CERTYFIKATY

Do uzyskania połączenia z systemem CEPIK 2.0 musimy posiadać trzy certyfikaty: VPN, SSL i certyfikat urzędu. VPN i certyfikat urzędu jest jeden na firmę. Te same są instalowane na wszystkich komputerach wykorzystywanych do prowadzenia rejestru badań. Certyfikatów SSL - a co za tym idzie czytników kart kryptograficznych - musi być tyle, ile stanowisk. W związku z tym w "konsoli Windows" obsługującej certyfikaty - na każdym komputerze - powinny być widoczne co najmniej 3 certyfikaty:

1) VPN - najczęściej oznaczony kodem stacji, np. ABC/123 (gdzie właściwość certyfikatu oznaczona jako "Użycie klucza" ma wartość: b8, a właściwość "zamierzone cele" ma najczęściej nieokreśloną wartość: <Wszyscy>)
2) SSL - najczęściej oznaczony kodem stacji, np. ABC/123 (gdzie właściwość certyfikatu oznaczona jako "Użycie klucza" ma wartość: e8, a właściwość "zamierzone cele" ma wartość: Uwierzytelnienie klienta)
3) certyfikat urzędu - oznaczony jako "Infrastruktura"

Brak takich certyfikatów na liście oznacza brak ich rejestracji w magazynie certyfikatów "Osobisty" (SSL i VPN) i "Zaufane główne urzędy certyfikacji" (certyfikat urzędu). Rejestracji certyfikatu SSL wykonujemy z poziomu aplikacji do obsługi czytnika. Pozostałe dwa rejestrujemy bezpośrednio z pobranych plików.

INSTALACJA SSL

Konsola Windows do obsługi certyfikatów zawiera istotne informacje o certyfikatach. Jeśli na liście Certyfikatów nie ma certyfikatu SSL (e8), należy go zainstalować do magazynu certyfikatów o nazwie "Osobisty". Jeśli posiadamy certyfikat w pliku (*.crt), kilkamy go 2-krotnie i postępujemy zgodnie z instrukcjami, pamiętając o wyborze magazynu o nazwie „Osobisty”. W przypadku pobrania certyfikatu "na kartę", do jego rejestracji wykorzystujemy aplikację do obsługi czytnika kart.

Proces rejestracji certyfikatów na przykładzie aplikacji „ENCARD - zarządca kart” (wspierana przez MC wersja: 4.0.8.89):

1) umieścić kartę kryptograficzną w czytniku
2) uruchomić program „ENCARD - zarządca kart”
3) wybrać właściwy czytnik kart z listy (tzw. token)
4) kliknąć na pierwszą ikonę z lewej (Logowanie)
5) rozwinąć wszystkie gałęzie (znaki plus z lewej strony nazw certyfikatów i kluczy)
6) zaznaczyć certyfikat SSL
7) kliknąć ikonę ”Zarejestruj certyfikat” (rejestracja "ręczna" z zaawansowanymi ustawieniami)
8) w ustawieniach zaawansowanych należy zmienić nazwę kontenera na własną

Proces rejestracji certyfikatów z karty CERTUM na przykładzie aplikacji „proCertum Card Manager” (wspierana przez MC wersja: 3.2.0.146) - opis dla wersji 3.2.0.190 lub wyższej poniżej:

1) umieścić kartę kryptograficzną w czytniku
2) uruchomić program „cryptoCertum Card Manager”
3) wybrać właściwy czytnik kart z listy „Nazwa czytnika”

4) nacisnąć klawisz „Czytaj kartę”
5) otworzyć zakładkę „Profil zwykły”
6) nacisnąć klawisz „Rejestruj certyfikaty”

Karty CERTUM rejestrują certyfikaty automatycznie podczas startu systemu Windows lub po podłączeniu czytnika do komputera (należy poczekać kilka-kilkanaście sekund na automatyczną rejestrację).

Dla "proCertum Card Manager" w wersji 3.2.0.190 lub wyższej po zainstalowaniu tego oprogramowania należy:

1) otworzyć program
2) nacisnąć klawisz "Opcje"
3) w sekcji "Opcje profilu zwykłego" włączyć Sterownik: CSP
4) zatwierdzić klawiszem OK i zrestartować Windows
5) po restarcie ponownie uruchomić "proCertum Card Manager"
6) wybrać właściwy czytnik kart z listy „Nazwa czytnika”
7) nacisnąć klawisz "Czytaj kartę"
8) włączyć zakładkę " Profil zwykły"
9) nacisnąć klawisz "Rejestruj certyfikaty"

INSTALACJA VPN

Nieco inaczej wygląda kwestia certyfikatu VPN. Jest on instalowany z pliku *.pfx (*.p12). Ten certyfikat należy pobrać ze strony Ministerstwa Cyfryzacji po uprzednim złożeniu wniosku o certyfikat VPN. Po wygenerowaniu takiego wniosku uzyskamy pierwszą część klucza jednorazowego do późniejszego pobrania certyfikatu. Drugą część klucza otrzymamy w mailu z ministerstwa, w którym również znajdziemy link do strony, z której pobierzemy certyfikat. Proces pobierania wygląda następująco:

1) w przeglądarce internetowej otwieramy stronę: www.cepik.gov.pl/si-cepik-2.0/zdalna-certyfikacja?infrastruktura
2) uruchamiamy link: Generowanie nowych certyfikatów za pomocą kodu jednorazowego użycia w pliku *.p12

Jeśli pojawi się w międzyczasie okienko pytające o zgodę na uruchomienie apletu Java - proszę zezwolić na jego uruchomienie. Nie aktualizujemy samej Javy. Należy obserwować po każdym kolejnym kroku, czego oczekuje od nas przeglądarka, o co pyta na ekranie.

UWAGA: certyfikat można pobrać tylko przy pomocy przeglądarki internetowej obsługującej wtyczkę Java.

Jeśli już uda się uruchomić proces pobierania, wówczas wykonujemy kolejne kroki:

1) wskazujemy docelowe miejsce przechowywania certyfikatu *.pfx i podajemy jego nazwę (np."certyfikat.pfx").

2) w następnym okienku definiujemy hasło, które będzie potrzebne podczas instalacji certyfikatu w systemie Windows. Proponujemy zapisać je do pliku tekstowego do tego samego folderu co plik pfx.
3) w kolejnym okienku "Wprowadź kod jednorazowy", podajemy otwartym tekstem dwie części kodu - pierwsza część jest na wniosku o certyfikat VPN (na pierwszej stronie pod kodem 2D lub na ostatniej stronie), druga jest w mail'u z Ministerstwa Cyfryzacji.
4) następnie proszę wykonać kopię certyfikatu i pliku z hasłem w bezpiecznym miejscu (np. pendrive) i przystąpić do jego instalacji:
   - klikamy dwukrotnie na pobranym pliku "certyfikat.pfx" i naciskamy klawisz "Dalej"
   - podajemy hasło zdefiniowane podczas pobierania (pkt.2)
   - jako miejsce przechowywania wskazujemy magazyn o nazwie "Osobisty"
   - zatwierdzamy i czekamy na potwierdzenie poprawności zainstalowania (2-3 sekundy)

   UWAGA: w wersjach sieciowych operację należy wykonać na każdym stanowisku roboczym.

INSTALACJA CERTYFIKATU URZĘDU

Ostatnim krokiem jest instalacja CERTYFIKATU URZĘDU, bez którego nawiązanie połączenia z CEPIK jest niemożliwe.

Instrukcja instalacji:
- pobrać certyfikat urzędu kilkając w link w oknie głównym SKP PRO: **CERTYFIKAT INFRAC2_CA.crt** lub z poziomu przeglądarki internetowej, wpisując adres:
http://www.stacja.com.pl/upgrades/INFRAC2_CA.crt
- po uruchomieniu pobranego pliku, w okienku "*Pobieranie pliku ...*" nacisnąć klawisz "Otwórz"
- w okienku "*Certyfikat*" nacisnąć klawisz "Zainstaluj certyfikat"
- w kolejnym okienku "*Kreator importu certyfikatów*" nacisnąć "Dalej"
- wybrać opcję "*Umieść wszystkie certyfikaty w następującym magazynie*", nacisnąć klawisz "Przeglądaj", wskazać magazyn o nazwie "*Zaufane główne urzędy certyfikacji*" i zatwierdzić klawiszem "OK"
- w oknie "*Kreator importu certyfikatów*" nacisnąć klawisz "Dalej", a następnie "Zakończ"
- POCZEKAĆ KILKA-KILKANAŚCIE sekund na wyświetlenie komunikatu "*Import został pomyślnie ukończony*"
- zamknąć okienko "Certyfikaty" klawiszem "OK"
Teraz można ponowić połączenie VPN z CEPIK za pomocą oprogramowania Cisco.

UWAGA: w wersjach sieciowych operację należy wykonać na każdym stanowisku roboczym.

W przypadku problemu z zestawieniem połączenia VPN:

UWAGA: Tę część polecamy wykonać tylko i wyłącznie osobom o wiedzy informatycznej.

Może być konieczne „oczyszczenie” wszystkich magazynów certyfikatów z tych posiadających w swojej nazwie słowo „Infrastruktura”. Niezależnie od daty ważności takiego certyfikatu, należy go usunąć i powtórzyć powyższe kroki. Aby oczyścić magazyny należy:
- uruchomić konsolę certyfikatów z wiersza poleceń wpisując: certmgr.msc
- wybrać polecenie: Akcja > Znajdź certyfikaty > w polu „Zawiera” wpisać słowo „Infrastruktura”
- usunąć te, które w polu „Wystawiony dla” zawierają słowo „Infrastruktura” (TYLKO TE!)
- zainstalować pobrany powyżej certyfikat urzędu.

UWAGI

Jeśli próba połączenia z CEPIK 2.0 z poziomu programu SKP PRO daje wynik w postaci komunikatu „Connection lost (error code is 100353)” może to świadczyć o:

- braku dostępności serwisu CEPIK
- braku aktualnego certyfikatu SSL, o którym mowa powyżej lub jego niepoprawnym zarejestrowaniu w systemie Windows
- niepoprawnym działaniu czytnika karty kryptograficznej lub jej uszkodzeniu

Inną przyczyną takiego stanu może być oprogramowanie blokujące programowi SKP PRO dostęp do internetu. We wszystkich programach zabezpieczających należy włączyć (ustawić) tzw. wyjątki (wykluczenia) wskazując jako wyjątek, cały folder pakietu SKP PRO.