



KOMISJA
NADZORU
FINANSOWEGO

ABC PORTALU KNF

**System PORTAL KNF – Informacje
podstawowe**

oraz

Najczęściej zadawane pytania

Wersja 1.4

30-01-2021

Spis treści

1 Informacje podstawowe dotyczące systemu Portal KNF	3
1.1 Wstęp	3
1.2 Materiały związane z systemem Portal	3
1.3 Obszary merytoryczne	3
1.4 Role	5
2 Trzy podstawowe funkcjonalności w Portalu:	5
2.1 Rozmowa (Wiadomość).....	5
2.2 Artykuł	6
2.3 Ankieta	6
4 Najczęściej zadawane pytania dotyczące Portalu KNF	7
A. CZYM JEST PORTAL I NA JAKICH ZASADACH FUNKCJONUJE	7
B. CERTYFIKATY CYFROWE.....	8
C. UPRAWNIENIA, KONTA, ADMINISTRACJA.....	9
D. PROBLEMY TECHNICZNE I MERYTORYCZNE.....	10
Załącznik nr 1 Przykłady Instalacji certyfikatów softwareowych w popularnych przeglądarkach internetowych	12

1 Informacje podstawowe dotyczące systemu Portal KNF

1.1 Wstęp

Portal KNF jest systemem do bezpiecznej i szybkiej wymiany informacji UKNF z podmiotami nadzorowanymi, Bankowym Funduszem Gwarancyjnym oraz Powiernikami banków hipotecznych.

Podstawą przekazywania informacji w ramach Portalu KNF jest obustronne podpisanie *Umowy na korzystanie z Portalu KNF* lub zaakceptowanie przez UKNF wniosku o dostęp do Portalu KNF w celu realizacji prawnego obowiązku przekazywania określonego rodzaju informacji za pomocą systemu teleinformatycznego.

Zasady dostępu i korzystania z wymiany informacji poprzez Portal KNF, wyłączenia z zakresu przekazywanych informacji, zasady administrowania Portalem oraz zasady ochrony przetwarzanych informacji określa *Regulamin korzystania z Portalu KNF*.

1.2 Materiały związane z systemem Portal

UKNF przygotował następujące materiały związane z systemem Portal:

1. Instrukcję obsługi systemu Portal dla użytkownika merytorycznego podmiotu nadzorowanego
2. Instrukcję obsługi systemu Portal dla administratora podmiotu nadzorowanego
3. Wytyczne dotyczące zasad bezpiecznego przechowywania certyfikatów.

1.3 Obszary merytoryczne

W systemie Portal podmiot nadzorowany może mieć dostęp do różnych obszarów merytorycznych:

OBSZARY MERYTORYCZNE	Przykładowy opis obszaru
Regulacje nadzorcze	Publikacja interpretacji przepisów, w tym z dziedziny rachunkowości, regulacji, zapytań do uchwał i wydanych rozporządzeń oraz kwestii związanych z Instrukcją do sprawozdawczości FINREP i COREP.
Nadzór analityczny	Publikacja pism, ankiet, zbiorczych analiz, raportów nt. sektora, wszelakich raportów innych instytucji, które są ważne dla danej grupy podmiotów. Wyjaśnianie informacji o rozbieżnościach w raportach. Publikacje związane z BION.
Inspekcje i kontrole	Publikacja materiałów związanych z inspekcją w podmiotach nadzorowanych, za wyjątkiem inspekcji odnoszących się do ochrony klientów.

Licencjonowanie	Publikacje związane ze zmianą regulacji wewnętrznych i zakresu działalności podmiotów. Dodatkowo wszelkie zmiany związane ze zmianami warunków jakie były podstawą do wydania licencji.
Pozostałe zezwolenia i zgody	Publikacje związane z pozostałymi zgodami i zezwoleniami, nie obejmujące zakresem obszaru licencjonowania (np. walidacja, zmiany w sposobie wyliczania wymogu kapitałowego).
EKZ i znaczące zaangażowania	Publikacje związane z EKZ i znaczącymi zaangażowaniami.
Obrót na rynku regulowanym	Publikacje związane z działalnością podmiotu w zakresie obrotu papierami na rynku regulowanym.
Nadzór uzupełniający	Publikacja pism, ankiet, zbiorczych analiz, raportów związanych z działaniem konglomeratu finansowego, które będą wymieniane z podmiotem nadzorowanym przez KNF pełniącym wiodącą rolę w konglomeracie finansowym.
Praktyki Rynkowe	Publikacje związane ze skargami składanymi na działalność podmiotów nadzorowanych przez KNF.
Sprawozdawczość	Obszar wykorzystywany w procesie przekazywania sprawozdawczości Powszechnych Towarzystw Emerytalnych
BFG Banki komercyjne/Banki Spółdzielcze/ SKOKI/Firmy inwestycyjne	Wymiana korespondencji w ramach odrębnych obszarów przeznaczonych do wymiany korespondencji między departamentami UKNF, sprawującymi nadzór nad podmiotami i BFG
AML/CFT	Publikacje dotyczące tematyki AML/CFT oraz zbierania danych statystycznych do Krajowej Oceny Ryzyka (NRA);
Wymiana informacji na potrzeby współpracy międzynarodowej	Wymiana informacji dotyczących historii transakcji na rachunkach bankowych
Postępowania korespondencja	Korespondencja związana z realizacją zadań obejmujących czynności sprawdzające dotyczących naruszeń przepisów karnych ustaw rynku finansowego i w związku z czynami skierowanymi przeciwko interesom uczestników rynku finansowego.
Działalność z art. 70.2 uoif	Korespondencja z bankami, które mogą bez zezwolenia prowadzić działalność maklerską oraz świadczyć niektóre usługi maklerskie na podstawie art. 70 ust. 2 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U z 2020 r. poz. 89 z późn. zm.), zwanej dalej "uoif".
Pośrednicy hipotecznego kredytu	Korespondencja z kredytodawcami w celu wykonywania bieżących czynności nadzorczych.

1.4 Role

W kontaktach z UKNF podmiot nadzorowany może występować w różnych rolach w zależności od tego, w zakresie jakiego rynku jest nadzorowany. W Portalu zdefiniowane są następujące role:

- Bank
- Depozytariusz
- Firma inwestycyjna
- Emitent
- Towarzystwo funduszy inwestycyjnych/Fundusz inwestycyjny
- SKOK
- KIP
- BFG
- SWI
- Operator usług kluczowych
- Powiernik
- Dystrybutor ubezpieczeń

Obszary merytoryczne i role służą do adresowania informacji publikowanej tj. rozmowy/wiadomości, artykułu i ankiety do określonej grupy uprawnionych odbiorców zarówno po stronie podmiotu jak i UKNF.

Użytkownik z podmiotu nadzorowanego może zaadresować publikację do UKNF tylko w ramach posiadanych uprawnień do wskazanych obszarów merytorycznych i ról, które otrzymał od Administratora Portalu w podmiocie.

2 Trzy podstawowe funkcjonalności w Portalu:

Aktualnie w Portalu KNF dostępne są trzy podstawowe funkcjonalności: rozmowy, artykuły i ankiety.

2.1 Rozmowa (Wiadomość)

Rozmowa – jest adresowana do jednego podmiotu. Z wyjątkiem wiadomości informacyjnych, UKNF oczekuje odpowiedzi ze strony podmiotu na przesłaną wiadomość.



Przykłady wiadomości:

Styl i forma pisania treści Wiadomości w Portalu będą analogiczne do pism wytwarzanych w UKNF w formie papierowej.

2.2 Artykuł

Artykuł – jest jednostronną publikacją UKNF adresowaną do wielu podmiotów. Na artykuł UKNF nie oczekuje odpowiedzi podmiotu, z wyjątkiem sytuacji, gdy Urzędowi zależy na poznaniu opinii podmiotów np. na temat zmian regulacji nadzorczych. Możliwość zadania zapytania do artykułu przez podmiot jest opcjonalna.



Przykłady artykułów

Styl i forma pisania treści Artykułów w Portalu będą analogiczne do pism wytwarzanych w UKNF w formie papierowej.

2.3 Ankieta

Ankieta – jest publikacją UKNF adresowaną do wielu podmiotów. UKNF oczekuje odpowiedzi ze strony podmiotu na przesłaną ankietę w formacie i czasie określonym w ankiecie.



Przykłady ankiet

Publikowaneankiety w Portalu będą dotyczyły zebrania informacji z obszarów działalności podmiotów, które są przedmiotem szczególnego zainteresowania UKNF.

4 Najczęściej zadawane pytania dotyczące Portalu KNF

A. CZYM JEST PORTAL I NA JAKICH ZASADACH FUNKCJONUJE

1. Czy komunikacja przez Portal KNF ma charakter oficjalny?

Wymiana informacji pomiędzy UKNF a podmiotami nadzorowanymi z wykorzystaniem systemu teleinformatycznego Portal KNF ma charakter oficjalny.

2. Czy publikowane przez podmiot dokumenty trafiają do konkretnych osób merytorycznych, czy np. do sekretariatów?

Publikowane przez podmiot dokumenty trafiają do osób z UKNF, które mają nadane odpowiednie uprawnienia do systemu Portal KNF.

3. Czy system Portal KNF jest to ESPI- bis? Czy system Portal KNF zastąpi system ESPI?

System Portal KNF nie zastępuje systemu ESPI. Działa niezależnie od systemu ESPI. Obowiązek oraz zakres przesyłania dokumentów przez system ESPI wynika z odrębnych przepisów prawa.

4. Czy istnieją zalecenia co do prezentacji graficznej rozmów (wiadomości) /artykułów/ankiet?

Tekst w Portalu UKNF należy pisać zawsze od lewej strony (w tym wszelkie nagłówki, oznaczenie adresatów pisma), jest to zasada konieczna w celu umożliwienia wykonania poprawnego wydruku odbiorcy informacji.

Informacje formalne przekazywane za pośrednictwem Portalu, które mają być uznane za skutecznie doręczone, powinny zawierać w treści, oprócz załącznika w postaci skanu dokumentu, tekst dokumentu. Tekst ten winien być umieszczony bezpośrednio w treści wiadomości.

5. Co będzie wysyłane jako artykuł?

Styl i forma pisania treści Artykułów w Portalu będą analogiczne do pism wytwarzanych w UKNF w formie papierowej. Przykłady zostały umieszczone w tabelach w rozdziale 3.

6. Podmiot wysłał wiadomość z błędnie załączonym plikiem. Czy można usunąć wiadomość z systemu?

Nie można. Należy wysłać ponownie wiadomość z wyjaśnieniem i poprawnym plikiem.

7. Czy jest ograniczenie na wielkość przesyłanego załącznika?

W systemie ustawione jest ograniczenie do 100MB na rozmiar pojedynczego pliku załącznika oraz ograniczenie do max 10 takich plików możliwych do załączenia do jednej informacji którą możemy opublikować. Łącznie zatem możemy poprzez załącznik przesłać w jednej publikacji nie więcej niż 1 GB danych.

Aby załączyć pliki w systemie Portal KNF, należy wybrać w menu Ustawienia użytkownika **Standardowy mechanizm przeglądarki** przy wyborze sposobu przesyłania plików.

8. Co będzie w sytuacji, gdy czas sesji skończy się, a użytkownik będzie w trakcie udzielania odpowiedzi np. plik będzie w trakcie wysyłania?

W systemie zaimplementowany jest specjalny zegar odmierzający przybliżony czas do zakończenia sesji, dodatkowo użytkownik jest ostrzegany odpowiednim komunikatem na ekranie o zbliżającym się czasie końca sesji, jednakże są to mechanizmy informacyjne.

Jeśli użytkownik redaguje informację i potrzebuje więcej czasu, aby nie utracić wprowadzonych zmian powinien skorzystać z przycisku „Zapisz” powodującego zapis wprowadzonych do tej pory informacji do bazy danych oraz przedłużenie/odnowienie czasu do zakończenia sesji.

W przypadku gdy użytkownik przesyła plik znacznych rozmiarów może się zdarzyć, że czas odmierzany przez wspomniany zegar upłynie, jednakże w tym przypadku nie należy się tym przejmować gdyż sama sesja z serwerem jest podtrzymywana przez mechanizm przesyłania pliku.

B. CERTYFIKATY CYFROWE

Certyfikaty cyfrowe: w taki sposób umownie określone są w ABC Portalu nowe certyfikaty udostępniane przez Portal KNF.

9. Czym są certyfikaty cyfrowe?

Certyfikaty cyfrowe przekazywane są za pośrednictwem Portalu. Może je pobrać z Portalu administrator Portalu w podmiocie. Wyjątkiem jest pierwszy certyfikat dla pierwszego administratora podmiotu oraz certyfikat dla administratora podmiotu wydawany w przypadku wygaśnięcia/unieważnienia wszystkich certyfikatów administratorów podmiotu.

10. Jaki jest okres ważności certyfikatów do logowania do systemu?

1 rok. Po upływie tego okresu wystawiony certyfikat traci swoją ważność. Celem wydania nowego certyfikatu należy wystawić żądanie certyfikatu w aplikacji Portal.

12. Czy system Portal będzie powiadamiał o terminie wygaśnięcia certyfikatu? Tak, na 30 dni przed upływem terminu ważności certyfikatu będą wysyłane powiadomienia mailowe.

13. Jak uzyskać pierwszy certyfikat pierwszego administratora podmiotu?

Przyznanie uprawnień pierwszego administratora podmiotu, założenie konta i wydanie certyfikatu następuje na wniosek podmiotu nadzorowanego, złożony na formularzu stanowiącym załącznik nr 2 do Regulaminu Portalu KNF i podpisany zgodnie z zasadami reprezentacji Podmiotu Nadzorowanego.

14. Czy sposób autoryzacji przy użyciu certyfikatów cyfrowych jest bezpieczny?

Autoryzacja przy użyciu certyfikatów cyfrowych jest bezpieczna. Całe rozwiązanie zostało poddane audytowi bezpieczeństwa przeprowadzonemu przez zewnętrzną firmę zgodnie z zaleceniami OWASP.

15. Czy zainstalowany w przeglądarce certyfikat cyfrowy można zabezpieczyć hasłem/pinem aby zabezpieczyć go przed nieuprawnionym użyciem

Tak certyfikat można dodatkowo zabezpieczyć, jednak funkcjonalność ta jest wbudowana w system operacyjny lub przeglądarkę internetową i w zależności od tego sposób zabezpieczenia może się różnić. W załączniku nr 1 zamieszczone zostały przykłady instalacji certyfikatów cyfrowych na trzech najbardziej popularnych przeglądarkach internetowych pracujących w środowisku Windows wraz ustawieniem ww. zabezpieczeń.

C. UPRAWNIENIA, KONTA, ADMINISTRACJA

20. Jaka jest dopuszczalna liczba użytkowników merytorycznych w Podmiocie? Zakłada się, że grupa użytkowników merytorycznych w Podmiocie nie powinna przekraczać liczby 2. W uzasadnionych przypadkach Podmiot Nadzorowany może wystąpić z wnioskiem o zwiększenie liczby użytkowników merytorycznych.

21. Jaka jest dopuszczalna liczba administratorów Portalu w Podmiocie

Zakłada się, że grupa administratorów Portalu w Podmiocie nie powinna przekraczać liczby 2. W uzasadnionych przypadkach Podmiot Nadzorowany może wystąpić z wnioskiem o zwiększenie administratorów Portalu w Podmiocie.

22. Z uwagi na ograniczoną liczbę użytkowników dedykowanych dla podmiotu, czy jest możliwość stworzenia w Portalu użytkowników o bardzo wąskim zakresie uprawnień, którzy logowaliby się bez certyfikatów?

Nie ma takiej możliwości. Każdy użytkownik z podmiotu musi logować się do Portalu za pomocą certyfikatu.

23. Czy administrator Portalu w Podmiocie może być użytkownikiem merytorycznym?

Tak, ale musi posiadać osobne konto i osobny certyfikat udostępniony przez UKNF.

24. Czy można zwiększyć liczbę użytkowników merytorycznych/administratorów w podmiocie?

Istnieje taka możliwość. W uzasadnionych przypadkach Podmiot może wystąpić z wnioskiem o zwiększenie liczby administratorów/użytkowników merytorycznych. Po akceptacji wniosku przez UKNF:

- jeżeli wniosek dotyczy użytkownika merytorycznego - administrator Portalu w Podmiocie zakłada konto użytkownika i generuje żądanie wystawienia certyfikatu
- jeżeli wniosek dotyczy administratora Portalu w Podmiocie – konto nowego administratora zostanie założone przez administratora UKNF, po przesłaniu do UKNF z dopiskiem „Departament Informatyki – PORTAL”, podpisanego zgodnie z reprezentacją przez osoby upoważnione, Załącznika nr 1 do Regulaminu korzystania z Portalu KNF wraz z kopią aktualnego KRS.

25. Co należy zrobić, aby odebrać dostęp do Portalu KNF administratorowi Portalu w Podmiocie?

Jeżeli w podmiocie jest Administrator podmiotu z ważnym certyfikatem, to może on unieważnić certyfikat innego Administratora. Unieważniony certyfikat uniemożliwia zalogowanie do systemu Portal. W celu usunięcia konta Administratora podmiotu, Podmiot

nadzorowany zobowiązany jest przesłać do UKNF pismo z dopiskiem „Departament Informatyki – PORTAL”, podpisane zgodnie z reprezentacją przez osoby upoważnione, informujące o odwołaniu administratora. Do pisma należy załączyć kopię aktualnego KRS. Jeżeli konto musi być usunięte w trybie natychmiastowym, to należy dodatkowo skorzystać z formularza do zgłaszania problemów technicznych (patrz pkt 29) załączając zeskanowane wymagane wyżej dokumenty i wpisując uzasadnienie skorzystania z tego trybu. Konto nowego administratora zostanie założone po przesłaniu wniosku do UKNF z dopiskiem „Departament Informatyki – PORTAL”, podpisanego zgodnie z reprezentacją przez osoby upoważnione, Załącznika nr 2 do *Regulaminu korzystania z Portalu KNF* wraz z kopią aktualnego KRS.

26. Co należy zrobić, aby odebrać dostęp do Portalu użytkownikowi merytorycznemu? W zależności od potrzeb dostęp do Portalu może odebrać Administrator w Podmiocie na dwa sposoby:

- poprzez skorzystanie z funkcji „zablokuj użytkownika” dostępnej w panelu administracyjnym w zakładce zarządzania użytkownikami, operacja ta jest odwracalna i w każdej chwili administrator może odblokować użytkownika,
- poprzez skorzystanie z funkcji „usuń użytkownika” dostępnej w panelu administracyjnym w zakładce zarządzania użytkownikami, operacja ta różni się od poprzedniej tym, że automatycznie unieważnia certyfikat użytkownika.

Obie wymienione wyżej metody uniemożliwiają zalogowanie się do systemu skutecznie blokując dostęp takiego użytkownika do Portalu.

27. Jak dokonać zamiany administratorów Portalu z podmiotu nadzorowanego? Podmiot nadzorowany przesyła do UKNF z dopiskiem „Departament Informatyki – PORTAL”, pismo z prośbą o usunięcie konta administratora, podpisane zgodnie z reprezentacją przez osoby upoważnione. Do pisma należy załączyć kopię aktualnego KRS. Konto nowego administratora zostanie założone po przesłaniu wniosku do UKNF z dopiskiem „Departament Informatyki – PORTAL”, podpisanego zgodnie z reprezentacją przez osoby upoważnione, Załącznika nr 2 do *Regulaminu korzystania z Portalu KNF* wraz z kopią aktualnego KRS. Patrz również: odpowiedź na pytanie 25.

28. Jak dokonać zamiany użytkowników merytorycznych Portalu?

Należy usunąć konto użytkownika, który ma być pozbawiony dostępu - patrz odpowiedź na pytanie 26. Konto nowego użytkownika merytorycznego zakłada Administrator Portalu w Podmiocie w ramach posiadanych uprawnień.

D. PROBLEMY TECHNICZNE I MERYTORYCZNE

29. Gdzie należy zgłaszać problemy techniczne dotyczące Portalu?

Użytkownik merytoryczny w Podmiocie zawsze zgłasza problem techniczny do administratora Portalu w Podmiocie. Użytkownik merytoryczny z Podmiotu nie zgłasza bezpośrednio problemów technicznych do UKNF.

Administrator Portalu w Podmiocie zgłasza problemy techniczne dotyczące użytkowników merytorycznych lub administratorów Portalu za pomocą formularza znajdującego się na stronie <https://www.knf.gov.pl/pomoc>.

30. Gdzie można zgłaszać problemy natury merytorycznej dotyczące informacji publikowanej (rozmowy/artykułu/ankiety)?

W przypadku pojawienia się problemu natury merytorycznej należy go zgłosić wysyłając zapytanie na adres (obszar/role), z którego została wysłana rozmowa(wiadomość)/artykuł/ankieta.

31. Gdzie można zgłaszać wnioski dotyczące funkcjonalności Portalu KNF/sugestie dotyczące ulepszenia funkcjonalności?

Uwagi dotyczące funkcjonalności można zgłaszać tak samo jak problemy techniczne, za pośrednictwem administratora Portalu w Podmiocie, poprzez formularz na stronie <https://www.knf.gov.pl/pomoc>.

32. Jak otrzymać instrukcje dotyczące korzystania z Portalu?

Przy pierwszym logowaniu system prosi o zapoznanie się z instrukcjami i Regulaminem korzystania z Portalu. Dokumenty dostępne są w samym Portalu KNF, ponadto elektroniczną kopię oryginałów dokumentów można otrzymać po przesłaniu prośby przez Administratora podmiotu na adres <https://www.knf.gov.pl/pomoc>.

33. Czy można uruchomić system Portal z dwóch certyfikatów na raz na jednej maszynie?

Nie. System przewiduje pracę tylko jednego użytkownika w danej chwili. W przypadku posiadania dwóch certyfikatów przez jedną osobę, np. certyfikatu administratora podmiotu oraz użytkownika merytorycznego, należy korzystać rozdzielnie z obu certyfikatów. Pojawienie się równoległych tzw. sesji przy użyciu jednego certyfikatu jest monitorowane przez UKNF.

34. Czy możliwa jest zmiana prefiksu w założonym już podmiocie?

Nie. Prefiks nadawany jest w trakcie wprowadzania informacji o podmiocie i nie powinien być modyfikowany, gdyż ma on zapewnić unikalność loginów dla tworzonych użytkowników – jest dodawany do każdego loginu tworzonego w danym podmiocie użytkownika.

Załącznik nr 1 Przykłady Instalacji certyfikatów w softwareowych w popularnych przeglądarkach internetowych

1. Instalacja certyfikatu w przeglądarkach Internet Explorer i Google Chrome Przeglądarki te wykorzystują systemowy magazyn do przechowywania certyfikatów.

Instrukcja instalacji certyfikatu i pierwszego logowania do Portalu. Przeglądarka Internet Explorer

Otrzymany na przenośnym nośniku certyfikat umieszczamy w komputerze, na którym zamierzamy zainstalować certyfikat.

W komputerze wyszukujemy wolumin z podłączonym nośnikiem.

- klikamy w wolumin i uruchamiamy plik z certyfikatem, np.:



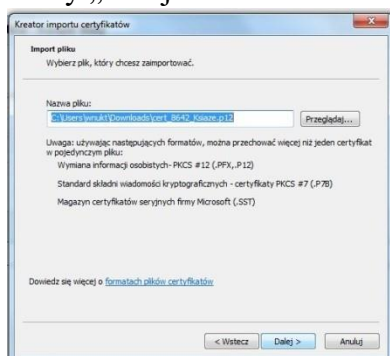
cert_8642_TestowyNowak.p12

- klikając na nim dwukrotnie

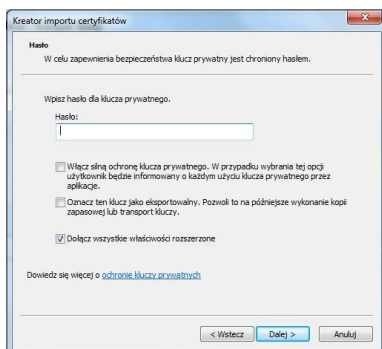
Uruchamia się proces instalacyjny:



Klikamy „Dalej”



Ścieżka do pliku z certyfikatem pojawia się automatycznie. Importujemy plik z certyfikatem, klikając „Dalej”.



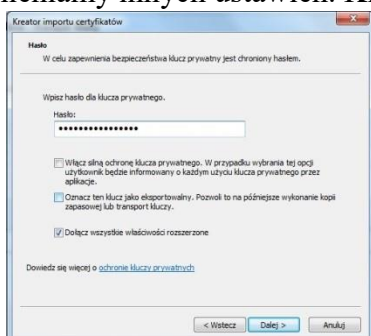
Pojawia się okno do wpisania hasła. Odnajdujemy otrzymany wcześniej mail z unikalnym pinem do instalacji certyfikatu, np.:

Pin dla certyfikatu: hWy5BVdaSm4Sw3Z7

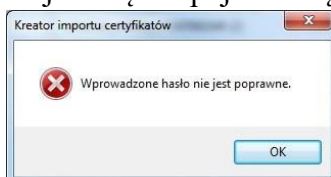
Numer seryjny certyfikatu: 7669445657176930163

Login użytkownika: 8642_TestowyNowak

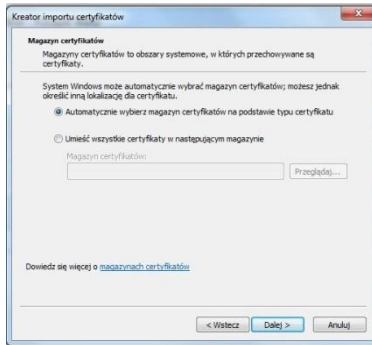
W pole „Hasło” wpisujemy (kopiujemy) otrzymane hasło do instalowanego certyfikatu i nie zmieniamy innych ustawień. Klikamy „Dalej”.



***UWAGA** poniżej możliwość rozszerzenia ochrony Jeśli hasło jest błędne pojawia się komunikat

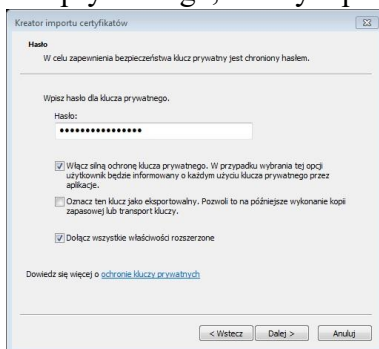


Jeśli hasło jest poprawnie wprowadzone po kliknięciu przycisku „Dalej” kolejnym etapem instalacji jest wybór miejsca docelowego, gdzie w magazynie plików będzie zainstalowany certyfikat, domyślnie program proponuje magazyn na podstawie danego certyfikatu.

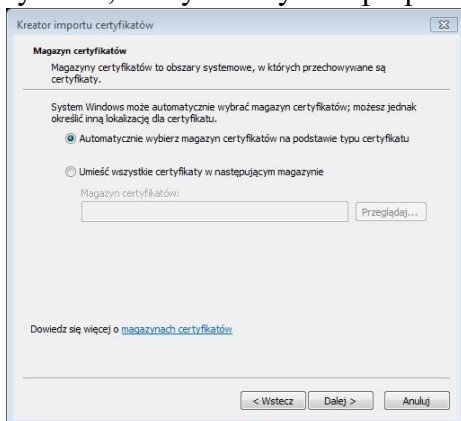


*UWAGA

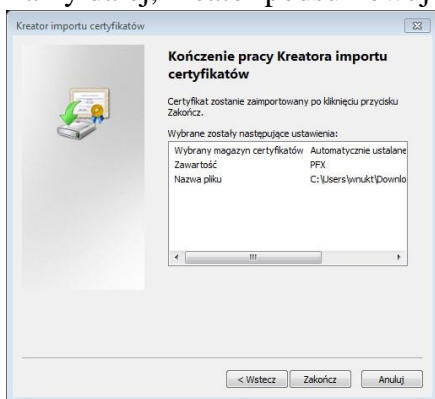
Przy instalacji należy rozszerzyć ochronę naszego certyfikatu zaznaczając opcję silnej ochrony klucza prywatnego, należy wpisać hasło otrzymane mailowo i zaznaczyć check-box



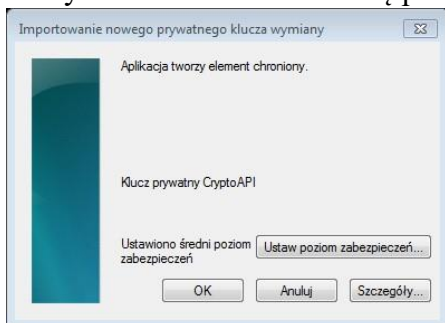
W przypadku opcji z włączoną ochroną kolejnym etapem jest wybór miejsca umieszczenia certyfikatu, domyślnie system proponuje automatyczny magazyn certyfikatu.



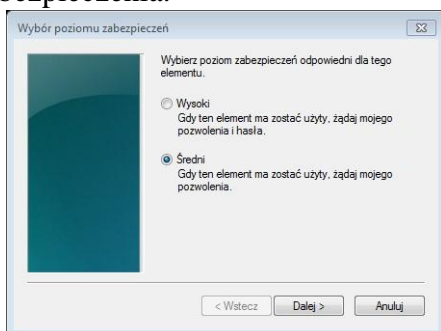
Klikamy dalej, kreator podsumowuje import certyfikatu



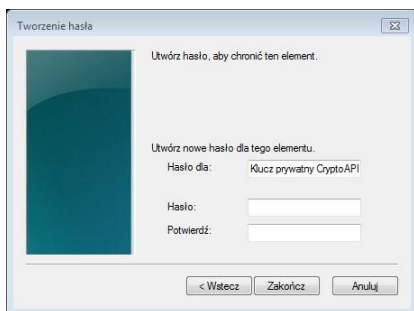
Klikamy zakończ. Uruchamia się proces importowania unikalnego hasła do Portalu,



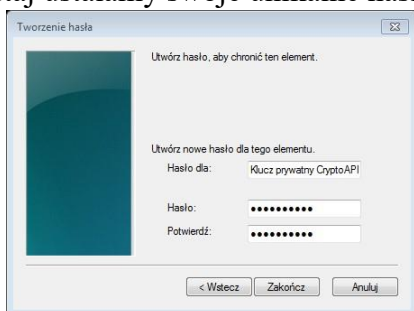
klikając w opcję „Ustaw poziom zabezpieczeń” możemy samodzielnie ustalić poziom zabezpieczenia.



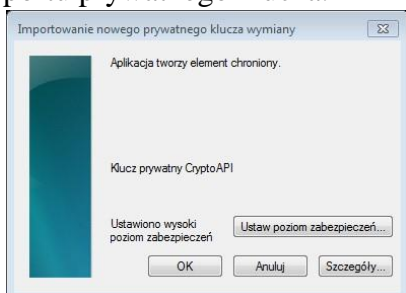
By ustalić hasło, które będzie wymagane przy każdorazowym logowaniu, wybieramy opcję Wysokiego poziomu zabezpieczeń.



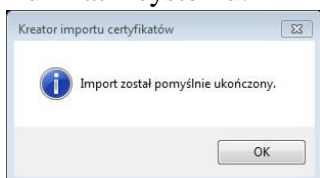
Tutaj ustalamy swoje unikalne hasło do logowania w Portalu.



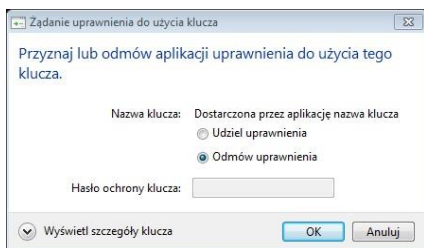
Po wprowadzeniu hasła klikamy Zakończ, proces instalacji przeniesie nas ponownie do okna z importu prywatnego klucza.



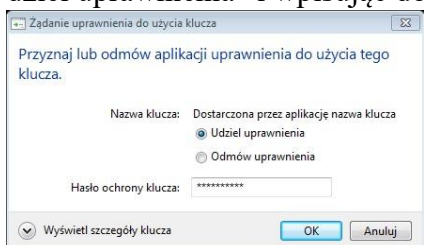
Akceptujemy import klikając Ok, potwierdzeniem poprawności procesu ustalania hasła jest komunikat z systemu.



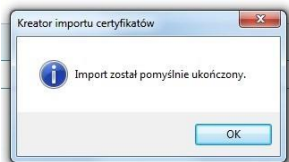
Teraz użytkownik logując się do portalu będzie zobowiązany podać swoje hasło.



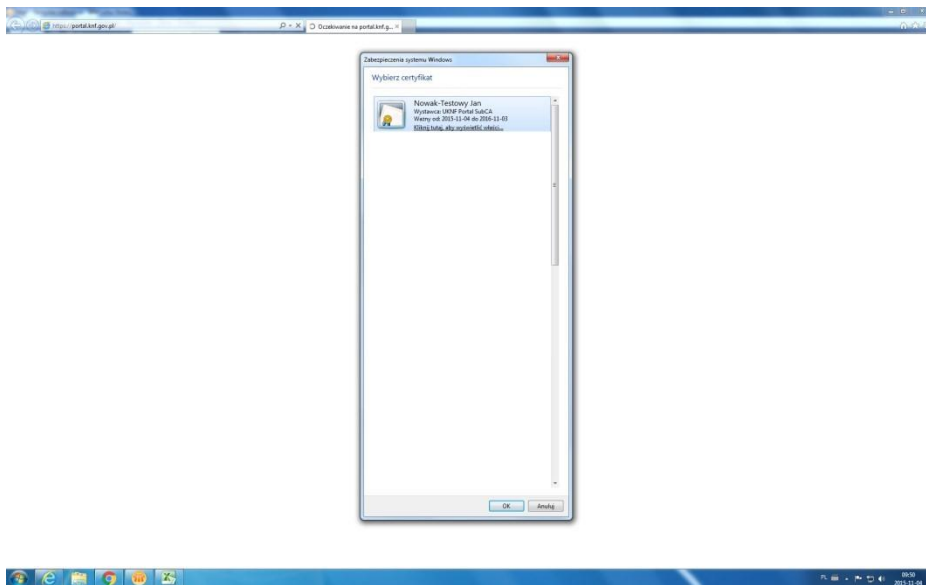
Domyślnie zaznaczona jest opcja „Odmów uprawnienia”, musimy to zmienić na opcję powyżej „Udziel uprawnienia” i wpisując do tego hasło ochrony klucza.



Zatwierdzamy przyciskiem Ok, użytkownik jest zalogowany.



Po zainstalowaniu certyfikatu możliwe jest zalogowanie się do Portalu. W przeglądarce internetowej wybieramy stronę internetową portalu: <https://portal.knf.gov.pl> Pojawia się okno do logowania:



Wybieramy swojego użytkownika i klikamy „OK”. Pojawi się okno:



Klikamy „Zaloguj”.

Przy pierwszym logowaniu do Portalu niezbędna jest akceptacja regulaminów.

2. Instalacja certyfikatu w przeglądarce FireFox

Przeglądarka te wykorzystuje swój magazyn do przechowywania certyfikatów.

Otrzymany na przenośnym nośniku certyfikat umieszczamy w komputerze, na którym zamierzamy zainstalować certyfikat.

W komputerze wyszukujemy wolumin z podłączonym nośnikiem.

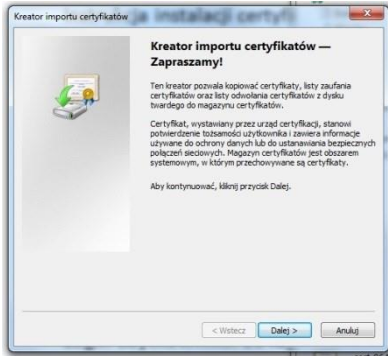
- klikamy w wolumin i uruchamiamy plik z certyfikatem, np.:



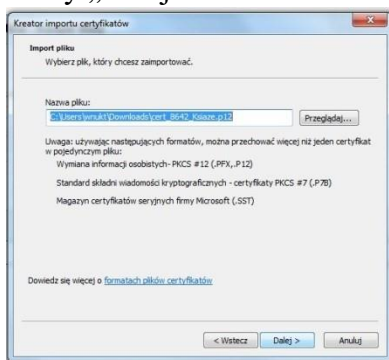
cert_8642_TestowyNowak.p12

- klikając na nim dwukrotnie

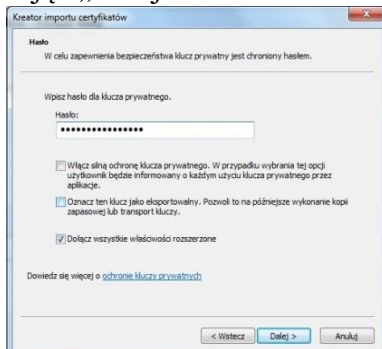
Uruchamia się proces instalacyjny:



Klikamy „Dalej”



Ścieżka do pliku z certyfikatem pojawia się automatycznie. Importujemy plik z certyfikatem, klikając „Dalej”.



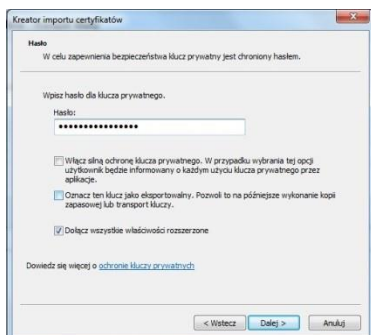
Pojawia się okno do wpisania hasła. Odnajdujemy otrzymany wcześniej mail z unikalnym pinem do instalacji certyfikatu, np.:

Pin dla certyfikatu: hWy5BVdaSm4Sw3Z7

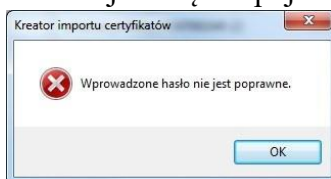
Numer seryjny certyfikatu: 7669445657176930163

Login użytkownika: 8642_TestowyNowak

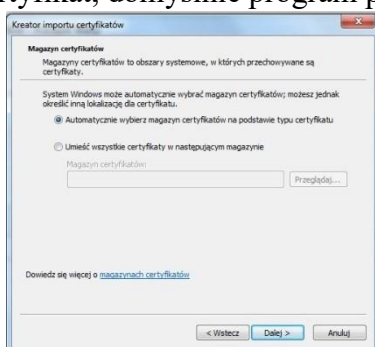
W pole „Hasło” wpisujemy (kopiujemy) otrzymane hasło do instalowanego certyfikatu i nie zmieniamy innych ustawień. Klikamy „Dalej”.



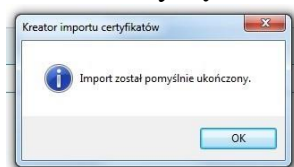
Jeśli hasło jest błędne pojawia się komunikat



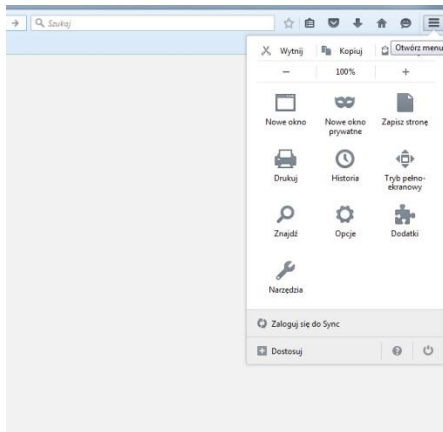
Jeśli hasło jest poprawnie wprowadzone po kliknięciu przycisku „Dalej” kolejnym etapem instalacji jest wybór miejsca docelowego, gdzie w magazynie plików będzie zainstalowany certyfikat, domyślnie program proponuje magazyn na podstawie danego certyfikatu.



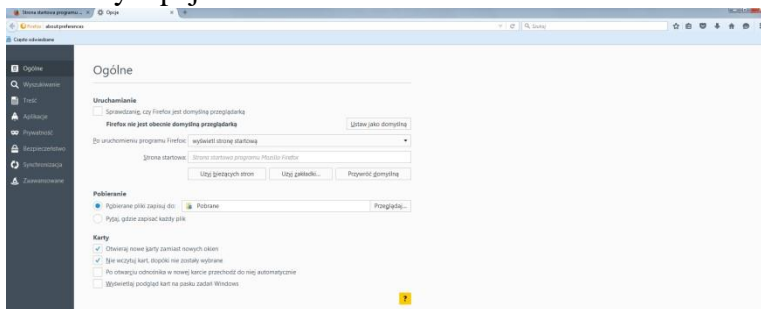
Po wyborze miejsca docelowego instalacji certyfikatu klikamy „Dalej”, użytkownik poinformowany będzie o poprawnej instalacji certyfikatu.



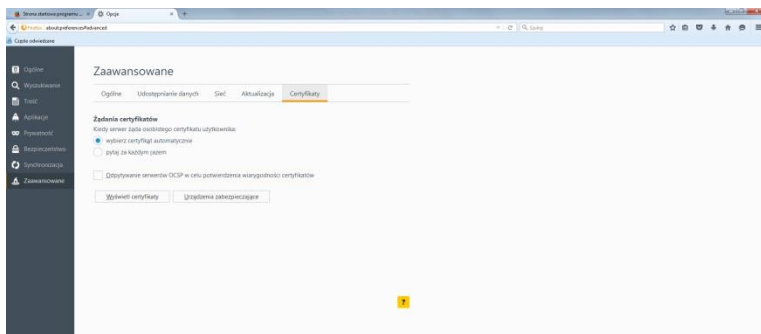
Po otwarciu strony internetowej w przeglądarce FireFox wybieramy opcję menu.



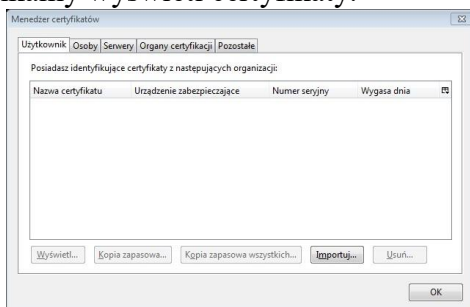
Zaznaczamy Opcje



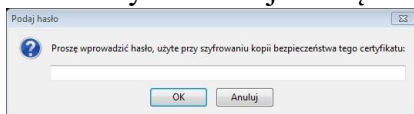
Wybieramy opcje Zaawansowane.



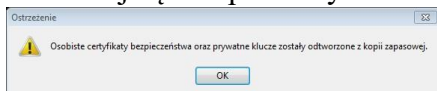
Klikamy wyświetl certyfikaty.



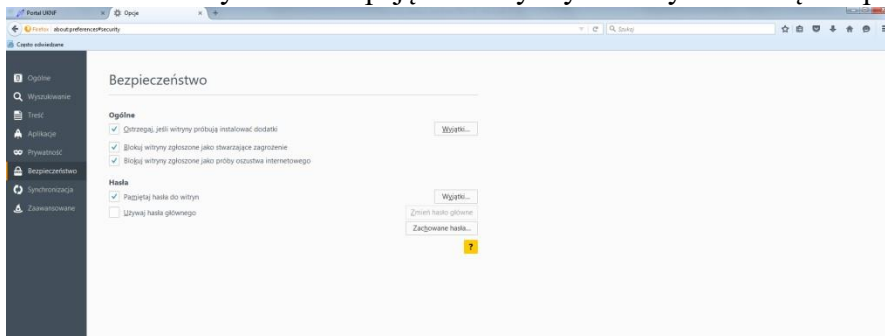
Wybieramy Importuj i wybieramy miejsce lokalizacji zaimportowanego w poprzednich krokach certyfikatu. Pojawi się okno do ponownego wpisania hasła otrzymanego mailem.



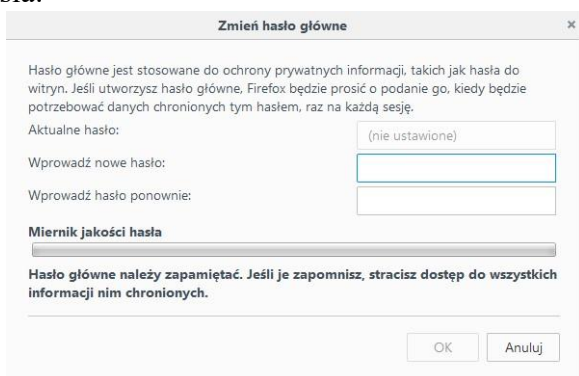
Wpisujemy hasło i zatwierdzamy klikając Ok, pomyślność dodania certyfikatu do przeglądarki internetowej będzie poniższy komunikat.



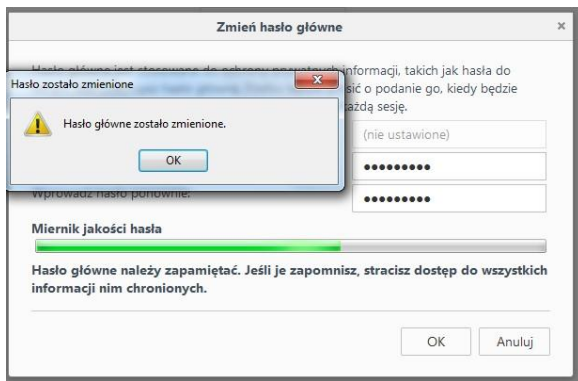
Dla większego bezpieczeństwa użytkownika zaleca się zabezpieczenie logowania się na podstawie hasła. Aby ustawić opcję ochrony wybieramy zakładkę Bezpieczeństwo.



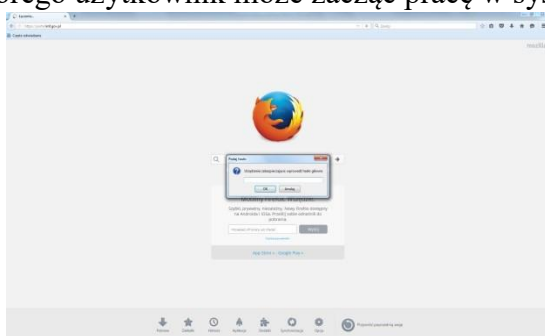
Zaznaczamy check-box „Używaj hasła głównego”, pojawi się okno z możliwością ustalenia hasła:



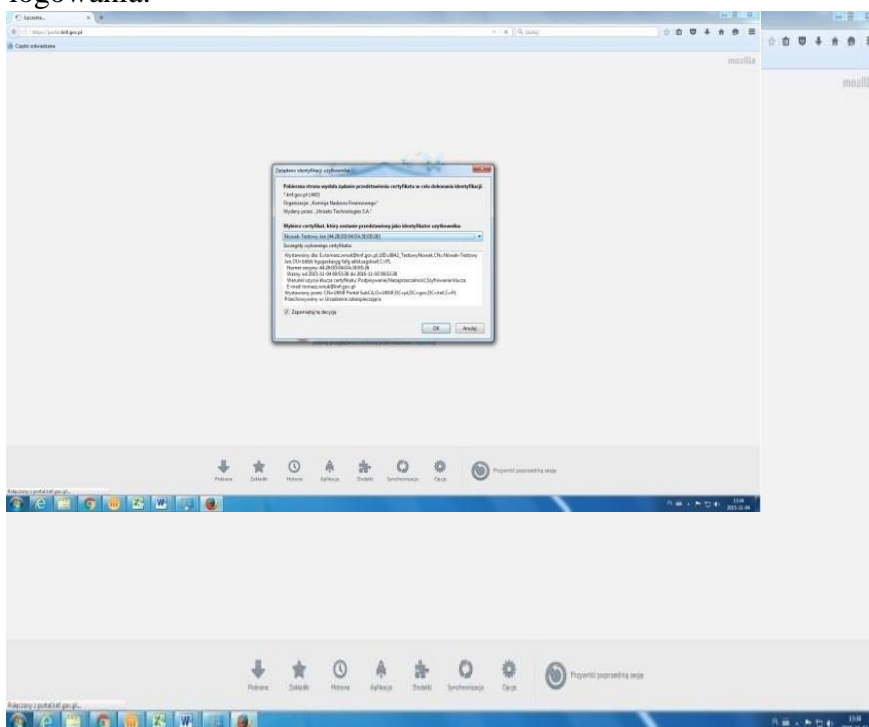
Wprowadzamy hasło zatwierdzając przyciskiem OK.



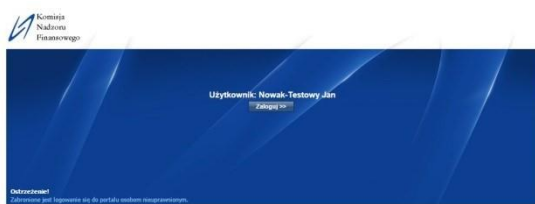
Przy logowaniu do systemu portal pojawia się okno do wpisania hasła, po wprowadzeniu którego użytkownik może zacząć pracę w systemie.



Po zainstalowaniu certyfikatu możliwe jest zalogowanie się do Portalu. W przeglądarce internetowej wybieramy stronę internetową portalu: <https://portal.knf.gov.pl> Pojawia się okno do logowania:



Wybieramy swojego użytkownika i klikamy „OK”. Pojawi się okno:



Klikamy „Zaloguj”.

Przy pierwszym logowaniu do Portalu niezbędna jest akceptacja regulaminów.