Certyfikaty

- Certyfikaty w portalu PLGrid
  - Certyfikat Simple CA
  - Certyfikat Polish Grid CA
  - Udogodnienia dotyczące certyfikatów w Infrastrukturze PLGrid - certyfikat główny
- Operacje na certyfikatach
  - Konwersja certyfikatu
  - Import certyfikatu do przeglądarki
  - Kopiowanie certyfikatu na UI
- Zalecenia bezpieczeństwa
- Simple CA i Polish Grid CA - dodatkowe informacje
  - Polish Grid CA - szczegóły

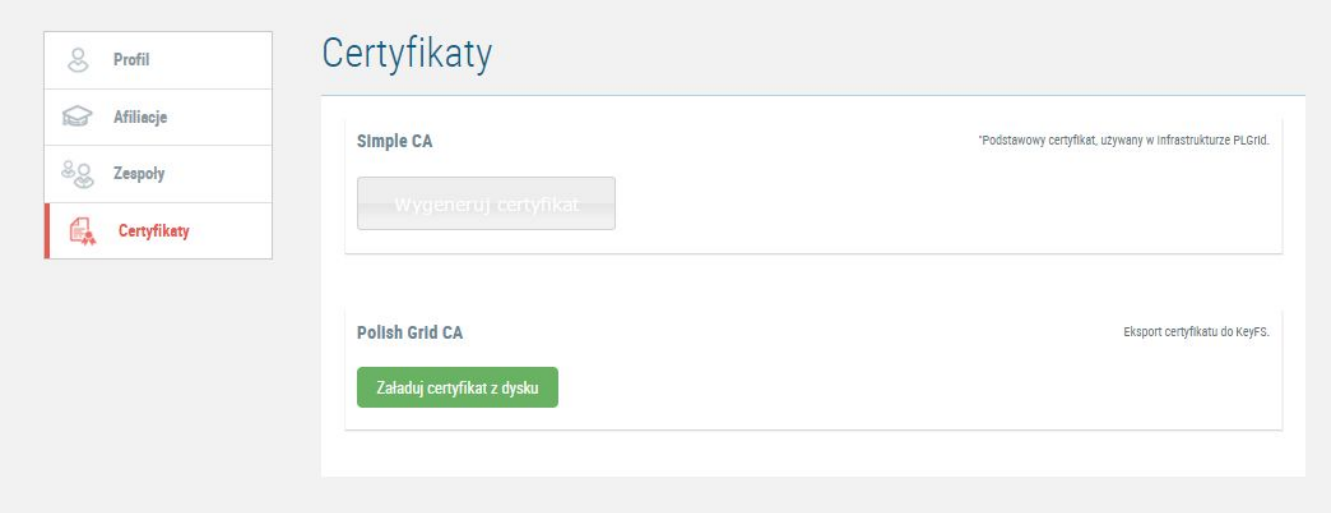
Certyfikaty w portalu PLGrid

Z pomocą certyfikatu można wygodniej korzystać z Infrastruktury PLGrid. Stanowi on poświadczenie tożsamości użytkownika i umożliwia dostęp do usług oraz do Portalu PLGrid bez konieczności każdorazowego podawania loginu oraz hasła podczas logowania.

Zarządzanie certyfikatami odbywa się z widoku **Certyfikaty** w Portalu.

W ramach Infrastruktury PLGrid stosujemy 2 typy certyfikatów:

- **Simple CA**
- **Polish Grid CA**

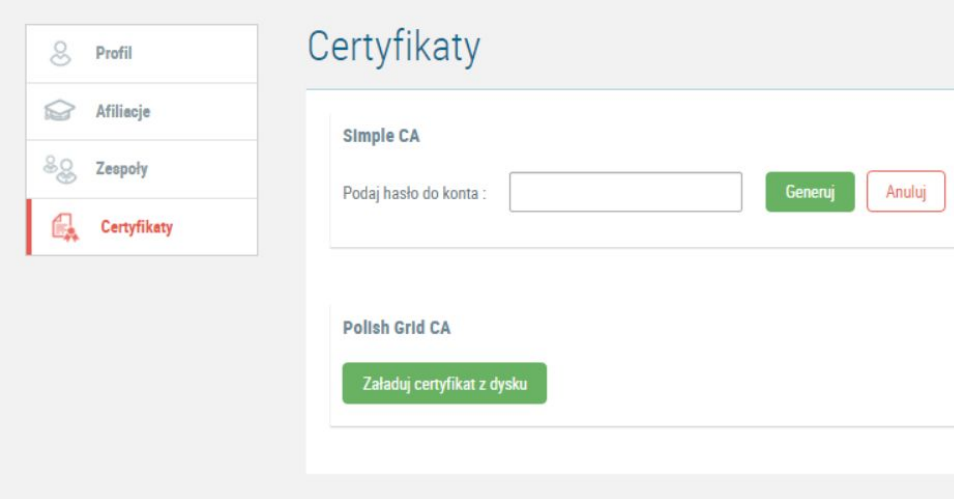


Widok Certyfikaty

Certyfikat Simple CA

Simple CA wystawiany jest w Portalu i nie wymaga dodatkowej weryfikacji tożsamości. Generowany jest w zakładce **"Certyfikaty"** za pomocą opcji **"Wygeneruj certyfikat".**

Po kliknięciu **"Wygeneruj certyfikat"** pojawi się widok z polem do podania hasła - tego samego, które używane jest do zalogowania się do Portalu. Po podaniu poprawnego hasła wybieramy opcję **"Generuj"** - po chwili pojawi się informacja o wygenerowanej paczce w postaci pliku p12 z certyfikatem i kluczem prywatnym, który można zapisać na dysku.



Widok Generuj Certyfikat

Jeśli użytkownik nie ma certyfikatu Polish Grid CA zarejestrowanego w portalu, wówczas certyfikat Simple CA po wygenerowaniu automatycznie ustawia się jako główny: może służyć do autologowania do Portalu, zapisuje się w keyFS i w OpenID. W przeciwnym wypadku użytkownik może wybrać, które certyfikat ustawić jako główny.

Plik certyfikatu możemy zapisać w przeglądarce w celu umożliwienia logowania się do Portalu bez konieczności podawania każdorazowo hasła i loginu.

Unieważnienie Simple CA

Istnieje możliwość unieważnienia certyfikatu. W sytuacji kiedy certyfikat zostanie skompromitowany przez udostępnienie go osobom trzecim, użytkownik ma możliwość unieważnienia obecnego certyfikatu oraz wygenerowanie kolejnego.

Certyfikat można też odwołać, jeśli dane użytkownika (np. nazwisko) uległy zmianie lub gdy użytkownik nie potrzebuje już certyfikatu.

Uwaga

Unieważnienie certyfikatu powoduje jego usunięcie z Portalu i wszystkich narzędzi, do których Portal je przesłał.

Odnowienie Simple CA

Certyfikat Simple CA jest ważny przez rok. Aby przedłużyć ważność certyfikatu, należy unieważnić stary certyfikat (jeśli jest jeszcze aktywny), a następnie zaaplikować o nowy. Miesiąc przed datą wygaśnięcia certyfikatu system generuje stosowną informację.

Certyfikat Polish Grid CA

Polish Grid CA wystawiany jest przez Urząd Certyfikacji Polish Grid CA i jest respektowany przez inne europejskie infrastruktury gridowe.

W zasadzie nie powinien być potrzebny użytkownikom podczas korzystania z Infrastruktury PLGrid.

Aby uzyskać ten certyfikat, należy przejść na stronę: https://plgrid-ca.pl/, gdzie dostępne są instrukcje oraz informacje o tym, w jaki sposób przejść procedurę wnioskowania.

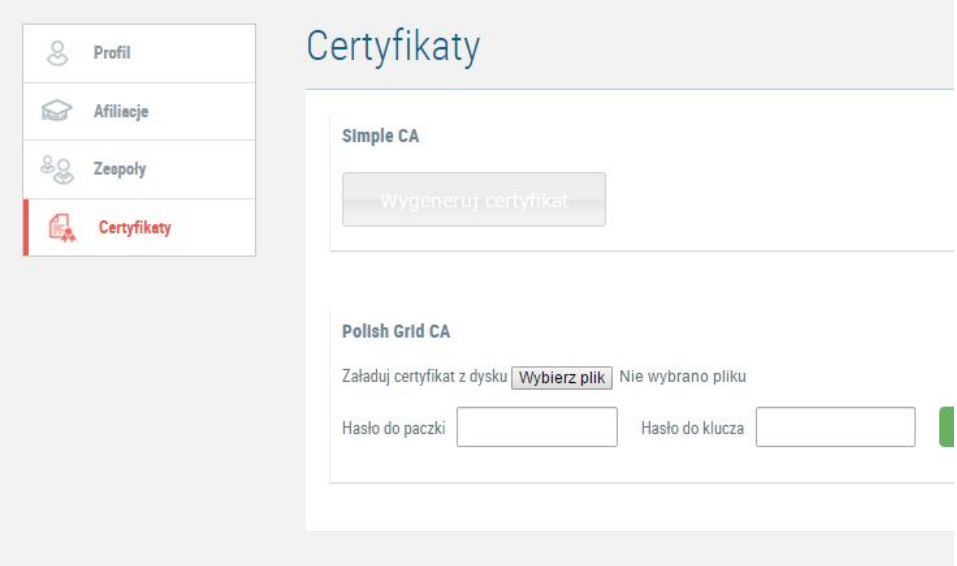
Po wystawieniu certyfikatu użytkownik otrzymuje wiadomość e-mail z odnośnikiem do pobrania certyfikatu.

Użytkownik może zapisać certyfikat na lokalnym dysku (w formacie PEM) lub pobrać bezpośrednio do przeglądarki, z której występował z wnioskiem o certyfikat. Jeżeli certyfikat zostanie pobrany w formacie PEM, trzeba skonwertować certyfikat do formatu PKCS12, a następnie zainstalować go w przeglądarce oraz zarejestrować w Portalu.

Rejestracja Polish Grid CA w Portalu

Rejestracji certyfikatu Polish Grid CA można dokonać w przestrzeni "**Certyfikaty**" w polu "**Polish Grid CA**" za pomocą opcji "**Załaduj certyfikat z dysku**".

Pojawią się pola z hasłem do paczki oraz hasłem do klucza i możliwość zainstalowania skonwertowanego pliku. Po uzupełnieniu danych za pomocą opcji "Wyślij" rejestrujemy paczkę w Portalu.



Widok rejestracji certyfikatu Polish Grid CA w Portalu

Jeśli użytkownik posiada już certyfikat zarejestrowany w Portalu (Simple CA rejestruje się automatycznie po wygenerowaniu), a następnie zarejestruje kolejny certyfikat (np. Polish Grid CA), wówczas ma możliwość ustawienia dowolnego certyfikatu jako głównego, co umożliwia autologowanie tym certyfikatem do portalu oraz zapisanie go w keyFS i w OpenID.

Udogodnienia dotyczące certyfikatów w Infrastrukturze PLGrid - certyfikat główny

W Infrastrukturze PLGrid istnieje szereg udogodnień dotyczących certyfikatów, do których należą:

- możliwość autologowania do portalu za pomocą certyfikatu zarejestrowanego w przeglądarce,
- umieszczenie certyfikatu w keyFS, co pozwala na generowanie proxy na maszynie dostępowej bez konieczności kopiowania certyfikatu na nią,
- umieszczenie certyfikatu w OpenID, co pozwala na generowanie proxy za pomocą OpenID w portalu usługi.

Udogodnienia te działają dla certyfikatu ustawionego jako główny w portalu PLGrid.

Rejestracja certyfikatu w portalu w momencie, gdy użytkownik nie ma żadnego innego certyfikatu w portalu, powoduje automatyczne ustawienie tego certyfikatu jako główny.

W przypadku gdy użytkownik rejestruje w portalu drugi certyfikat, pojawia się przycisk "Ustaw jako główny certyfikat", umożliwiający ustawienie wybranego certyfikatu jako główny

Operacje na certyfikatach

Konwersja certyfikatu

Do operacji związanych z certyfikatami (m.in. konwersji) konieczne jest posiadanie dostępu do komputera z zainstalowanym narzędziem **openssl.** Można z niego skorzystać na maszynach dostępowych (UI).

PKCS12 → PEM

Generowanie certyfikatu proxy wymaga użycia certyfikatu użytkownika oraz klucza prywatnego. Można je uzyskać z kontenera PKCS12 otrzymanego z portalu (Simple CA) lub wyeksportowanego z przeglądarki (Polish Grid CA). W tym celu należy wykonać polecenia:

```
$ openssl pkcs12 -nocerts -in usercred.p12 -out userkey.pem
$ openssl pkcs12 -clcerts -nokeys -in usercred.p12 -out usercert.pem
$ chmod 644 usercert.pem
$ chmod 400 userkey.pem
```

Gdzie:

- usercred.p12 - ścieżka do paczki PKCS12
- userkey.pem - klucz prywatny użytkownika

- usercert.pem - certyfikat użytkownika

PEM → PKCS12

Natomiast tworzenie kontenera PKCS12 z plików z certyfikatem oraz kluczem przeprowadzane jest następująco:

```
$ openssl pkcs12 -export -descert -inkey userkey.pem -in usercert.pem -out usercred.p12 -name "Certyfikat
vo. plgrid"
```

Gdzie:

- userkey.pem - ścieżka do klucza prywatnego użytkownika
- usercert.pem - ścieżka do certyfikatu użytkownika
- usercred.p12 - uzyskana paczka PKCS12
- "Certifikat vo. plgrid" - opcjonalna nazwa dla Twojego certyfikatu. Ma ona za zadanie ułatwić wybór odpowiedniego certyfikatu w przeglądarce.

Import certyfikatu do przeglądarki

Certyfikat można zaimportować do przeglądarki internetowej, aby móc korzystać z certyfikatu do bezhasłowego logowania się do stron PLGrid.

W celu importu certyfikatu uruchom przeglądarkę na Twoim lokalnym komputerze, na który został skopiowany certyfikat w formacie PKCS12 (np. usercred.p12).

Instrukcja importu zależy od używanej przeglądarki i systemu operacyjnego:

Firefox (Windows)

- Narzędzia → Opcje → Zaawansowane → Szyfrowanie → Wyświetl certyfikaty → Użytkownik → Importuj
- Tools → Options → Advanced → Security → Manage certificates → Your certificates → Import

Firefox (Linux)

- Edycja → Preferencje → Zaawansowane → Szyfrowanie → Wyświetl certyfikaty → Użytkownik → Importuj
- Edit → Preferences → Advanced → Certificates → View certificates → Your certificates → Import

Internet Explorer

  - Narzędzia → Opcje internetowe → Zawartość → Certyfikaty → Importuj
  - Tools → Internet Options → Content → Certificates → Import

Google Chrome

    - Opcje → Dla zaawansowanych → Zarządzaj certyfikatami → Importuj
    - Options → Under the Hood → Manage certificates... → Import...

⚠ W przypadku importu certyfikatu do przeglądarek Google Chrome oraz Internet Explorer w kroku dotyczącym wyboru **Magazynu certyfikatów** należy wybrać opcję: "Automatycznie wybierz magazyn certyfikatów na podstawie typu certyfikatu"

Mozilla, Netscape (ver. 7.x)

- Edycja → Preferencje → Prywatność i zabezpieczenia → Certyfikaty → Menedżer certyfikatów → Twoje certyfikaty → Importuj
- Edit → Preferences → Privacy & Security → Certificates → Manage Certificates → Import Certificate

Netscape (ver. 4.x)

- Tools → Security Info → Certificates/yours → Import a Certificate

Opera

- Ustawienia → Preferencje → Zaawansowane → Bezpieczeństwo → Zarządzaj certyfikatami → Importuj
- Tools → Preferences → Advanced → Security → Manage Certificates → Personal → Import

Konqueror

- Settings → Configure Konqueror → Crypto → Your certificates → Import

Kopiowanie certyfikatu na UI

Użytkownik może własnoręcznie skopiować certyfikat na maszyny dostępowe, z których chce skorzystać. Aby uzyskać dostęp do UI należy aktywować odpowiednie usługi dostępowe w Portalu. Dalsze instrukcje zakładają, że usługi te zostały aktywowane.

W szczególności poniżej opisano postępowanie dla certyfikatów wystawionych przez Polish Grid CA oraz PLGrid SimpleCA. Domyślną ścieżką, w której oprogramowanie pośredniczące gLite szuka certyfikatów użytkownika jest katalog ~/.globus.

Procedura:

- Skopiuj uzyskany certyfikat i klucz prywatny w formacie PEM i/lub w formacie PKCS12 na maszynę dostępową (więcej na temat metod kopiowania znajduje się w osobnym rozdziale). Przykład:

```
$ scp usercert.pem userkey.pem usercred.p12 login@ui.cyfronet.pl:.globus/
```

- Jeżeli katalog `.globus` nie został odnaleziony zaloguj się na maszynie dostępowej (więcej na temat metod logowania znajduje się w osobnym rozdziale) i utwórz ten katalog poleceniem:

```
$ mkdir ~/.globus
```

następnie powtórz próbę kopiowania.

- Po zalogowaniu na maszynę dostępową należy upewnić się, że ustawione są dobre prawa dostępu do plików. Przykład:

```
$ cd ~/.globus
$ chmod 600 usercred.p12
$ chmod 644 usercert.pem
$ chmod 400 userkey.pem
```

Zalecenia bezpieczeństwa

- Klucz prywatny wygenerowany podczas tworzenia certyfikatu należy bezwzględnie chronić przed dostępem osób trzecich.
- Zaleca się wykonanie kopii zapasowej pary kluczy (klucz prywatny i certyfikat) i przechowywanie jej w bezpiecznym miejscu.
- W razie kompromitacji certyfikatu należy go natychmiast odwołać i poinformować o tym fakcie Operatora PLGrid, pisząc zgłoszenie na Helpdesk.

Simple CA i Polish Grid CA - dodatkowe informacje

Simple CA i Polish Grid CA to certyfikaty osobiste zgodne ze standardem X.509, które poświadczają tożsamość użytkownika. Z punktu widzenia użytkownika certyfikat jest po prostu plikiem (bądź plikami) zawierającym dane certyfikujące. Niektóre z tych plików są chronione hasłem znanym jedynie osobie, do której należy certyfikat.

Certyfikat może być dołączany do zadań obliczeniowych, a także służy do logowania się do różnych narzędzi PLGrid bez konieczności podawania hasła.

Użytkownikom PLGridu certyfikat mogą wystawić dwa centra certyfikacji (ang. *Certification Authority*, CA):

- Simple CA (http://plgrid-sca.wcss.wroc.pl),
- Polish Grid CA (https://plgrid-ca.pl).

Certyfikaty wystawiane przez **Simple CA** są łatwiejsze do uzyskania i respektowane tylko w ramach infrastruktury PLGrid. Tożsamość osoby będącej użytkownikiem PLGridu nie musi już być dodatkowo weryfikowana podczas ubiegania się o certyfikat Simple CA.

Certyfikaty podpisywane przez **Polish Grid CA** są trudniejsze do uzyskania, jednak mogą być respektowane także w infrastrukturze europejskiej, poza PLGridem. Tożsamość użytkownika PLGrid musi być dodatkowo zweryfikowana przez jeden z Urzędów Rejestracji Polish Grid CA (ang. *Registration Authority*, RA).

Użytkownik składa wniosek o certyfikat do wybranego przez siebie CA. Można złożyć też dwa niezależne wnioski do każdego z CA.

Polish Grid CA - szczegóły

Aplikowanie o certyfikat

Użytkownik infrastruktury PLGrid może wystąpić o certyfikat do Polish Grid CA za pośrednictwem strony WWW (https://plgrid-ca.pl/) lub wysyłając pocztą elektroniczną odpowiednio przygotowane zlecenie certyfikacji.

Strona WWW pozwala na składanie nowych wniosków o certyfikat poprzez:

- wygenerowanie pary kluczy oraz wniosku przez przeglądarkę (opcja "Utwórz certyfikat osobisty"),
- wygenerowanie pary kluczy oraz wniosku przez użytkownika (opcja "Utwórz certyfikat osobisty w oparciu o wniosek CSR").

Różnica polega tylko na miejscu przechowywania i sposobie generowania klucza prywatnego. W pierwszej opcji klucz prywatny jest przechowywany w przeglądarce (można go wyeksportować do pliku) w drugiej opcji to użytkownik jest odpowiedzialny za ochronę i przechowywanie klucza prywatnego.

Generowanie pary kluczy i wniosku przez przeglądarkę

Aby przejść do formularza zgłaszającego wniosek o certyfikat w przeglądarce należy wybrać z menu pozycję "Stwórz certyfikat" a następnie opcję "Utwórz certyfikat osobisty". W formularzu trzeba podać swoje imię, nazwisko, adres email oraz nazwę organizacji, do której się należy. Opcjonalnie można także podać modyfikator pola CN (np. nazwa dodatkowej organizacji), dodać adres email do certyfikatu (email zostanie dodany do certyfikatu jako pole w *Subject Alternative Name*) lub do nazwy wyróżniającej (ang. *Distinguished Name*, DN). Po uzupełnieniu pól formularza na stronie pojawi się pole pokazujące DN, jaki zostanie użyty do wygenerowania nowego wniosku o certyfikat. Jeżeli wszystko się zgadza to należy kliknąć przycisk "Złóż wniosek o certyfikat".

Na podany we wniosku adres email zostanie wysłana wiadomość, którą trzeba odebrać, przejść na wskazany adres internetowy oraz skopiować przesłane w wiadomości hasło. Po przejściu na podaną stronę mamy możliwość wybrania długości klucza publicznego (w różnych przeglądarkach jest to obsługiwane w różny sposób). Po wybraniu długości klucza (system Polish Grid CA akceptuje klucze o długości minimum 2048 bitów), podaniu hasła oraz kliknięciu przycisku "Złóż wniosek o certyfikat" przeglądarka zacznie generować klucz prywatny oraz wyśle wniosek o certyfikat do centrum certyfikacji Polish Grid CA.

Generowanie pary kluczy i wniosku przez użytkownika

Jeżeli użytkownik chce wygenerować klucze oraz wniosek osobiście, może to zrobić przy użyciu programu OpenSSL. Podczas generowania nowego wniosku o certyfikat programem OpenSSL należy zastosować format pola DN wymagany przez Polish Grid CA. Reguły dotyczące formatowania DN spisane są na stronie "Reguły dotyczące formatowania DN".

- Jeżeli użytkownik nie jest pewien czy dobrze wygenerował klucz i wniosek lub nie wie jak to zrobić, może przejść na stronę Generowanie komendy w programie OpenSSL, która pomoże przygotować odpowiednie polecenie programu OpenSSL.
- W poleceniu programu OpenSSL nie można stosować polskich znaków (np. podając imię i nazwisko).
- Wielkość liter podana w opcji `-subj` ma znaczenie.

Po wygenerowaniu klucza prywatnego i wniosku należy przejść na stronę Utwórz certyfikat osobisty w oparciu o wniosek CSR i wypełnić formularz. W miejsce "Plik wniosku CSR" należy podać wygenerowany przed chwilą plik (z rozszerzeniem .csr). Oprócz tego trzeba podać imię, nazwisko, adres email oraz nazwę organizacji, do której się należy. Po wypełnieniu wniosku trzeba kliknąć przycisk "Złóż wniosek o certyfikat".

Na podany w formularzu adres email wysłana zostanie wiadomość zawierająca adres internetowy, na który trzeba przejść w celu potwierdzenia odebrania wiadomości. Po przejściu na w/w stronę, należy przekopiować hasło, które zostało przesłane w wiadomości email i kliknąć przycisk "Złóż wniosek o certyfikat".

Weryfikacja tożsamości w RA

Po złożeniu wniosku o certyfikat oraz potwierdzeniu adresu email kolejnym krokiem jest potwierdzenie swojej tożsamości w odpowiednim Urzędzie Rejestracji (RA).

W poprzednim kroku system przyjął zgłoszenie i wyświetlił stronę zawierającą dalsze informacje. Jeżeli przypadkiem strona ta została zamknięta to zawsze mona do niej powrócić korzystając z odnośnika w ostatniej wiadomości email lub przechodząc na stronę Sprawdź status wniosku o certyfikat i podając swoją nazwę użytkownika (wygenerowaną przez system, wysłaną do użytkownika w wiadomości email).

Aby potwierdzić swoją tożsamość w RA trzeba pobrać "Wniosek o certyfikat Polish Grid CA", wydrukować go, wypełnić i przynieść do najbliższego Urzędu Rejestracji (RA). Lista osób, do których można przyjść potwierdzić tożsamość jest podana na w/w stronie.

Osoby, które nie mogą skontaktować się osobiście z żadnym z powyższych RA proszone są o kontakt z CA (ca@plgrid-ca.pl) w celu ustalenia innej możliwości weryfikacji tożsamości.

Pobranie certyfikatu

Po potwierdzeniu tożsamości przez jedno z RA CA wystawia certyfikat na podstawie danych zawartych w elektronicznym zleceniu certyfikatu. Po wystawieniu certyfikatu użytkownik otrzymuje wiadomość email z odnośnikiem do pobrania certyfikatu.

Użytkownik może zapisać certyfikat na lokalnym dysku (w formacie PEM) lub pobrać bezpośrednio do przeglądarki, z której występował z wnioskiem o certyfikat. Jeżeli certyfikat zostanie pobrany w formacie PEM to trzeba skonwertować certyfikat do formatu PKCS12 a następnie zainstalować go w przeglądarce oraz zarejestrować w portalu.

Odnowienie certyfikatu

Jeżeli certyfikat jest jeszcze ważny można go odnowić bez pośrednictwa RA za pomocą strony https://plgrid-ca.pl.

Jeśli dotychczasowy certyfikat stracił już ważność, a użytkownik chce zachować w nowym certyfikacie ten sam DN, to powinien zgłosić się do RA po instrukcje postępowania w takim przypadku.

- Przy odnowieniu certyfikatu należy zmienić klucz prywatny! Nie można tworzyć nowego wniosku na podstawie poprzedniego certyfikatu, ani nie można przesyłać ponownie tego samego wniosku.
- Trzeba uważać, żeby nie nadpisać sobie poprzedniego certyfikatu i klucza!

Odnawianie certyfikatu zainstalowanego w przeglądarce

Aby odnowić certyfikat w przeglądarce, należy otworzyć stronę Odnów certyfikat osobisty zainstalowany w przeglądarce przy użyciu dotychczasowego certyfikatu wystawionego przez Polish Grid CA. Jeżeli certyfikat ten nie został użyty, należy zamknąć przeglądarkę i otworzyć ponownie w/w stronę. Po wybraniu długości nowego klucza publicznego i opcjonalnym uaktualnieniu posiadanego adresu email trzeba kliknąć przycisk "Odnów certyfikat". System sprawdzi poprawność zgłoszenia i jeżeli zlecenie zostanie pozytywnie zweryfikowane prześle prośbę o odnowienie certyfikatu bezpośrednio do CA. Użytkownik musi teraz poczekać na otrzymanie na podany adres email wiadomości o wygenerowaniu nowego certyfikatu.

Odnawianie certyfikatu na podstawie pliku PEM

Jeżeli użytkownik nie posiada certyfikatu zaimportowanego do przeglądarki, ale posiada pliki wygenerowane podczas poprzedniego składania wniosku o certyfikat oraz wydany przez Polish Grid CA poprawny i ważny certyfikat to musi przejść na stronę Odnów certyfikat osobisty w oparciu o CSR. W celu odnowienia certyfikatu osobistego, należy przesłać nowy wniosek podpisany przez stary, ciągle ważny certyfikat.

W nowym wniosku pole DN musi być takie samo jak w aktualnie ważnym certyfikacie.

Jeżeli użytkownik nie wie jak wygenerować nowy wniosek powinien przejść na stronę Generowanie komendy w programie OpenSSL.

Aby podpisać nowy wygenerowany CSR swoim certyfikatem użytkownik może użyć następującej komendy OpenSSL:

```
openssl smime -sign -in your_new_csr.pem -out new_csr.signed -signer your_valid_certificate.pem -inkey
private.key -text
```

Gdzie:

- `your_new_csr.pem` jest nowym wnioskiem wygenerowanym krok wcześniej,
- `private.key` jest kluczem prywatnym zgodnym z aktualnym certyfikatem,
- `new_csr.signed` jest nazwą pliku z jaką ma zostać zapisany nowy podpisany wniosek
- `your_valid_certificate.pem` jest plikiem z aktualnym, ważnym certyfikatem

Po wygenerowaniu nowego wniosku podpisanego certyfikatem trzeba przejść na stronę Odnów certyfikat osobisty w oparciu o CSR, wskazać plik z wnioskiem i opcjonalnie uaktualnić adres email. System sprawdzi poprawność zgłoszenia i jeżeli wszystko zostanie pozytywnie zweryfikowane prześle prośbę o odnowienie certyfikatu bezpośrednio do CA. Użytkownik musi teraz poczekać na otrzymanie na podany adres email wiadomości o wygenerowaniu nowego certyfikatu.

Pobranie certyfikatu

Po wygenerowaniu certyfikatu przez CA użytkownik otrzymuje wiadomość email z odnośnikiem do pobrania certyfikatu. Użytkownik może zapisać certyfikat na lokalnym dysku (w formacie PEM) lub pobrać bezpośrednio do przeglądarki, z której występował z wnioskiem o certyfikat.

Unieważnienie certyfikatu

Aby unieważnić swój certyfikat osobisty zaimportowany w przeglądarce należy przejść na stronę Unieważnij certyfikat osobisty w przeglądarce podają c certyfikat, który ma zostać unieważniony. Po podaniu powodu unieważnienia wskazany certyfikat zostanie zgłoszony do odwołania. Po potwierdzeniu unieważnienia przez CA certyfikat staje się nieważny.

Problemy

W razie problemów z uzyskaniem lub unieważnieniem certyfikatu, można skorzystać z serwisu Helpdesk (http://helpdesk.plgrid.pl) lub bezpośrednio kontaktować się z Polish Grid CA (https://plgrid-ca.pl/contact.jsp).

SPRAWDŹ: **SŁOWNICZEK**