Repozytorium Cyfrowe BN

Instrukcja pozyskiwania certyfikatu oraz importowania certyfikatu osobistego w celu dodatkowej weryfikacji użytkownika podczas logowania do systemu

Spis treści

1. Informacje podstawowe

Aby mieć możliwość poprawnego zalogowania się w systemie Repozytorium Cyfrowe BN dostępnego pod adresem https://do.bn.org.pl użytkownik musi być w posiadaniu następujących danych:

- nazwa użytkownika
- hasło do konta
- certyfikat

Nazwa użytkownika oraz hasło jest definiowane przez użytkownika podczas procesu rejestracji.

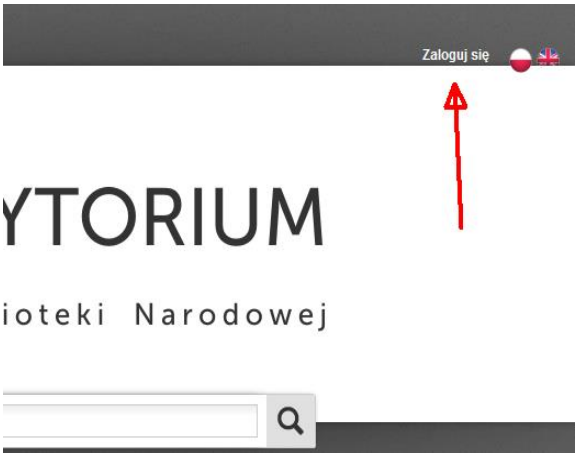
Poza nazwą użytkownika oraz hasłem do konta, aby użytkownik mógł się poprawnie zalogować w systemie, niezbędne jest aby podczas autoryzacji w przeglądarce z której użytkownik korzysta, był poprawnie zainstalowany certyfikat osobisty, który potwierdzi jego tożsamość. Certyfikat ten użytkownik może pobrać ze strony na której znajduje się system Repozytorium Cyfrowe BN czyli https://do.bn.org.pl. Przed przystąpieniem do logowania się w systemie użytkownik zobowiązany jest zatem wykonać procedurę mającą na celu pobranie ważnego na dzień obecny certyfikatu osobistego oraz zaimportowanie otrzymanego certyfikatu w przeglądarce, z której będzie korzystał podczas pracy z systemem Repozytorium Cyfrowe BN. Procedura ta będzie również wymagana za każdym razem kiedy ważność certyfikatu wygaśnie (ważność certyfikatu wynosi 2 lata – okres ważności można sprawdzić w informacjach o certyfikacie po zaimportowaniu certyfikatu).

UWAGA! Szczególne środki ostrożności:

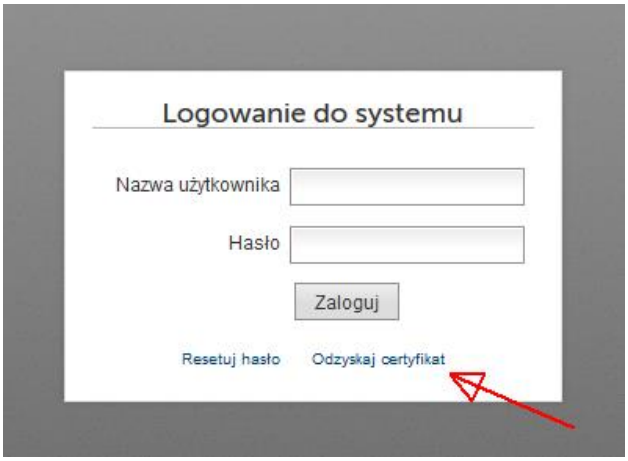
> Hasła do konta nigdy nie należy nikomu przekazywać ani używać w innym miejscu niż ekran logowania do systemu Repozytorium Cyfrowe BN. Podczas procesu resetowania hasła lub pobierania nowej kopii certyfikatu nie jest potrzebne podawanie hasła użytkownika do konta i nie wolno tego robić. Jeżeli zostanie wyświetlona taka prośba wówczas należy zwrócić uwagę czy użytkownik na pewno znajduje się na stronie do.bn.org.pl oraz wysłać powiadomienie do administratora systemu.

1. Pozyskiwanie kopii certyfikatu osobistego (również odnawianie ważności wygasłego certyfikatu)

Aby uzyskać plik z kopią aktualnego certyfikatu osobistego przypisanego do konta użytkownika (również odnowić ważność certyfikatu – uzyskać kopię odnowionego certyfikatu) należy przejść na stronę Repozytorium Cyfrowe BN pod adresem https://do.bn.org.pl gdzie należy wybrać opcję „Zaloguj się" a następnie na formularzu logowania który się wyświetli wybrać opcję „odzyskaj certyfikat".

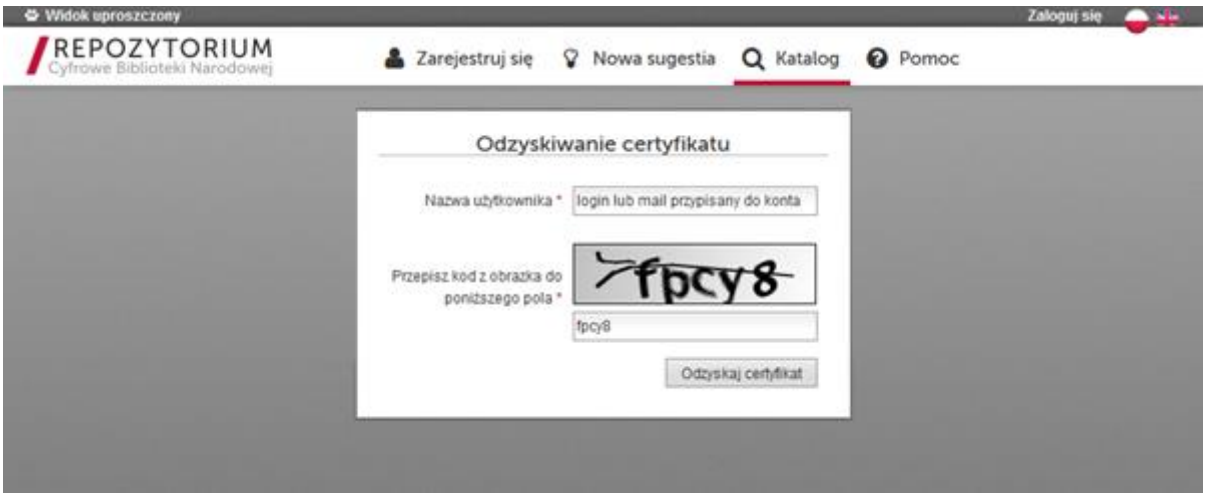


ekran 1: ekran główny RCBN



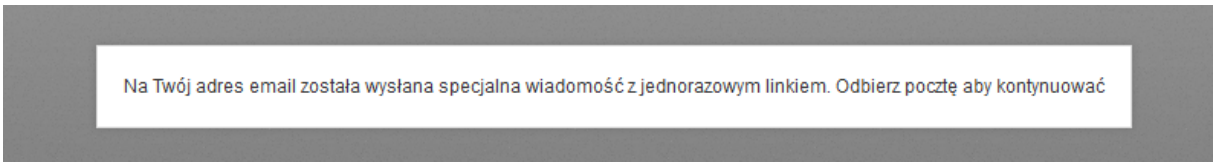
ekran 2: formularz logowania

Po wybraniu tej opcji zostanie wyświetlony formularz na którym w polu „Nazwa użytkownika" należy wpisać login lub mail przypisany do konta natomiast w poniżej obrazka należy przepisać kod z obrazka celem dodatkowej weryfikacji. Po wypełnieniu należy wybrać przycisk „Odzyskaj certyfikat".

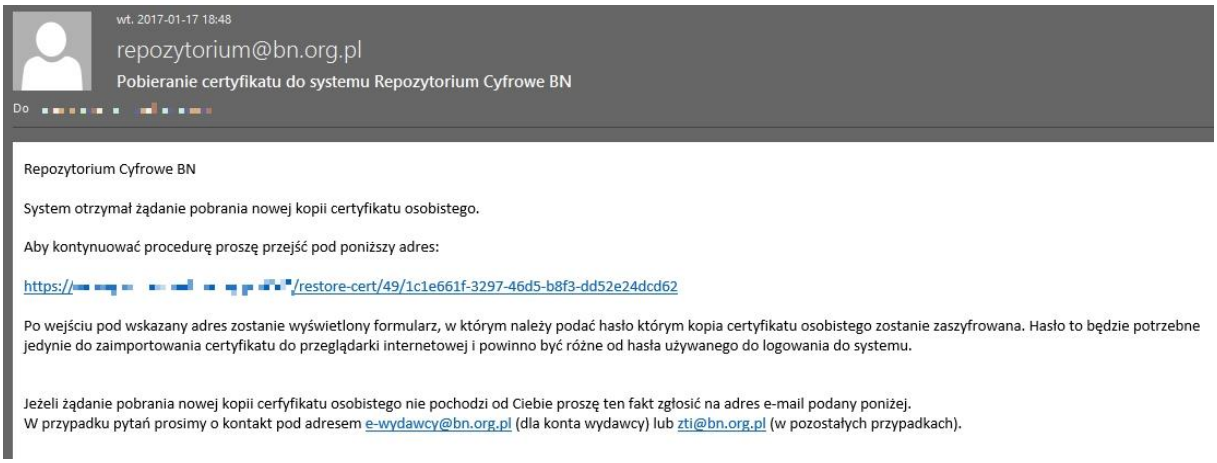


ekran 3: formularz uruchamiania procedury pobierania nowej kopii certyfikatu osobistego

System wyświetli informację potwierdzającą uruchomienie procedury a na mail użytkownika zostanie wysłany link z kodem autoryzacyjnym potwierdzającym dostęp do maila oraz weryfikującym prośbę odzyskania certyfikatu.



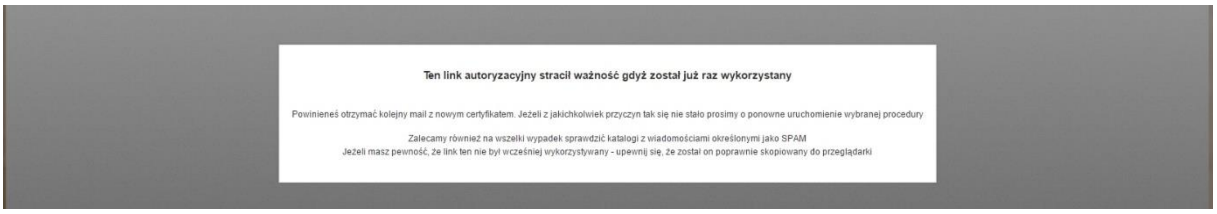
ekran 4: komunikat potwierdzający wysłanie linku z tokenem autoryzacyjnym



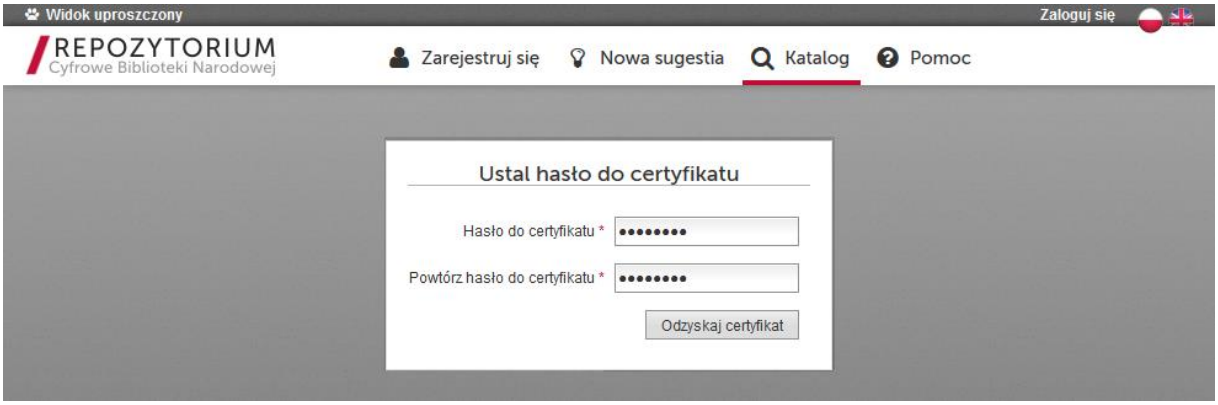
ekran 5: wiadomość e-mail zawierająca link z tokenem autoryzacyjnym

Po otrzymaniu maila z kodem autoryzacyjnym należy przejść pod załączony w mailu link (klikając go lub przeklejając do przeglądarki). Wówczas system wyświetli użytkownikowi formularz do podania hasła do nowej kopii certyfikatu. W tym miejscu nie należy wpisywać hasła do konta, powinno to być nowe hasło i będzie ono potrzebne tylko na czas importowania przysłanego certyfikatu do przeglądarki.

Może się zdarzyć iż link z tokenem autoryzacyjnym nie zostanie rozpoznany przez system – wówczas system wyświetli odpowiednie powiadomienie. W takim przypadku należy zweryfikować czy link nie jest stary lub czy został poprawnie przeklejony do przeglądarki. W ostateczności należy ponownie uruchomić procedurę pozyskiwania nowej kopii certyfikatu zwracając uwagę aby użyć najbardziej aktualnego linku z tokenem autoryzacyjnym który zostanie wysłany na mail.

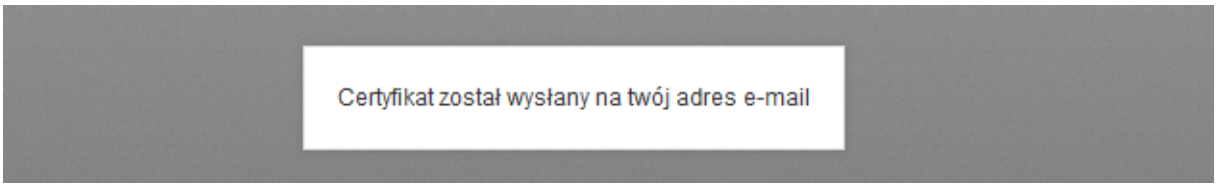


ekran 6: powiadomienie o niepoprawnym linku z tokenem autoryzacyjnym

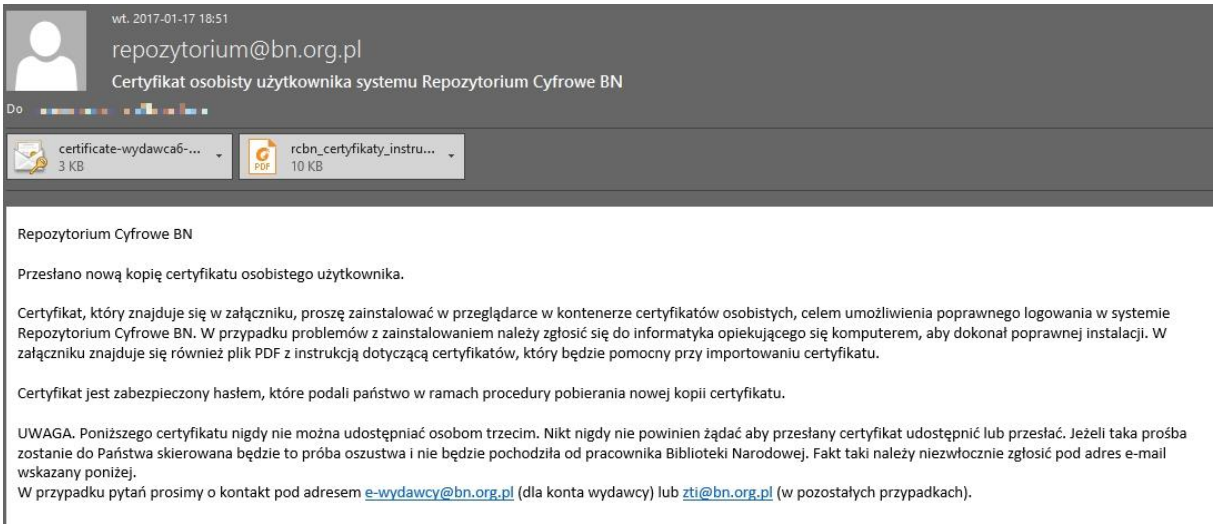


ekran 7: formularz definiowania hasła do nowej kopii certyfikatu

Po wprowadzeniu nowych haseł do certyfikatu użytkownika należy kliknąć przycisk „Odzyskaj certyfikat”. System wyświetli potwierdzenie a na mail powiązany z kontem użytkownika zostanie wysłany plik z kopią ważnego certyfikatu osobistego przypisanego do konta użytkownika.



ekran 8: komunikat o wysłaniu nowej kopii certyfikatu na adres e-mail przypisany do konta


wt. 2017-01-17 18:51

repozytorium@bn.org.pl

Certyfikat osobisty użytkownika systemu Repozytorium Cyfrowe BN

Do [redacted]

certificate-wydawca6-... 3 KB

rcbn_certyfikaty_instru... 10 KB

Repozytorium Cyfrowe BN

Przesłano nową kopię certyfikatu osobistego użytkownika.

Certyfikat, który znajduje się w załączniku, proszę zainstalować w przeglądarce w kontenerze certyfikatów osobistych, celem umożliwienia poprawnego logowania w systemie Repozytorium Cyfrowe BN. W przypadku problemów z zainstalowaniem należy zgłosić się do informatyka opiekującego się komputerem, aby dokonał poprawnej instalacji. W załączniku znajduje się również plik PDF z instrukcją dotyczącą certyfikatów, który będzie pomocny przy importowaniu certyfikatu.

Certyfikat jest zabezpieczony hasłem, które podali państwo w ramach procedury pobierania nowej kopii certyfikatu.

UWAGA. Poniższego certyfikatu nigdy nie można udostępniać osobom trzecim. Nikt nigdy nie powinien żądać aby przesłany certyfikat udostępnić lub przesłać. Jeżeli taka prośba zostanie do Państwa skierowana będzie to próba oszustwa i nie będzie pochodziła od pracownika Biblioteki Narodowej. Fakt taki należy niezwłocznie zgłosić pod adres e-mail wskazany poniżej.
W przypadku pytań prosimy o kontakt pod adresem e-wydawcy@bn.org.pl (dla konta wydawcy) lub zti@bn.org.pl (w pozostałych przypadkach).

ekran 9: wiadomość e-mail z nową kopią certyfikatu osobistego oraz instrukcją importowania

Pozyskany w ten sposób plik kopii certyfikatu osobistego przypisanego do konta użytkownika, należy zaimportować do przeglądarki której użytkownik używał do korzystania z serwisu Repozytorium Cyfrowe BN. Instrukcja instalacji jest opisana w następnym rozdziale.

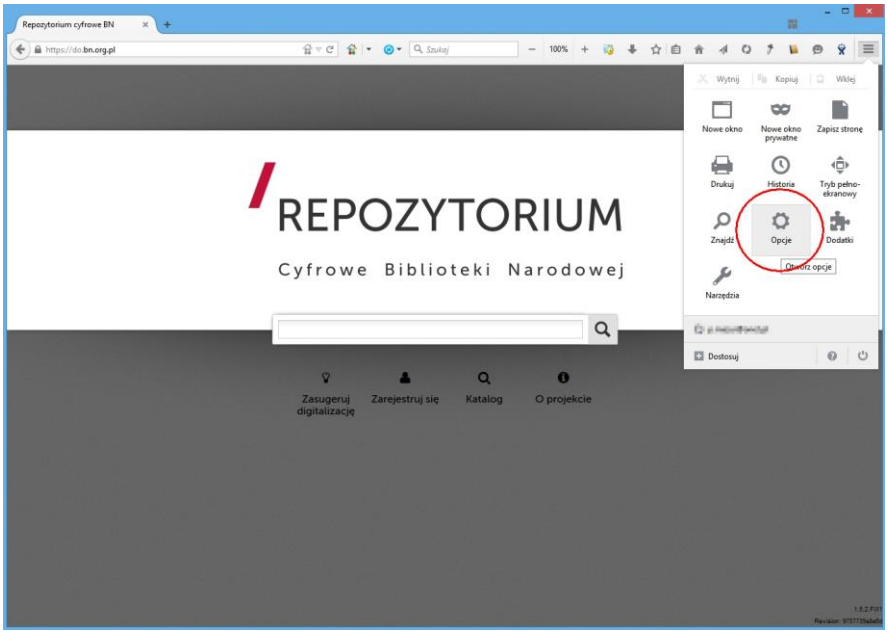
2. Importowanie otrzymanego certyfikatu w przeglądarce

UWAGA: Na wstępie należy zwrócić uwagę, iż w przypadku kiedy w przeglądarce był już zainstalowany certyfikat osobisty powiązany z kontem użytkownika w Repozytorium Cyfrowe BN to rzez zaimportowaniem nowego certyfikatu stary należy usunąć.

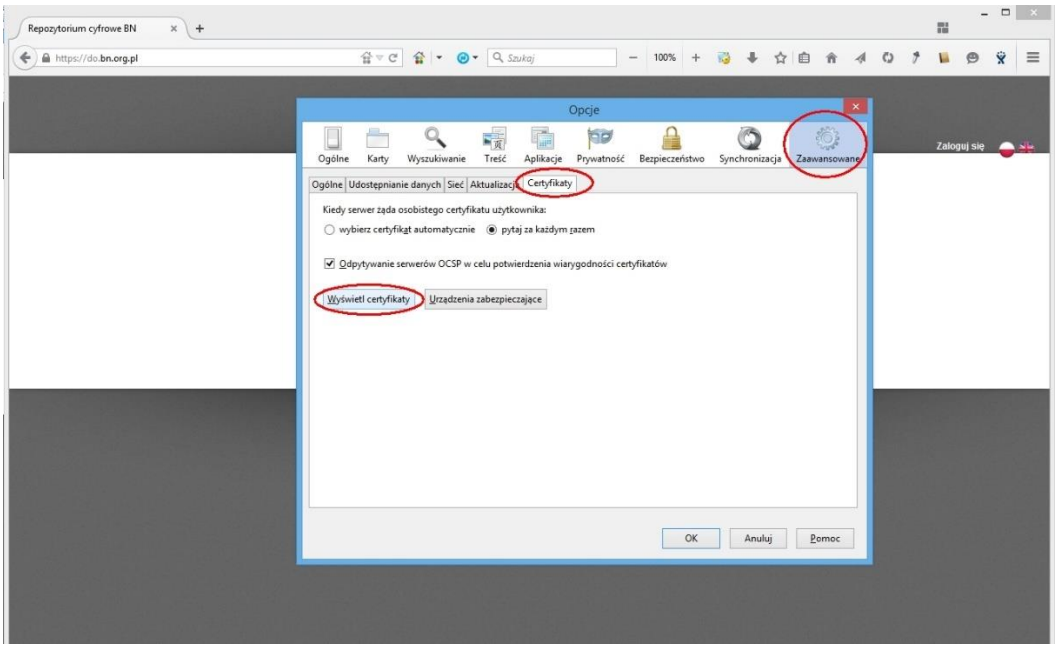
Sposób instalacji jest uzależniony od używanej przeglądarki. Przykład importowania certyfikatu zostanie zaprezentowany w oparciu o trzy najbardziej popularne przeglądarki – w pozostałych przypadkach proces jest analogiczny i różni się tylko dostępnym menu.

2.1. Firefox

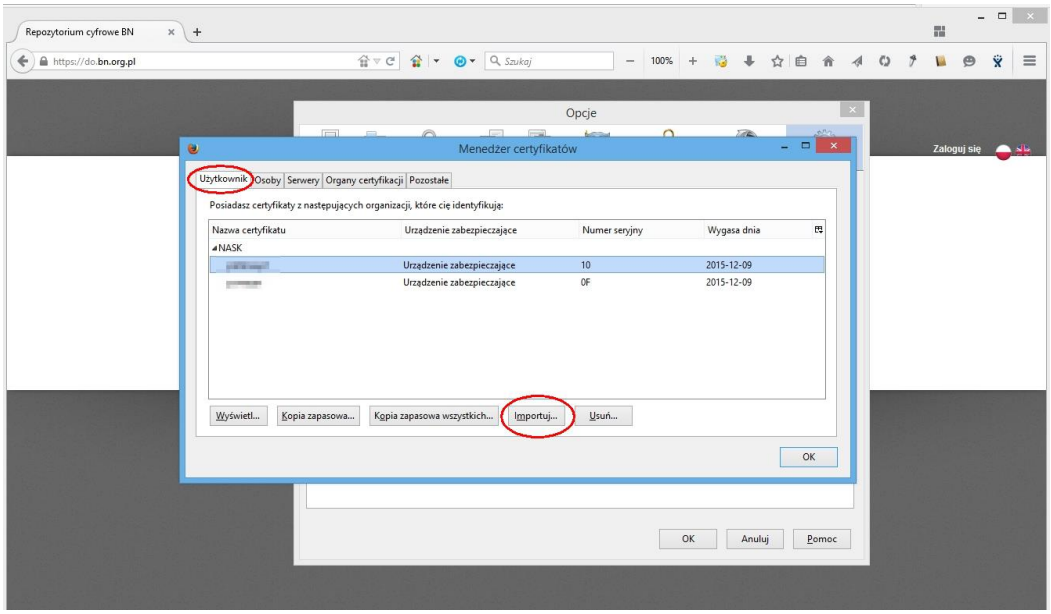
W przypadku tej przeglądarki import należy wykonać tylko poprzez mechanizm Firefoxa ponieważ korzysta on z własnego kontenera certyfikatów i nie zwraca uwagi na certyfikaty zaimportowane w systemie operacyjnym. Import certyfikatu rozpoczynamy od otwarcia ustawień przeglądarki.



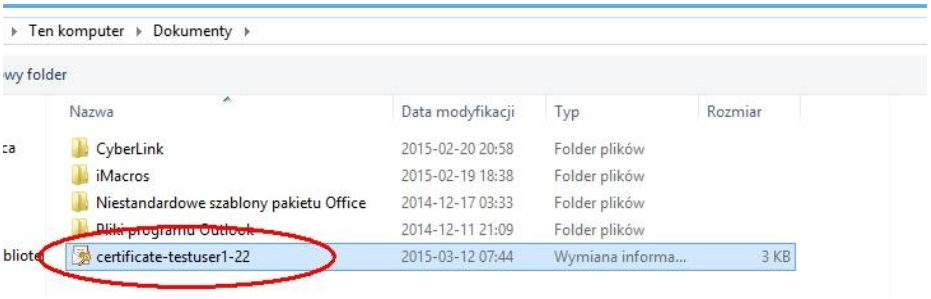
Następnie przechodzimy na zakładkę „Zaawansowane”, na, której wybieramy panel „Certyfikaty” i z tego panelu klikamy przycisk „Pokaż certyfikaty”

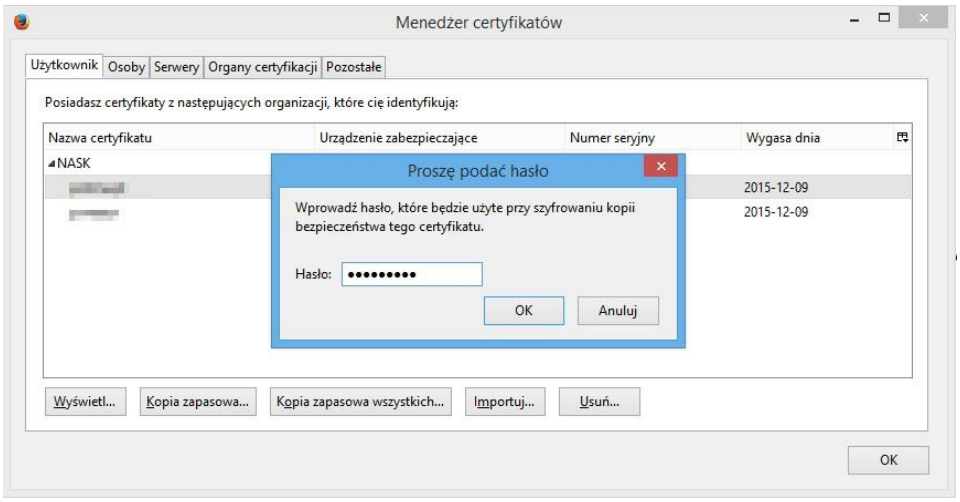


W wyświetlonym oknie wybieramy zakładkę „Użytkownik”. Tutaj wyświetlona jest lista wszystkich certyfikatów osobistych, które użytkownik zaimportował. Zazwyczaj w tym momencie może ona być pusta. Należy wybrać opcję „Importuj” znajdującą się na dole okna.

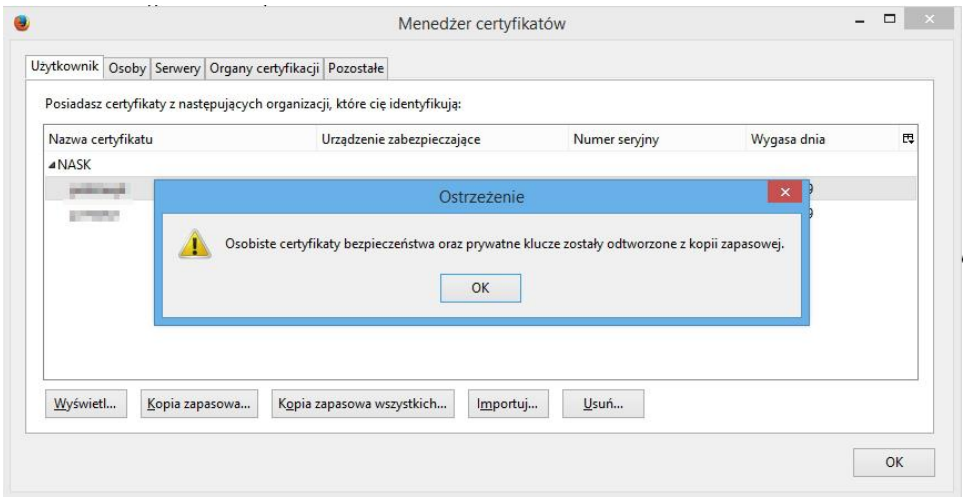


Pojawi się okno z wyborem plików. Należy wskazać plik z certyfikatem, który został dostarczony użytkownikowi. Po wybraniu pliku pojawi się okno umożliwiające wprowadzenie hasła do wybranego certyfikatu.

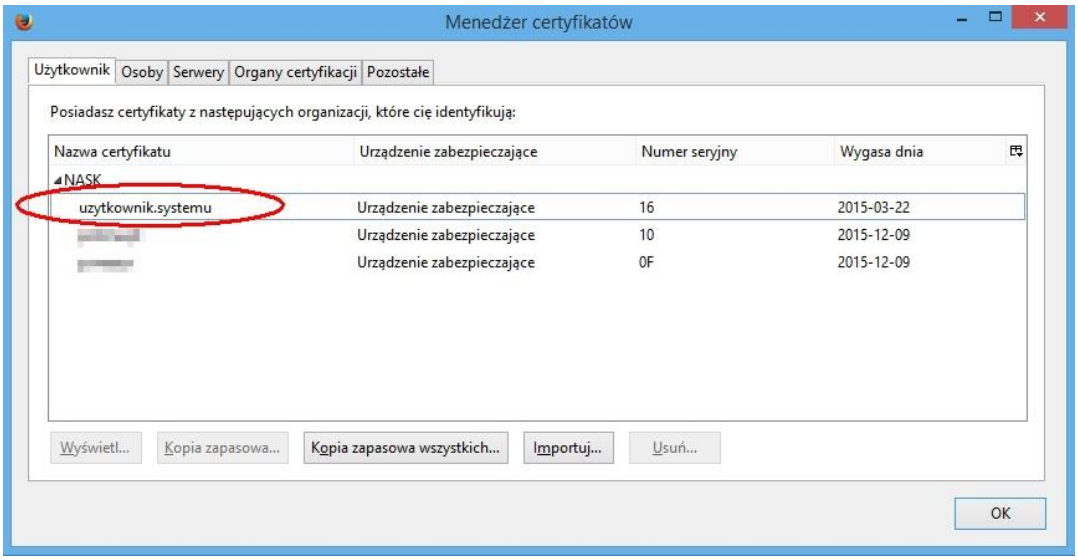




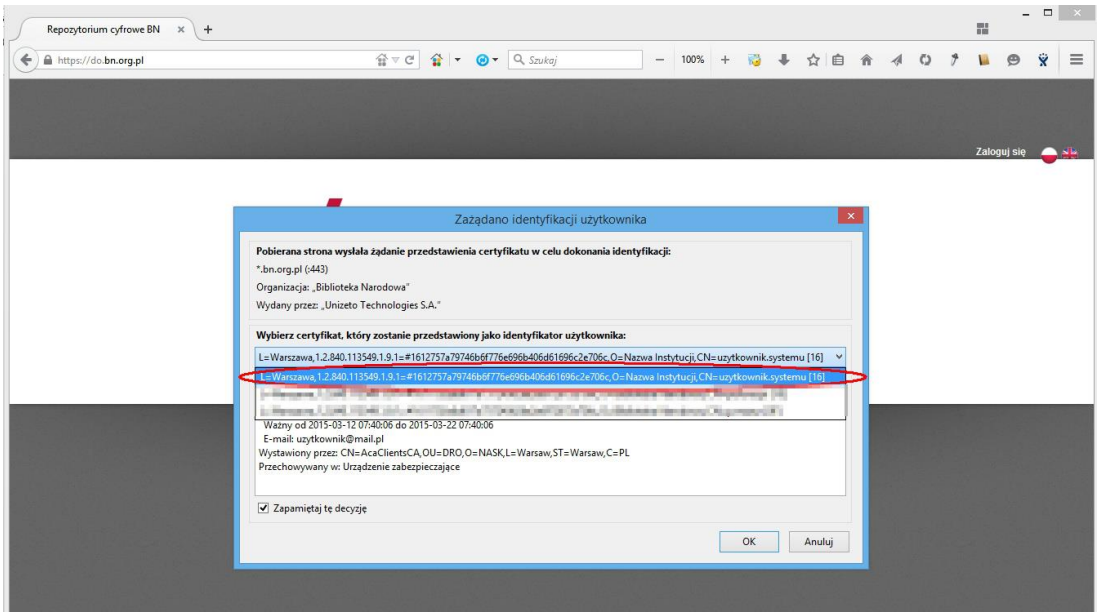
Po wprowadzeniu poprawnego hasła i zatwierdzeniu użytkownikowi powinien pojawić się komunikat informujący o poprawnym zaimportowaniu certyfikatu.



Po poprawnym zaimportowaniu na liście certyfikatów będzie widoczny nowo zaimportowany certyfikat



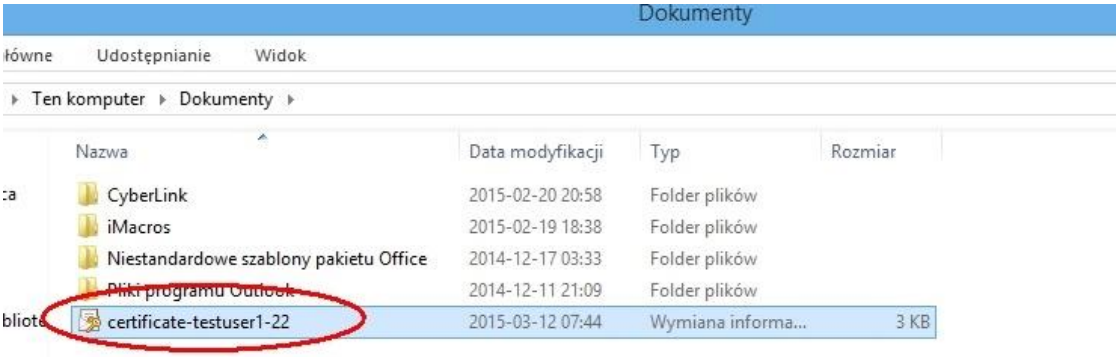
W dalszym kroku należy zrestartować przeglądarkę a następnie można zalogować się do systemu. Podczas logowania zostanie wyświetlony monit, w którym należy wskazać właściwy certyfikat do autoryzacji dla danego użytkownika. W przypadku, kiedy użytkownik ma zaimportowany tylko jeden certyfikat nie będzie trzeba nic dodatkowo wybierać, ponieważ właściwy certyfikat będzie już wybrany domyślnie i wystarczy wówczas potwierdzić wybór poprzez naciśnięcie przycisku kliknąć „ok”.



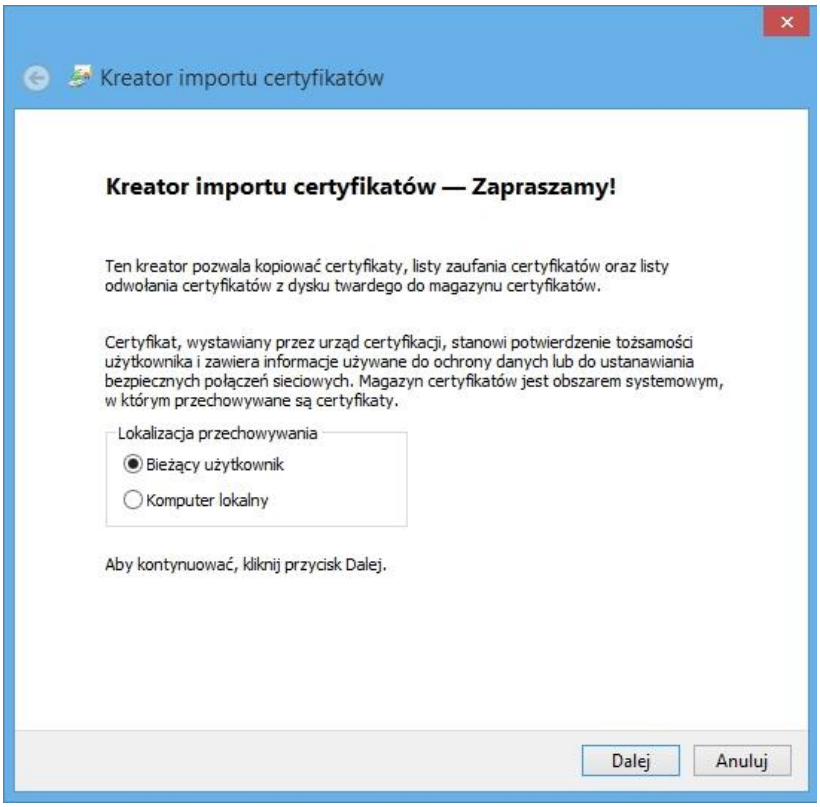
Można rozpocząć pracę w systemie.

2.2. Chrome/Internet Explorer

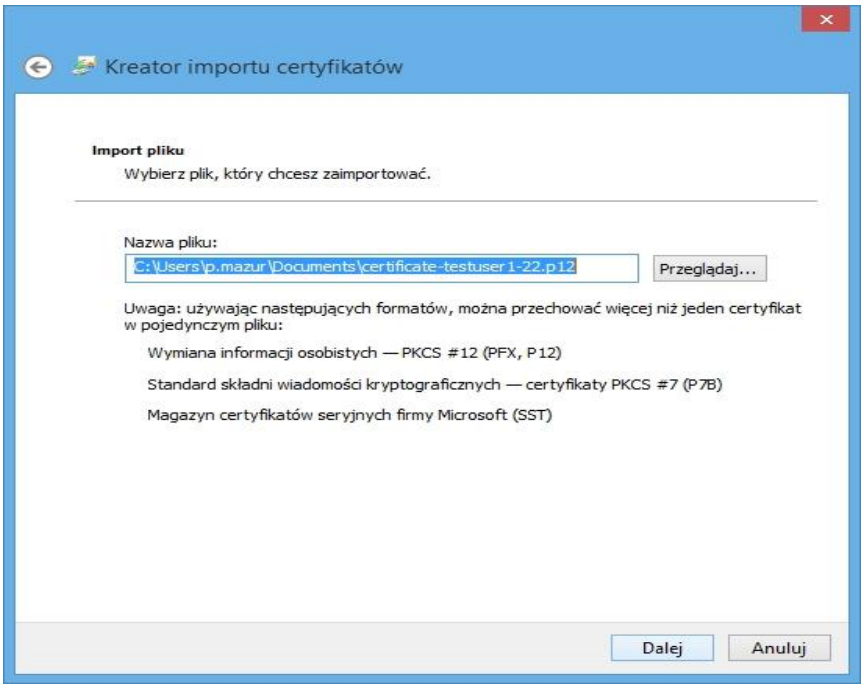
W odróżnieniu od przeglądarki Firefox w przypadku Chrome i Internet Explorera certyfikat można zaimportować za pomocą systemu.
Przechodzimy do katalogu, w którym znajduje się dostarczony certyfikat i rozpoczynamy jego importowanie poprzez dwukrotne kliknięcie pliku z certyfikatem.



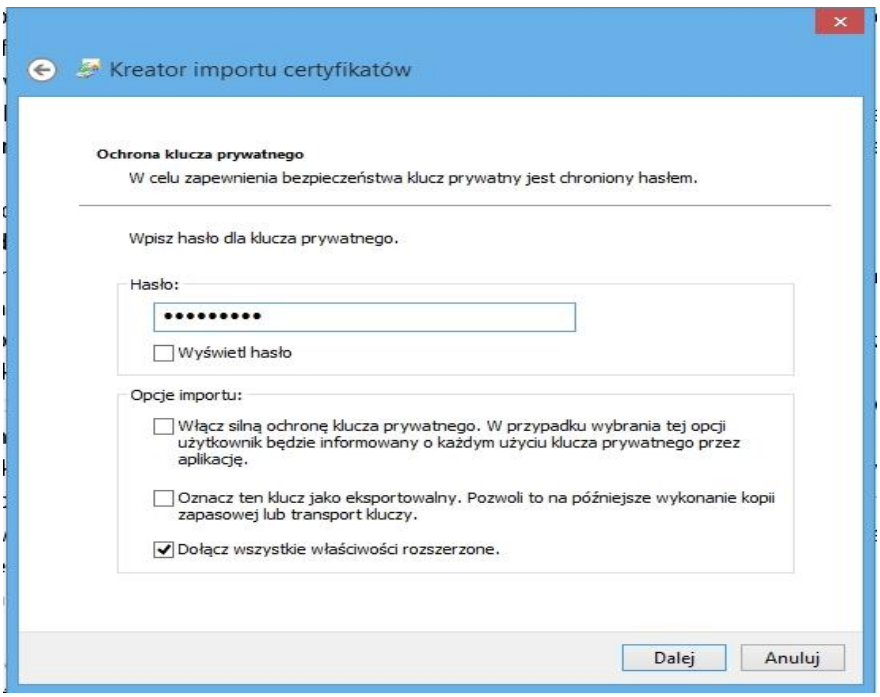
Pojawi się kreator importu certyfikatu (wygląd i układ okienek może się różnić w zależności od wersji systemu operacyjnego). Wybieramy opcję „Bieżący użytkownik” i klikamy „dalej”.



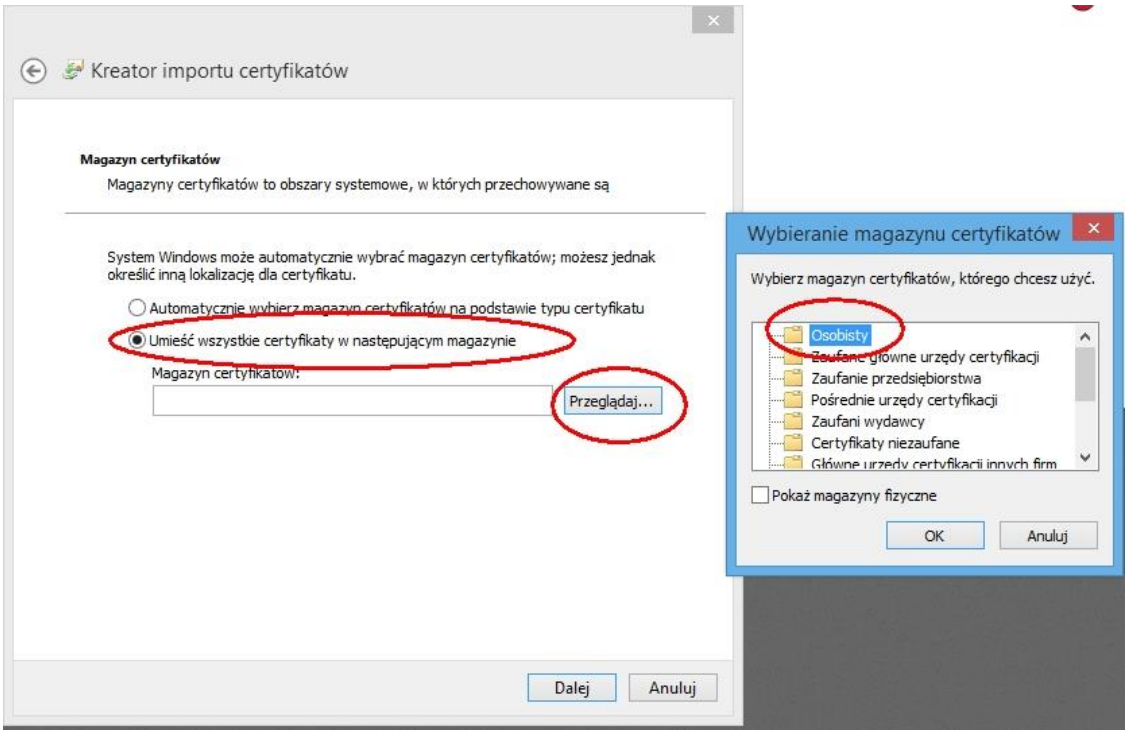
W następnym oknie kreator wyświetli ścieżkę pliku, który został wybrany – klikamy „dalej”.



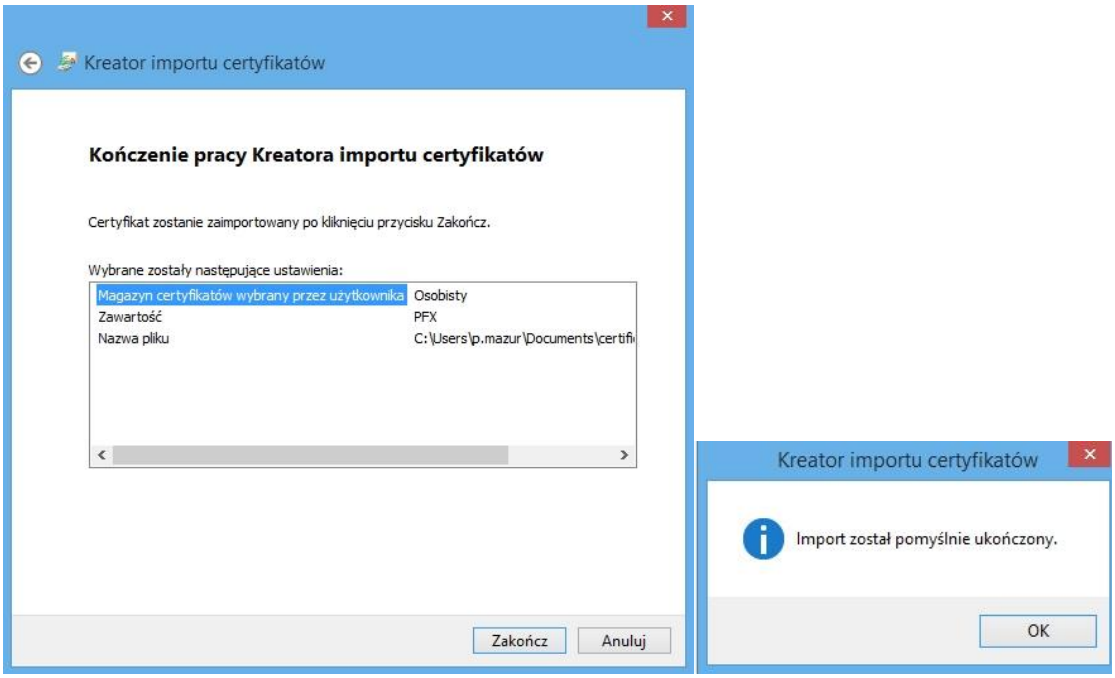
W kolejnym kroku podajemy hasło do certyfikatu oraz ustawiamy opcje dodatkowe zgodnie z poniższym ekranem:



Wybieramy opcję „Dalej” a na następnym ekranie opcję „umieść wszystkie certyfikaty w następującym magazynie”. Klikamy „przeglądaj” i wybieramy opcję „osobisty”. Klikamy „ok” i „dalej”.



Proces importowania został zakończony. Wybieramy opcję „zakończ”.



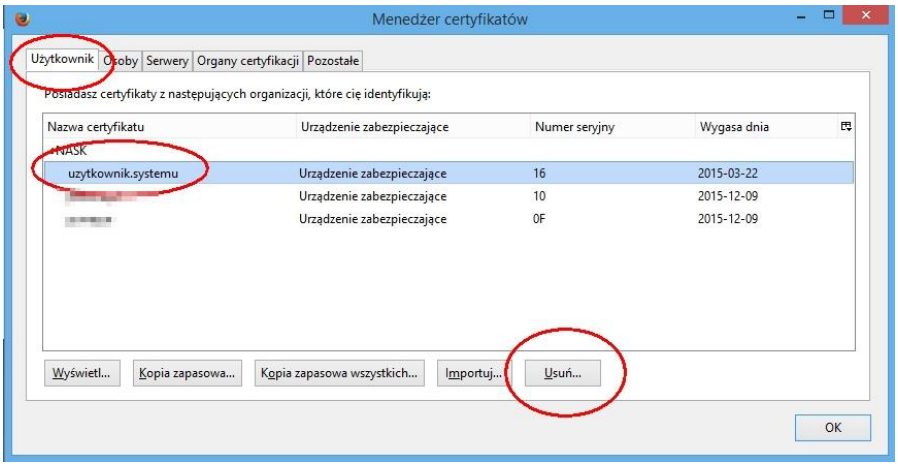
Jeżeli przeglądarka była otwarta to należy ją zrestartować.

3. Usuwanie certyfikatu któremu upłynął termin ważności

Każdy certyfikat ma ustawioną datę ważności, po której staje się nieaktualny i zalogowanie do systemu przy jego pomocy będzie niemożliwe. W takiej sytuacji, jeżeli konto użytkownika będzie nadal aktywne zostanie mu przysłany nowy aktualny certyfikat osobisty. W takiej sytuacji proces instalacji certyfikatu należy powtórzyć. Jednakże należy ten proces poprzedzić wówczas usunięciem starego certyfikatu.

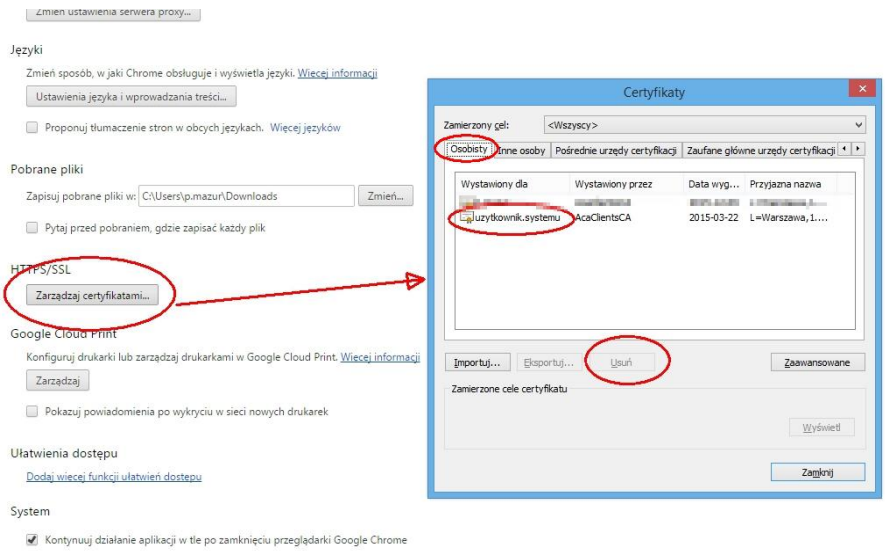
3.1. Firefox

W przypadku przeglądarki FF należy zgodnie z instrukcją importu przejść do listy certyfikatów użytkownika. Na tej liście zaznaczamy certyfikat, który jest nieaktualny (przy każdym wpisie jest data ważności) i wybrać opcję usuń.



3.2. Chrome

Należy wejść w ustawienia przeglądarki, w ustawieniach na samym dole wybrać opcję „Pokaż ustawienia zaawansowane”, po czym odnaleźć i wybrać opcję „Zarządzaj certyfikatami”. Wyświetli się okienko z listą certyfikatów. Przechodzimy na zakładkę „Osobisty” gdzie znajduje się lista certyfikatów osobistych. Zaznaczamy nieważny certyfikat osobisty używany do logowania w repozytorium i wybieramy opcję usuń. Po tej operacji należy zrestartować przeglądarkę.



3.3. Internet Explorer

Należy wybrać menu ustawień i wskazać pozycję „Opcje internetowe”. Przechodzimy na zakładkę zawartość i wybieramy opcję „Certyfikaty”. Wyświetli się okienko z listą certyfikatów. Przechodzimy na zakładkę „Osobisty” gdzie znajduje się lista certyfikatów osobistych. Zaznaczamy nieważny certyfikat osobisty używany do logowania w repozytorium i wybieramy opcję usuń. Po tej operacji należy zrestartować przeglądarkę.