytnik musi być podłączony i zainstalowany w komputerze (skonfigurowanym zgodnie z instrukcją), na którym uruchamiana jest strona do zdalnej recertyfikacji.

W przypadku pojawienia się monitu *Security Warning* (poniższy rysunek) należy zezwolić na podążanie za aplikacją poprzez wybranie opcji *Tak*.

Rysunek nr 2 - Security Warning

4 Proces zdalnej wymiany certyfikatów

4.1 Diagram procesu zdalnej wymiany certyfikatów



Rysunek nr 3 - Algorytm procesu zdalnej wymiany certyfikatu

4.2 Opis procesu zdalnej wymiany certyfikatu

Proces zdalnej wymiany certyfikatu wykonywany jest w następujący sposób:

1. Z poziomu przeglądarki należy wejść na stronę cc.msw.gov.pl. W przeglądarce pojawi się następująca strona.

Rysunek nr 4 - Strona cc.msw.gov.pl

2. Jeśli certyfikat na karcie jest ważny lub przeterminowany, należy użyć opcji „Wymiana certyfikatu na karcie”. Po wybraniu tej opcji pojawi się okno w którym należy podać indywidualny i przekazany użytkownikowi PIN do karty (poniższy rysunek).

Rysunek nr 5 - Okno w którym należy podać PIN

3. Jeśli na karcie znajduje się więcej niż jeden certyfikat, pojawi się okno z wyborem certyfikatu który należy wybrać, aby prawidłowo podpisać żądanie wymiany certyfikatu (poniższy rysunek). Nie należy wyjmować karty z czytnika podczas procesu recertyfikacji. Proces recertyfikacji może trwać kilka minut.

Rysunek nr 6 - Okno z wyborem certyfikatu

4. Prawidłowe zakończenie procesu recertyfikacji zakończy się komunikatem „Operacja zakończona sukcesem” (poniższy rysunek).

Rysunek nr 7 - Prawidłowe zakończenie procesu recertyfikacji

4.3 Opis procesu zdalnej wymiany certyfikatu za pomocą kodu jednorazowego

1. W przypadku kiedy uległy zmianie dane użytkownika należy poprawnie wypełnić *wniosek o dostęp do Systemu Rejestrów Państwowych* oraz przekazać do MSW. Po pozytywnym zweryfikowaniu wniosku CC MSW prześle na adres e-mail kod jednorazowy, który pozwoli na uwierzytelnienie osoby w systemie zdalnej recertyfikacji. Po otrzymaniu kodu na stronie głównej należy wybrać opcję „Generowanie nowych certyfikatów za pomocą kodu jednorazowego" (poniższy rysunek).

Rysunek nr 8 - Strona cc.msw.gov.pl

2. Po wybraniu tej opcji pojawi się okno w którym należy podać PIN do karty (poniższy rysunek).

Rysunek nr 9 - Okno w którym należy podać PIN

3. Następnie należy podać uwierzytelniający kod jednorazowy (poniższy rysunek).

Rysunek nr 10 - Okno w którym należy podać kod jednorazowy

4. Prawidłowe zakończenie procesu recertyfikacji zakończy się komunikatem „Operacja zakończona sukcesem” (poniższy rysunek).

Rysunek nr 11 - Prawidłowe zakończenie procesu recertyfikacji

4.4 Odroczona recertyfikacja

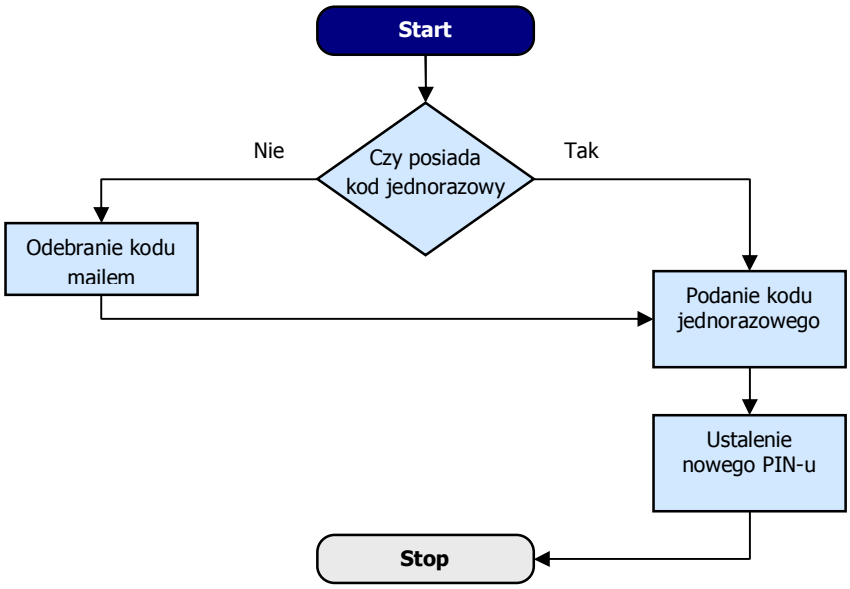
MSW zastrzega sobie możliwość akceptacji procesu zdalnej wymiany certyfikatów. W takim przypadku użytkownik, tuż po rozpoczęciu procesu recertyfikacji (opcja „Wymiana certyfikatów na karcie”), otrzyma informację *Zgłoszenie w trakcie realizacji* (poniższy rysunek).

Rysunek nr 12 - Zgłoszenie w trakcie realizacji

Po zaakceptowaniu przez pracownika MSW wniosku o zdalna recertyfikację przez pracownika MSW, użytkownik otrzyma powiadomienie e-mail o możliwości dokończenia procesu recertyfikacji. Zakończenie procesu odbywa się poprzez ponowne wejście na stronę zdalnej wymiany certyfikatów i wybranie opcji „Wymiana certyfikatów na karcie”.

5 Procedura zdalnego odblokowania karty

5.1 Diagram procesu zdalnego odblokowania



Rysunek nr 13 - Algorytm procesu odblokowania karty

5.2 Opis procesu zdalnego odblokowania

Zdalne odblokowanie karty przeprowadzane jest w sytuacji gdy karta użytkownika została zablokowana lub użytkownik zapomniał PIN.

Odblokowanie karty odbywa się w następujący sposób:

Na żądanie użytkownika zostanie wysłany na jego adres e-mail, zapisany w systemie CC MSW kod jednorazowy. Kod jednorazowy będzie niezbędny w dalszej części procesu odblokowania karty. Jeśli e-mail z kodem jednorazowym nie dotrze do użytkownika, należy skontaktować się z CC MSW w celu potwierdzenia czy zapisany adres e-mail jest poprawny. Podczas procesu odblokowania użytkownik zostanie poproszony o podanie kodu jednorazowego, a w dalszym kroku o dwukrotne podanie kodu PIN jaki będzie ustawiony na karcie.

Aby odblokować kartę należy:

1. Wejść na stronę zdalnego odblokowania karty pod adresem cc.msw.gov.pl (poniższy rysunek).

Rysunek nr 14 - Strona cc.msw.gov.pl

2. Na stronie należy wybrać opcję „Odblokowanie karty”, a następnie potwierdzić odblokowanie karty (poniższy rysunek).

Rysunek nr 15 - Odblokowanie karty

3. Zostanie wyświetlone zapytanie czy użytkownik posiada kod jednorazowy do karty. Aby pozyskać kod jednorazowy na komunikacie (widocznym na obrazku poniżej) należy wybrać opcję *NIE*. Spowoduje to przesłanie na adres e-mail użytkownika kodu jednorazowego (poniższy rysunek).

Rysunek nr 16 - Pobranie kodu jednorazowego

4. Operacja zakończy się komunikatem (poniższy rysunek):

Rysunek nr 17 - Potwierdzenie wysłania kodu jednorazowego

5. Po uzyskaniu kodu jednorazowego, należy ponownie wejść na stronę odblokowania karty, wybrać opcję „Odblokowanie karty” i na pytanie o kod jednorazowy wybrać *Tak*.
6. Następnie należy podać kod jednorazowy otrzymany drogą mailową (poniższy rysunek).

Rysunek nr 18 - Podanie kodu jednorazowego

7. Następnie należy podać nowy PIN do karty (poniższy rysunek). **UWAGA! Pin powinien mieć minimalnie 4 znaki różne od siebie i nie powinien być ujawniany osobom trzecim. Wszystkie działania w systemie są rejestrowane i podpisywane użytym certyfikatem danego użytkownika. Za wszystkie działania w systemie po stronie użytkownika odpowiada osoba, której karta i certyfikat został wykorzystany przy logowaniu i podpisywaniu wykonanych działań. Dlatego należy pamiętać, że nie należy użyczać nikomu swojej karty, a jedyną osoba znającą pin do karty powinien być jej właściciel.**

Rysunek nr 19 - Podanie nowego kodu PIN

8. Prawidłowe zakończenie procesu odblokowania zakończy się komunikatem „Karta odblokowana” (poniższy rysunek).

Rysunek nr 20 - Prawidłowe zakończenie procesu odblokowania

6 Możliwe problemy przy wykonywaniu procedury

- ***Na stronie wyświetla się komunikat „Nie znaleziono czytnika kart. SCardListReaders error: -2146435026 Cannot find a smart card reader.”***

Należy upewnić się, że w systemie operacyjnym czytnik jest poprawnie zainstalowany i widoczny. Należy również wykonać test podłączając czytnik do innej stacji w celu wyeliminowania podejrzeń o uszkodzenie czytnika.

- ***Na stronie wyświetla się komunikat „brak karty”.***

Należy upewnić się czy karta jest prawidłowo włożona do czytnika i sterowniki czytnika i karty są poprawnie zainstalowane. Można również sprawdzić kartę w innym czytniku przy innej stacji, aby wykluczyć lub potwierdzić uszkodzenie karty.

- ***Na stronie wyświetla się komunikat o nierozpoznanym nośniku.***

Należy upewnić się czy system zdalnej recertyfikacji obsługuje dany typ karty oraz czy sterowniki czytnika i karty są poprawnie zainstalowane. Komunikat może również oznaczać trwałe uszkodzenie karty lub problemy z czytnikiem. Proponuje się sprawdzenie karty na innej stacji z innym czytnikiem.

- ***Na stronie wyświetla się komunikat „Wystąpił błąd podczas uwierzytelnienia przed serwerem certyfikacji”.***

Tego rodzaju błąd oznacza, że certyfikat, który jest umieszczony na karcie, jest najprawdopodobniej unieważniony.

- ***Na stronie wyświetla się komunikat „Wystąpił błąd podczas uwierzytelnienia przed serwerem certyfikacji. Użytkownik nie został znaleziony”.***

Taki komunikat oznacza, że dany użytkownik nie figuruje w Urzędzie Certyfikacji. Należy przesłać informację za pośrednictwem poczty elektronicznej na adres centrum.certyfikacji@msw.gov.pl wraz z następującymi danymi: imię i nazwisko, nazwa gminy i kod terytorialny, numer telefonu oraz krótki opis problemu.

- ***Na stronie wyświetla się błąd „Niepoprawny PIN. Ponownie wprowadź PIN”.***

Błąd ten oznacza, że został podany niepoprawny kod PIN do karty.

- ***Na stronie wyświetla się komunikat „Wprowadzony kod jednorazowy jest niepoprawny lub został już wykorzystany”.***

Błąd oznacza, że kod jednorazowy został wykorzystany lub został wprowadzony niepoprawnie. Istnieje możliwość, że CC MSW unieważniło kod w systemie. Jeśli wprowadzony kod jest poprawny i niewykorzystany, należy przesłać informację za pośrednictwem poczty elektronicznej na adres centrum.certyfikacji@msw.gov.pl wraz z następującymi danymi: imię i nazwisko, nazwa gminy i kod terytorialny, numer telefonu oraz krótki opis problemu.

7 Spis ilustracji i tabel