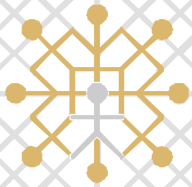


HEUTHES®

Administracja certyfikatami

Szczecin, 2006-10-03.

HEUTHES Sp. z o.o.

Status prawny: spółka z o.o. zarejestrowana pod numerem KRS 0000184163, istniejąca od marca 1989 roku.

Siedziba firmy: ul. Koński Jar 8/30, 02-785 Warszawa.

Biuro techniczno-handlowe: ul. Metalowa 6, 70-744 Szczecin

marketing@heuthes.pl, www.heuthes.pl , www.isof.pl

Tel./fax: (091) 460 89 74.

Spis treści

1. Wprowadzenie

Przedmiot

Instrukcja opisuje funkcje administrowania certyfikatami kluczy publicznych używanych w systemie ISOF do ochrony transmisji sieciowej pomiędzy przeglądarką użytkownika a serwerem.

Zagadnienia składające się na administrację certyfikatami

1 . Konfiguracja i przygotowanie do pracy

   1.1 .Opcje konfiguracyjne ISOF

   1.2 .Uprawnienia

2 . Tryby certyfikacji kluczy użytkowników

   2.1 .Certyfikacja bez dostępu użytkownika do systemu ISOF

   2.2 .Recertyfikacja - odnowienie aktywnego certyfikatu przez użytkownika ISOF

3 . Zmiany statusu certyfikatów - zawieszanie i unieważnianie

   3.1 .Unieważnienie certyfikatu

2. Konfiguracja i przygotowanie do pracy

2.1. Opcje konfiguracyjne ISOF

Uruchomienie funkcji certyfikacji i zarządzania certyfikatami w systemie ISOF klienta jest konfigurowane prawie w całości przez firmę HEUTHES. Spośród parametrów konfiguracyjnych dotyczących certyfikatów tylko dwa są dostępne dla administratora ISOF.

Parametr **cert_powiadamianie** jest domyślnie włączony w systemach ISOF, w których czynne są funkcje obsługi certyfikatów. Steruje on powiadomieniami wyświetlanymi w postaci okien dialogowych podczas logowania do systemu. Są to dwa rodzaje powiadomień:

- dla użytkownika – o zbliżającym się terminie wygaśnięcia ważności certyfikatu, z możliwością natychmiastowego przejścia do dialogu generowania nowych kluczy, oraz o oczekującym, gotowym do pobrania certyfikacie, z możliwością natychmiastowego jego zainstalowania;
- dla administratora z uprawnieniami do akceptacji żądań certyfikacyjnych – o oczekującym żądaniu recertyfikacyjnym (odnowienia certyfikatu) wygenerowanym przez użytkownika.

W wypadku gdy opcja konfiguracyjna cert_powiadamianie ma wartość 0, powiadomienia o zbliżającym się wygaśnięciu certyfikatu także są wyświetlane, ale jeszcze przed zalogowaniem się użytkownika i bez możliwości natychmiastowego uruchomienia funkcji odnowienia certyfikatu.

Parametr **login_days_to_warn_about_cert_exp** decyduje o wyprzedzeniu (w dniach), z jakim będą wyświetlane ostrzeżenia o wygasających certyfikatach. Domyślnie jest ustawiony na 14 dni.

2.2. Uprawnienia

Wszyscy użytkownicy ISOF mają uprawnienia do odnawiania certyfikatów za pomocą funkcji *Start / Odnowienie certyfikatu* i *Start / Pobranie certyfikatu*.

Czynności administracyjne dotyczące certyfikatów są regulowane przez następujące uprawnienia:

- **Administracja certyfikatami** daje dostęp do funkcji *Start / Administracja / Administracja certyfikatami*, z wyjątkiem funkcji, których dotyczą dwa pozostałe uprawnienia
- **Akceptacja żądań certyfikacji kluczy** pozwala na akceptowanie żądań certyfikacji zgłoszonych przez użytkowników, których lista dostępna jest w widoku Żądania oczekujące
- **Żądanie zmiany statusu certyfikatów** pozwala kierować do CA żądania zawieszenia, odwieszenia i unieważnienia certyfikatów.

3. Tryby certyfikacji kluczy użytkowników

Istnieją dwa warianty generacji certyfikatów kluczy użytkowników:

- Certyfikacja bez dostępu użytkownika do systemu ISOF - w sytuacji, gdy użytkownik nie posiada żadnego ważnego certyfikatu pozwalającego mu na dostęp do systemu ISOF (dotyczy to też sytuacji, gdy ważność jego certyfikatu wygasła);
- Recertyfikacja, odnowienie aktywnego certyfikatu przez użytkownika ISOF - w sytuacji, gdy użytkownik posiada przynajmniej jeden ważny certyfikat pozwalający na dostęp do systemu ISOF.

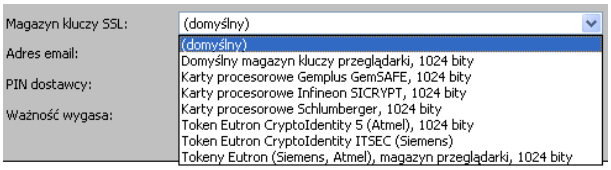
3.1. Certyfikacja bez dostępu użytkownika do systemu ISOF

Procedura obejmuje następujące działania:

- Administrator ISOF pobiera z systemu kod PIN dla użytkownika
- Użytkownik generuje klucze na stronie http://www.isof.pl/ca/,
- Użytkownik instaluje certyfikat ze strony http://www.isof.pl/ca/.

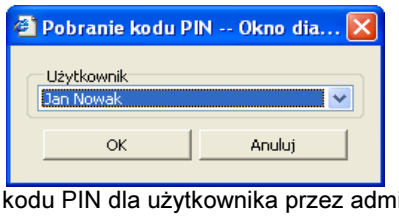
3.1.1. Pobranie kodu PIN dla użytkownika

Administrator tworzy w systemie ISOF konto dla użytkownika. Może ustawić urządzenie kryptograficzne, z którego będzie korzystał użytkownik. Ustawienie „(domyślny)" oznacza, że jeśli użytkownik ma zainstalowane oprogramowanie do obsługi tokenów kryptograficznych USB Eutron, to nastąpi próba generacji w takim urządzeniu, w innym wypadku klucze zostaną wygenerowane w magazynie przeglądarki.



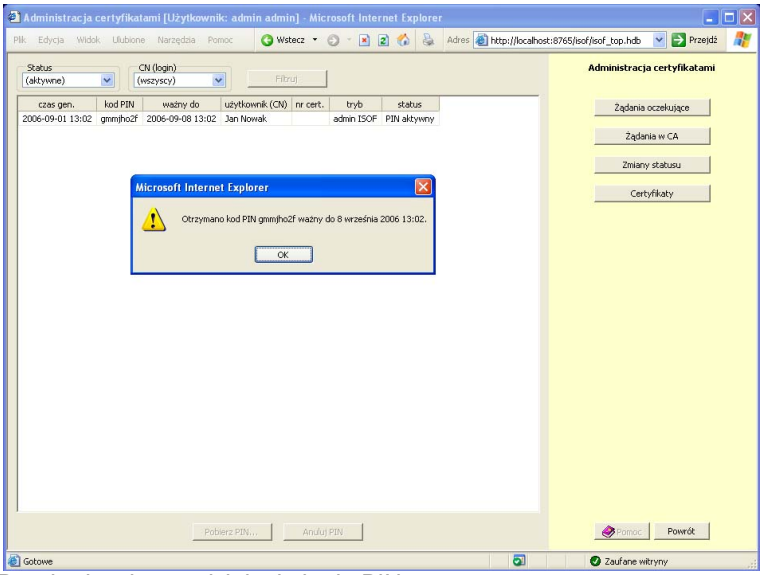
Wybór magazynu klucza SSL

Administrator pobiera kod PIN dla użytkownika, korzystając z funkcji *Start / Administracja / Administracja certyfikatami*, przycisk *Żądania w CA*. Po naciśnięciu na dole strony przycisku Pobierz PIN, pojawia się dialog, w którym należy wybrać z listy właściwego użytkownika.



Pobieranie kodu PIN dla użytkownika przez administratora

Żądanie przydzielenia kodu PIN zostaje wysłane do CA. Przydzielony jednorazowy kod pojawia się na liście i zostaje zakomunikowany dialogiem.



Potwierdzenie przydzielenia kodu PIN

Administrator przekazuje użytkownikowi uzyskany ośmioznakowy kod PIN, jego login name (odpowiadający polu CN w certyfikacie) oraz adres URL do publicznego serwisu certyfikacyjnego (http://www.isof.pl/ca/).

3.1.2. Wygenerowanie kluczy i wysłanie żądania certyfikacyjnego

Zanim użytkownik uzyska dostęp do systemu ISOF, musi posiadać certyfikat klucza publicznego.

Wprowadzanie kodu PIN i loginu

Klucz wystawiany jest przez Centrum Autoryzacji Kluczy (CA) firmy HEUTHES. W tym celu musi wygenerować sobie klucz prywatny i odpowiadający mu klucz publiczny, którego autentyczność zostaje potwierdzona przez CA certyfikatem.

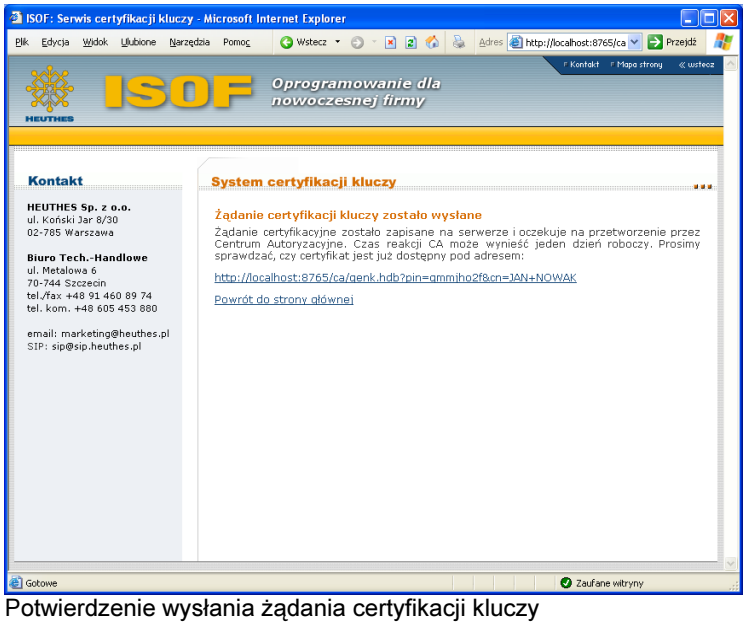
Wygenerowanie pierwszego certyfikatu wymaga wykonania specjalnej procedury z użyciem odrębnego serwisu internetowego, znajdującego się pod adresem: http://www.isof.pl/ca/. Do wykonania procedury potrzebny jest jednorazowy kod PIN, który użytkownikowi udostępnia administrator. Otrzymawszy kod PIN, użytkownik otwiera w przeglądarce, w której będzie pracował, stronę http://www.isof.pl/ca/. W pola formularza na tej stronie wpisuje otrzymany od administratora kod PIN i swój login - patrz rysunek *Wprowadzanie kodu PIN i loginu*.

Jeśli wpisane dane są prawidłowe, to zawartość okna przeglądarki zmieni się w sposób przedstawiony poniżej:

Generowanie żądania certyfikacyjnego

Jeśli użytkownik nie korzysta z żadnych specjalnych urządzeń kryptograficznych, w rodzaju wtyczki USB albo karty procesorowej, to wystarczy, że kliknie *Generuj*. W wypadku, gdy korzysta z któregoś z takich urządzeń, powinien je wybrać z listy *Urządzenie/magazyn*.

Po kilku do kilkudziesięciu sekund – zależnie od szybkości komputera lub rodzaju urządzenia kryptograficznego – pojawi się ekran z informacją jak poniżej. Oznacza on, że klucze zostały wygenerowane i do Centrum Autoryzacji Kluczy zostało wysłane żądanie certyfikacyjne.



Potwierdzenie wysłania żądania certyfikacji kluczy

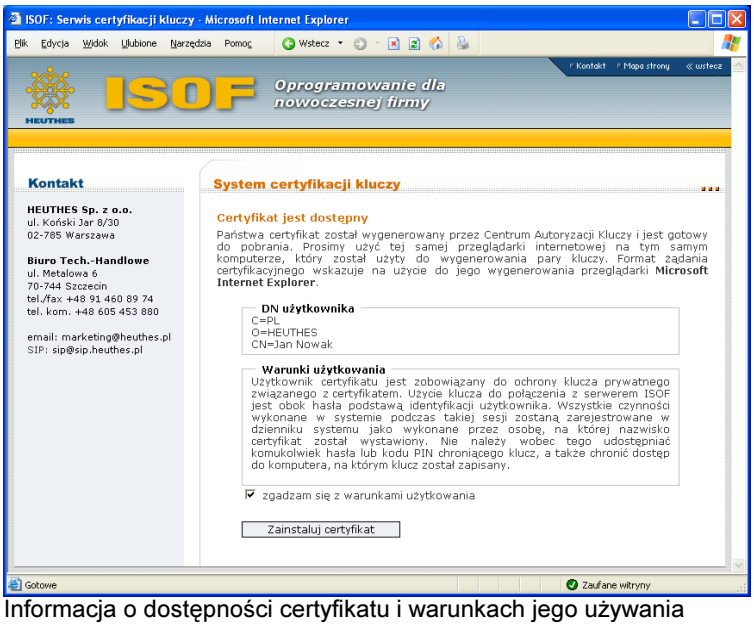
Dotarcie do tego punktu procedury oznacza, że zostało złożone zamówienie na certyfikaty. Jeśli nie zostały dokonane żadne specjalne uzgodnienia drogą telefoniczną lub poczty elektronicznej, to należy się liczyć z czasem około jednego dnia roboczego oczekiwania na ich wystawienie i udostępnienie.

Wysłanie przez użytkownika żądania certyfikacyjnego jest dla administratora ISOF widoczne w module *Administracja certyfikatami* jako zmiana statusu w widoku *Żądania w CA* – zmienia się on z *„PIN aktywny”* na *„Żądanie wysłane”*. Po wygenerowaniu i udostępnieniu certyfikatu przez HEUTHES, status zmienia się na *„dostępny”*.

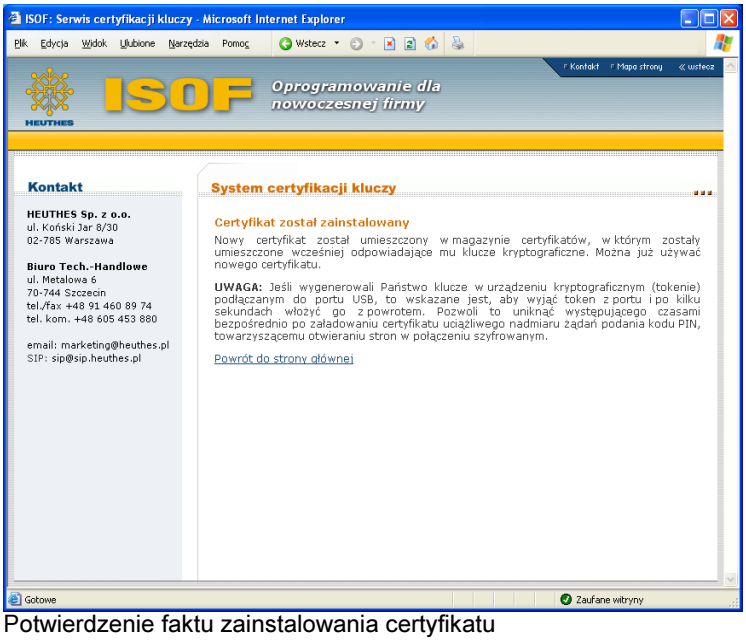
3.1.3. Zainstalowanie certyfikatu

Pobranie certyfikatu zaczyna się podobnie, jak generacja kluczy – użytkownik otwiera stronę http://www.isof.pl/ca/ i wpisuje kod PIN, który otrzymał od administratora, a także swój login (w pole CN). Alternatywnie, użytkownik może skorzystać z odnośnika, który został pokazany na ostatnim ekranie etapu pierwszego.

Po naciśnięciu przycisku *Wyślij*, jeśli certyfikat został już wystawiony przez CA Heuthes, pojawi się ekran informujący o dostępności certyfikatu i zawierający warunki jego użytkowania.



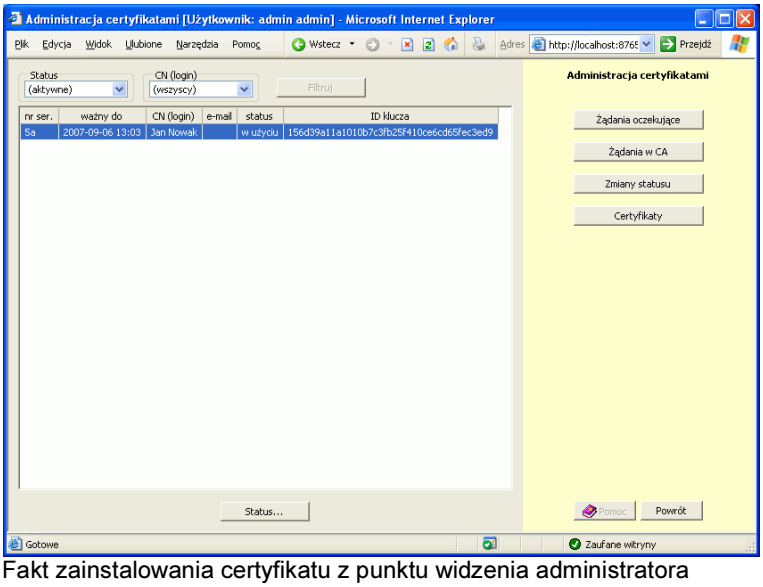
Informacja o dostępności certyfikatu i warunkach jego używania



Potwierdzenie faktu zainstalowania certyfikatu

Przycisk *Zainstaluj* certyfikat aktywuje się po zaznaczeniu „zgadzam się z warunkami użytkowania”. Po jego naciśnięciu pojawi się dialog przeglądarki, informujący o instalowaniu certyfikatu przez stronę internetową. Należy potwierdzić dialog przyciskiem *OK*. Rozpocznie to proces instalacji certyfikatu, który może, zależnie od sprzętu, trwać od kilku do kilkunastu sekund. Cały proces kończy się wyświetleniem ekranu z informacją ukazaną na rys. *Potwierdzenie faktu zainstalowania certyfikatu*.

Ze strony administratora zainstalowanie certyfikatu przez użytkownika objawi się tym, że dane o żądaniu znikną z widoku *Administracja certyfikatami*. (przy domyślnym ustawieniu filtru widoku *„(aktywne)”*). Informacja o certyfikacie jest widoczna natomiast w widoku *Certyfikaty*.



Fakt zainstalowania certyfikatu z punktu widzenia administratora

3.2. Recertyfikacja - odnowienie aktywnego certyfikatu użytkownika ISOF

Recertyfikacja jest procedurą, podczas której użytkownik ISOF, którego certyfikat jest bliski terminowi wygaśnięcia, generuje sobie nową parę kluczy i żądanie certyfikacyjne, a następnie, po wystawieniu certyfikatu przez HEUTHES, instaluje go w swojej przeglądarce. W odróżnieniu od procedury wystawienia certyfikatu dla nowego użytkownika, ta procedura jest w całości wykonywana wewnątrz systemu ISOF.

Procedura recertyfikacji obejmuje następujące działania:

- użytkownik generuje nową parę kluczy oraz żądanie certyfikacyjne używając funkcji *Start / Odnowienie certyfikatu*; funkcja ta może też być uruchomiona bezpośrednio z dialogu powiadamiającego o bliskim wygaśnięciu obecnego certyfikatu.
- administrator, lub inna osoba posiadająca uprawnienie *Akceptacja żądań certyfikacji kluczy*, akceptuje żądanie, które w tym momencie zostaje wysłane do CA HEUTHES
- po wystawieniu certyfikatu przez CA HEUTHES, użytkownik instaluje go używając funkcji *Start / Pobranie certyfikatu*; dialog z powiadomieniem o dostępności nowego certyfikatu jest wyświetlany bezpośrednio po zalogowaniu, dając możliwość natychmiastowego przejścia do funkcji instalacji.

3.2.1. Generowanie kluczy i żądania certyfikacyjnego

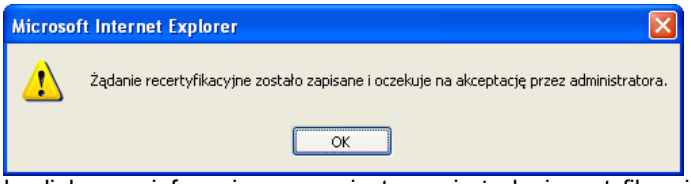
Certyfikaty kluczy publicznych wystawiane przez firmę HEUTHES mają z reguły roczny termin ważności. Dwa tygodnie przed upłynięciem tego terminu (domyślna wartość opcji systemowej **login_days_to_warn_about_cert_exp**) użytkownik zaczyna otrzymywać przy logowaniu do systemu informację

o zbliżającym się terminie wygaśnięcia certyfikatu. Jeśli opcja systemowa **cert_powiadamianie** ma wartość różną od 0, to dialog zawiera pytanie o natychmiastowe uruchomienie funkcji odnowienia certyfikatu. Użytkownik może wybrać przejście do tej funkcji, albo później uruchomić ją przez menu *Start*, wybierając opcję *Odnowienie certyfikatu*.

Okienko dialogowe odnawiania certyfikatu

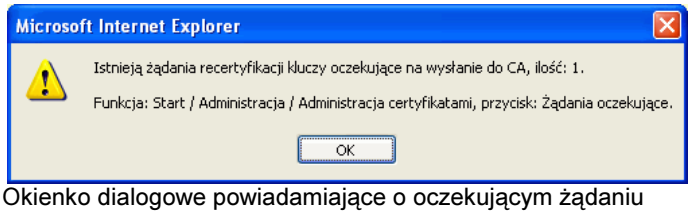
Informacja w ramce *Magazyn certyfikatów* mówi o urządzeniu, w którym para kluczy zostanie wygenerowana. Administrator może wybrać magazyn kluczy dla użytkownika zmieniając wartość combo *Magazyn kluczy SSL* w *Administracji użytkownikami i grupami*. Wartość *„(domyślny)”* działa dobrze w większości wypadków, w szczególności jeśli użytkownik nie używa żadnych specjalnych urządzeń kryptograficznych i nie ma zainstalowanego oprogramowania do nich. W takim wypadku, jak na ilustracji powyżej, klucze zostaną wygenerowane w domyślnym magazynie przeglądarki.

Akceptacja dialogu recertyfikacji powoduje rozpoczęcie generacji kluczy. Proces ten, w zależności od sprzętu, może trwać od kilku do kilkudziesięciu sekund. Kończy się dialogiem informującym o zarejestrowaniu żądania certyfikacyjnego.



Okienko dialogowe informujące o zarejestrowaniu żądania certyfikacyjnego

Powyższy komunikat oznacza, że żądanie zostało zapisane w bazie danych ISOF i oczekuje na zaakceptowanie przez administratora (osobę posiadającą uprawienie *Akceptacja żądań certyfikacji kluczy*). Administrator, w wypadku gdy opcja systemowa **cert_powiadamianie** jest włączona, zobaczy dialog powiadamiający o oczekującym żądaniu bezpośrednio po zalogowaniu się do systemu.

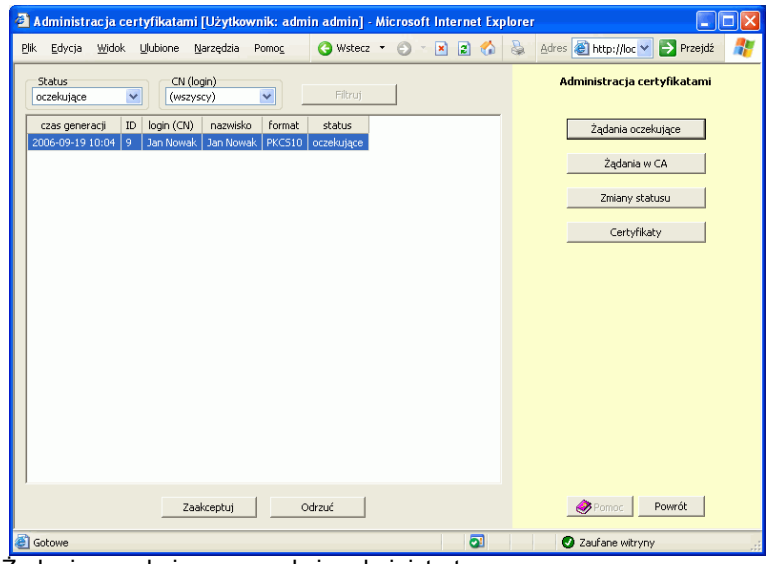


Okienko dialogowe powiadamiające o oczekującym żądaniu

Jeśli odnowienie kluczy jest przeprowadzane przez osobę posiadającą uprawienie do akceptacji żądań (lub jeśli CA jest lokalne – znajduje się w tym samym systemie ISOF), to etap akceptacji żądania jest pomijany i jest ono natychmiast wysyłane do CA.

3.2.2. Akceptacja żądania certyfikacyjnego przez administratora

Administrator ISOF widzi żądanie użytkownika w funkcji *Start / Administracja / Administracja certyfikatami*, w widoku *Żądania oczekujące*.

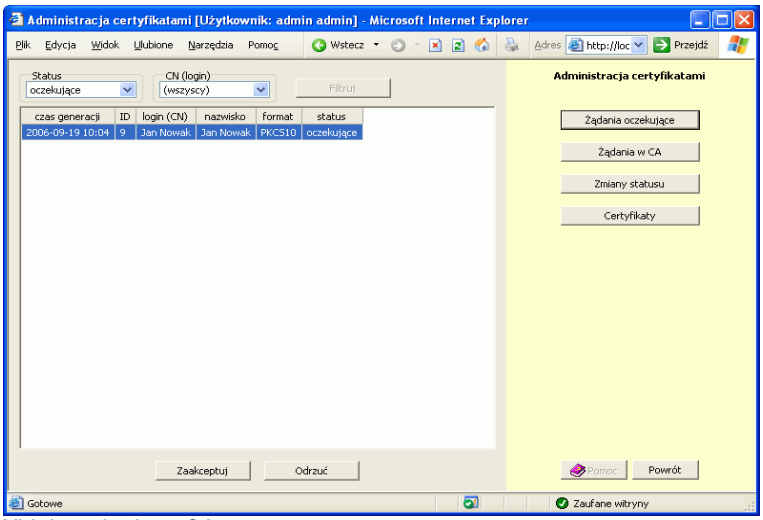


Żądanie oczekujące na reakcję administratora

Naciśnięcie *Zaakceptuj* i zaakceptowanie następującego po nim dialogu powoduje wysłanie żądania do CA. Żądanie zmienia status na *„zaakceptowane”* i znika z widoku.

Jeśli administrator uzna, że żądanie wystawienia certyfikatu nie powinno zostać wysłane do firmy HEUTHES (klient jest za tę usługę obciążany zgodnie z cennikiem), to powinien odrzucić żądanie (przycisk Odrzuć). Żądanie zmienia w tym wypadku status na *„odrzucone”* i znika z widoku.

Żądania wysłane do *CA*, a także otrzymane z CA kody PIN dla nowych użytkowników, są widoczne w widoku *Żądania w CA*. Również certyfikaty, które nie zostały jeszcze pobrane przez użytkowników, są widoczne w tym widoku przy domyślnym ustawieniu filtru statusu – *„(aktywne)”*. W ten sposób administrator ma szybki przegląd niedokończonych spraw związanych z wystawianiem certyfikatów kluczy dla użytkowników.

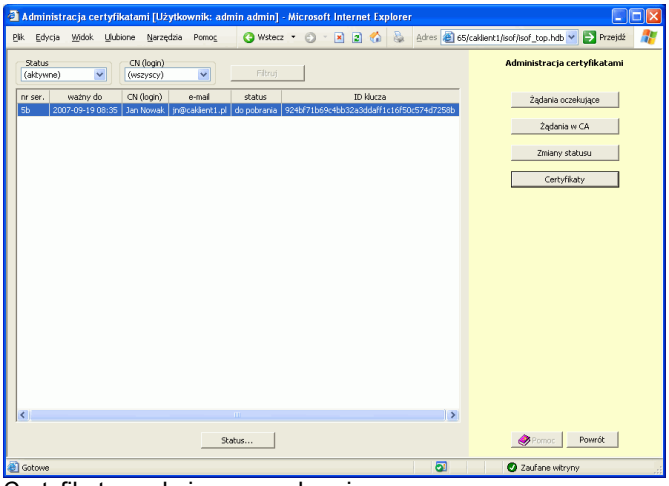


Widok żądania w CA

Dopóki żądanie ma status *„żądanie wysłane”*, co oznacza, że nie został jeszcze wystawiony certyfikat, administrator ma wciąż możliwość wycofać je z *CA* za pomocą przycisku *Anuluj PIN*.

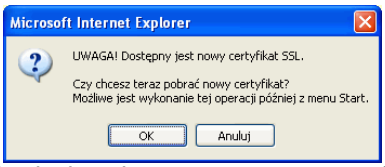
3.2.3. Pobranie i instalacja certyfikatu

Gdy CA wystawi certyfikat, status żądania zmieni się na *„dostępny”*. Oznacza to, że certyfikat jest oczekuje na pobranie przez użytkownika. Jednocześnie certyfikat pojawi się w widoku *Certyfikaty*.



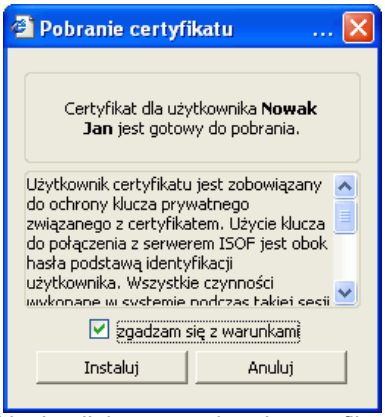
Certyfikat oczekujący na pobranie

Certyfikat ma status *„do pobrania”*. Jeśli opcja systemowa **cert_powiadamianie** jest włączona, to użytkownik otrzyma po zalogowaniu się powiadomienie:



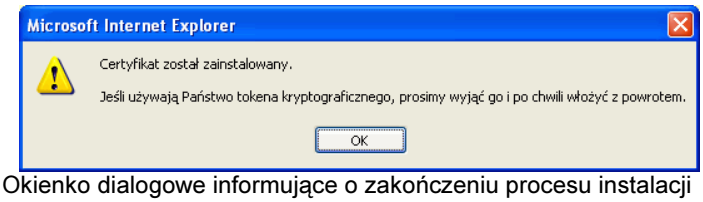
Powiadomienie o dostępnym, nowym certyfikacie

Użytkownik może natychmiast przejść do pobrania certyfikatu – naciskając *OK* – lub użyć później funkcji *Start / Pobranie certyfikatu*. W obu wypadkach po chwili oczekiwania pojawi się dialog:



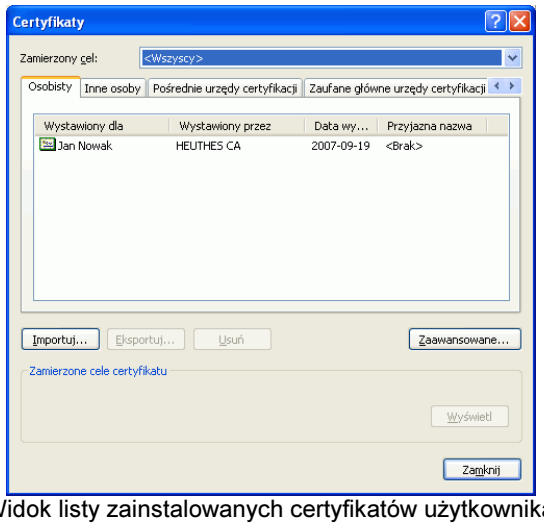
Okienko dialogowe pobrania certyfikatu

Po zaznaczeniu *„zgadzam się z warunkami”* aktywuje się przycisk Instaluj. Kliknięcie go powoduje rozpoczęcie instalacji certyfikatu, co zależnie od sprzętu może potrwać od kilku do kilkunastu sekund. Proces kończy się dialogiem:



Okienko dialogowe informujące o zakończeniu procesu instalacji

Od tego momentu użytkownik może używać certyfikatu do łączenia się z systemem ISOF. Certyfikat będzie widoczny na liście zainstalowanych certyfikatów użytkownika w przeglądarce – w Microsoft Internet Explorerze lista certyfikatów dostępna jest z menu *Narzędzia / Opcje internetowe*, zakładka *Zawartość*, przycisk *Certyfikaty*.



Widok listy zainstalowanych certyfikatów użytkownika

Administrator widzi pobranie certyfikatu przez użytkownika jako zmianę jego statusu na *„w użyciu”*. Jednocześnie żądanie znika z widoku *Żadania w CA* (przy domyślnym ustawieniu filtru).

4. Zmiany statusu certyfikatów

W typowym wypadku, certyfikat użytkownika jest ważny przez rok, do momentu, gdy minie zapisany w nim termin ważności. W momencie, gdy to nastąpi, jego status w widoku certyfikatów zmienia się automatycznie na *„wygasły”*, a próby połączenia użytkownika z serwerem ISOF kończą się niepowodzeniem. Jeśli certyfikat użytkownika wygasł zanim został odnowiony, to należy usunąć go z magazynu przeglądarki (ilustracja powyżej) i przeprowadzić procedurę jak dla nowego użytkownika, z użyciem strony http://www.isof.pl/ca/. Należy pamiętać o usunięciu przeterminowanego certyfikatu przed otwarciem tej strony, ponieważ w innym wypadku próba połączenia zakończy się niepowodzeniem.

Oprócz wygaśnięcia, możliwe są dwie inne sytuacje, w których certyfikat utraci swoją ważność:

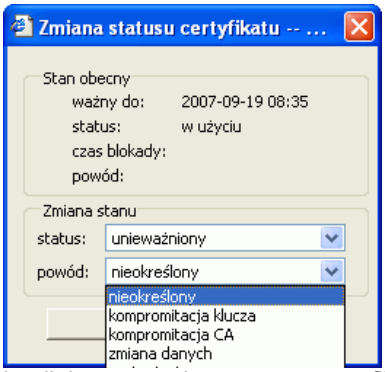
- unieważnienie certyfikatu – na przykład w sytuacji, gdy użytkownik zakończy na stałe swoją pracę z systemem, lub gdy klucz zostanie zagubiony,
- zawieszenie certyfikatu – w sytuacji, gdy przez dłuższy czas certyfikat nie będzie używany, na przykład w wypadku dłuższej nieobecności pracownika. Możliwe jest odwieszenie zawieszonego certyfikatu.

Wszystkie zmiany statusu certyfikatu – zawieszenie, odwieszenie i unieważnienie – są zgłaszane w postaci żądań do CA. Dopóki żądanie nie zostanie wykonane przez CA, status certyfikatu się nie zmienia, a żądanie zmiany statusu jest widoczne w widoku *Zmiany statusu*.

Uwaga! Do przeprowadzenia zmian statusu niezbędne jest uprawnienie *Żądanie zmiany statusu certyfikatów*.

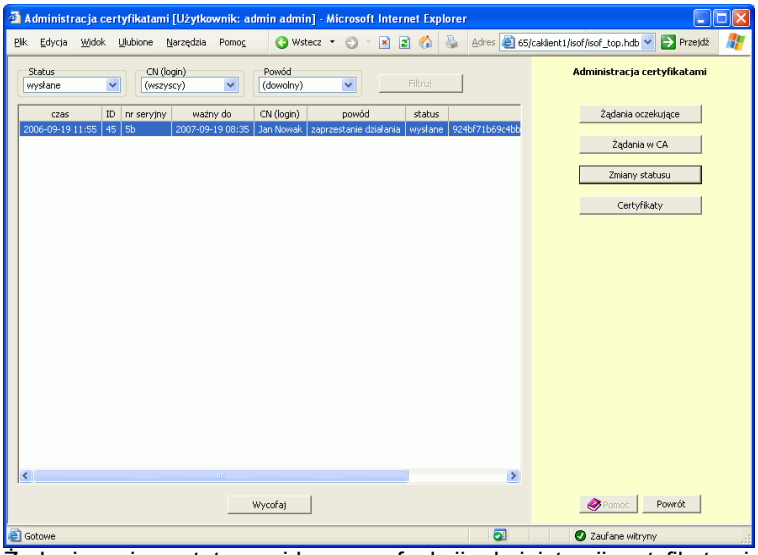
4.1. Unieważnienie certyfikatu

W widoku *Certyfikaty* należy nacisnąć przycisk *Status* u dołu ekranu. Otwiera to dialog statusu certyfikatu. Wybranie statusu *„unieważniony”* powoduje aktywowanie combo *powód*. Zawiera ono przewidziane standardem przyczyny unieważnienia certyfikatu. Można za jego pomocą dodatkowo określić przyczynę (w tym wypadku *„zaprzestanie działania”* – zakończenie pracy przez użytkownika) lub pozostawić *„nieokreślony”*.



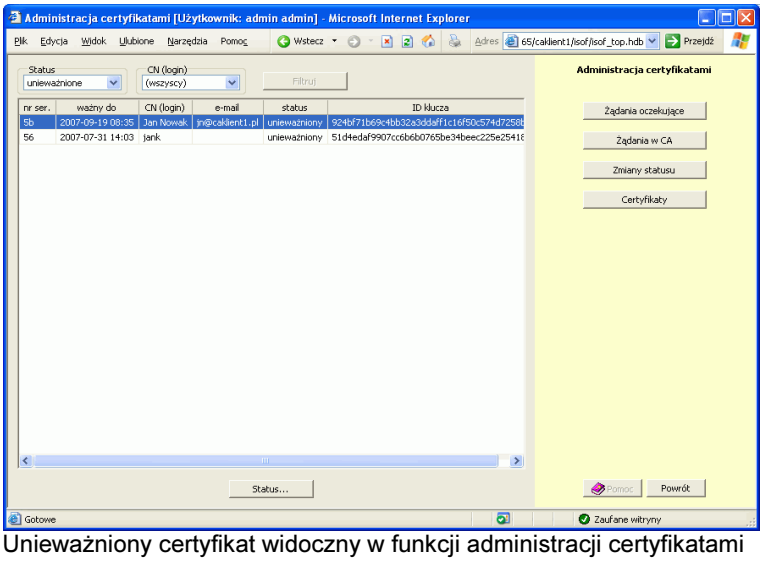
Okienko dialogowe zmiany statusu certyfikatu

Po zaakceptowaniu dialogu widać, że status certyfikatu się nie zmienił – zostało tylko wysłane do CA żądanie zmiany statusu. Widoczne jest ono w widoku *Zmiany statusu*.



Żądanie zmiany statusu widoczne w funkcji administracji certyfikatami

Widok pokazuje domyślnie żądania wysłane, czyli jeszcze nie wykonane przez CA. Dopóki mają one taki status, możliwe jest jeszcze wycofanie ich z CA za pomocą przycisku *Wycofaj*. Po zrealizowaniu znikają z tego widoku oraz z widoku *Certyfikaty*. Po zmianie filtra widoku certyfikatów na *„unieważnione”* lub *„(wszystkie)”* widać, że status certyfikatu zmienił się na *„unieważniony”*.



Unieważniony certyfikat widoczny w funkcji administracji certyfikatami