

Instrukcja –

Certum Commercial SSL



Aktywacja certyfikatu Certum Commercial SSL

wersja 1.4



Spis treści

1. Opis produktu.....	3
2. Aktywacja produktu	3
2.1. Dodanie kodu aktywacyjnego	3
2.2. Rozpoczęcie aktywacji certyfikatu.....	4
2.2.1. Metoda aktywacji – generowanie pary kluczy	5
2.2.2. Metoda aktywacji – żądanie CSR.....	8
3. Wypełnienie formularza przy aktywacji	8
4. Weryfikacja dostępu do domeny	10
4.1. Weryfikacja administratorskiego adresu email.....	12
4.2. Weryfikacja dostępu do domeny przez umieszczenie na serwerze pliku	12
4.3. Weryfikacja dostępu do domeny przez stworzenie odpowiedniego rekordu TXT w zasobach DNS	12
5. Pobranie certyfikatu	13
5.1. Pobranie pliku pfx/p12, po wykonaniu aktywacji metodą generowania pary kluczy	14
5.2. Pobranie pliku certyfikatu i klucza prywatnego (metoda CSR)	15

1. Opis produktu

Certyfikat SSL (TLS) to protokół bezpieczeństwa poświadczający autentyczność domeny i jej właściciela. Szyfruje i zabezpiecza ruch na stronach internetowych, w tym transmisję poufnych danych, które klienci wprowadzają w Twoim serwisie. Dzięki certyfikatowi SSL dane osobowe, loginy i hasła, numery kart kredytowych i inne dane Twoich klientów będą zabezpieczone.

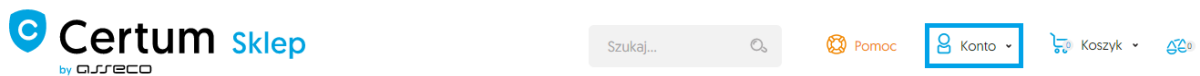
2. Aktywacja produktu

Instrukcja przygotowana jest na przykładzie przeglądarki Google Chrome i dotyczy procesu aktywacji certyfikatu [Certum Commercial SSL](#).

Po złożonym zamówieniu w sklepie Certum aktywacja dostępna będzie z poziomu konta w zakładce [Aktywacja certyfikatów](#) (patrz rozdział 2.2).

2.1. Dodanie kodu aktywacyjnego

Jeżeli chcesz aktywować produkt z otrzymanego np. na adres email kodu elektronicznego – przed rozpoczęciem aktywacji kod dodaj w zakładce [Kody elektroniczne](#). W tym celu zaloguj się do konta na stronie <https://sklep.certum.pl>



W przypadku gdy nie posiadasz konta kliknij na przycisk [Zakładam konto](#), dzięki temu utworzysz nowe konto. Jeżeli posiadasz już konto wybierz opcję [Zaloguj się](#).

Logowanie

Zarejestrowani klienci

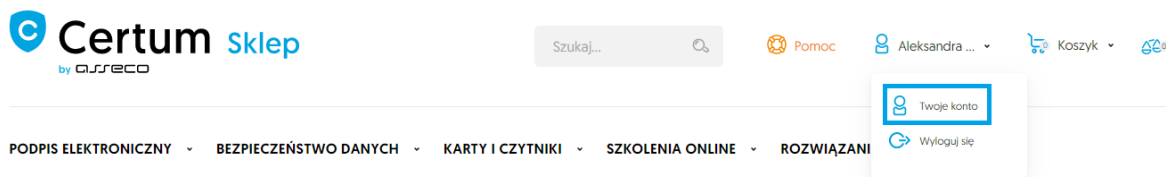
[Zaloguj się](#)[Nie pamiętasz hasła?](#)

Nowi klienci

Posiadanie konta ma wiele zalet. Szybszy proces składania zamówienia, możliwość zapisywania swoich adresów i śledzenie stanu zamówień to tylko niektóre z nich.

[Zakładam konto](#)

Po zalogowaniu się kliknij na panel klienta – [Twoje konto](#).



Aby dodać kod należy wybrać zakładkę [Kody elektroniczne](#). W polu [Nowy kod z karty aktywacyjnej](#) wpisz posiadany kod i kliknij [Dodaj](#).

Uwaga! Pamiętaj, że kod aktywacyjny składa się z 16 znaków. Po wpisaniu lub skopiowaniu kodu sprawdź czy ilość znaków się zgadza.

Twoje konto

- Twoje konto
- Zamówienia
- Produkty do pobrania
- Książka adresowa
- Dane konta
- Kody elektroniczne**
- Subskrypcje newslettera
- Salda konta
- Karty zarejestrowane w Dotpay
- Archiwalne zamówienia
- Aktywacja certyfikatów
- Zarządzanie certyfikatami
- Narzędzia ▾
- Weryfikacja domen

Kody elektroniczne

Nowy kod z karty aktywacyjnej

Twoje kody

Zakupione w sklepie

Wprowadzone ręcznie

Szukaj kodu 🔍

Wszystkie kody ▾

Nie znaleziono kodów spełniających warunki.

Gdy poprawnie wprowadzisz kod, produkt pojawi się na liście w sekcji [Twoje kody/Wprowadzone ręcznie](#). Po przetworzeniu kodu przejdź do zakładki [Aktywacja Certyfikatów](#) (patrz kolejny punkt 2.2).

2.2. Rozpoczęcie aktywacji certyfikatu

Po złożonym zamówieniu lub dodaniu kodu do konta, aktywację rozpocznij w zakładce [Aktywacja certyfikatów](#).

Kody elektroniczne
Aktywacja certyfikatów
Zarządzanie certyfikatami
Historia zamówień
Dane adresowe
Narzędzia
Weryfikacja domen
Newsletter
Wsparcie techniczne
Wiedza

Aktywacja certyfikatów

Nazwa usługi

Status aktywacji

Numer zamówienia

Status płatności

Odszukaj na liście odpowiedni certyfikat i kliknij [Aktywuj](#).

Nazwa usługi	Data zamówienia ▼	Numer zamówienia	Status płatności
Commercial SSL, 1 rok Wydanie	9 sierpień 2019	ZDRAPKA/nLiHWhexitpvJObB/09/08/19	Zaksięgowano Certyfikat nieaktywny <input type="button" value="Aktywuj"/>

Ważna informacja! Do wyboru będą dwie metody aktywacji certyfikatu. Zalecamy użycie metody CSR, dzięki której uzyskasz plik certyfikatu (część publiczną) i klucz prywatny. W przypadku tej metody najpierw należy wygenerować żądanie CSR:

- przez administratora serwera lub
- za pomocą [generatora CSR](#), dostępnego na koncie użytkownika sklepu Certum

Jeżeli potrzebujesz plik pfx/p12, możesz wybrać metodę generowania pary kluczy.

2.2.1. Metoda aktywacji – generowanie pary kluczy

Jeżeli aktywację chcesz wykonać metodą generowania pary kluczy kliknij na przycisk [Dalej](#).

Aktywacja

1. Zamówienia 2. Wybór metody 3. Klucze 4. Dane 5. Potwierdzenie

Nazwa usługi **Commercial SSL, 1 rok**
WydanieWybierz sposób dostarczenia kluczy dla certyfikatu
 Generowanie pary kluczy
 CSR

Utwórz żądanie CSR. Jeśli potrzebujesz dodatkowych informacji na temat sposobów przygotowania żądania CSR, przejdź w zakładki Wsparcie techniczne lub skontaktuj się z operatorem naszej infolinii.

Dalej >>

W celu wygenerowania kluczy pobierz i uruchom aplikację [Certum CryptoAgent](#) (do uruchomienia aplikacji niezbędne jest zainstalowane na komputerze środowisko Java <https://www.java.com/pl/>).

Aktywacja

1. Zamówienia 2. Wybór metody 3. Klucze 4. Dane 5. Potwierdzenie

Nazwa usługi **Commercial SSL, 1 rok**
Wydanie

W celu aktywacji certyfikatu pobierz i uruchom aplikację Certum CryptoAgent.

Uruchom Aplikację CryptoAgent



Do uruchomienia aplikacji Certum CryptoAgent niezbędne jest posiadanie najnowszej wersji środowiska JVM (Java Virtual Machine).

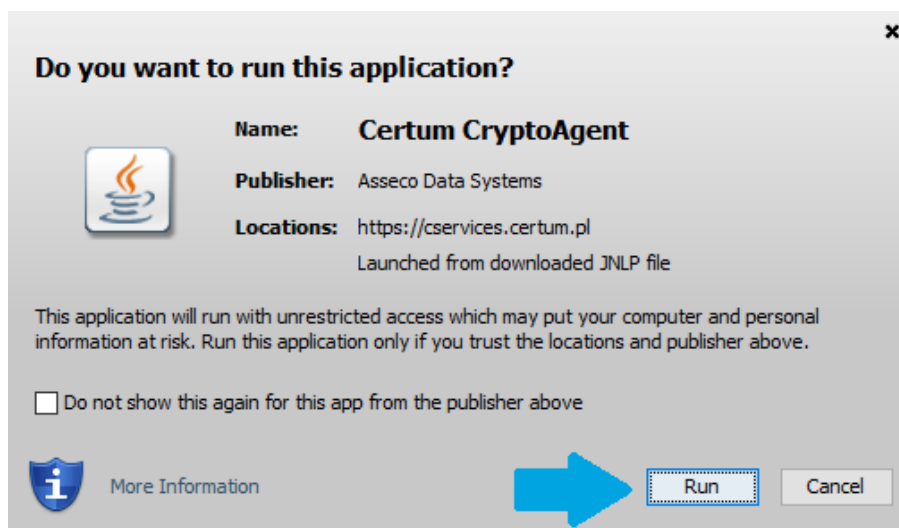
UWAGA: Aplikacja Certum CryptoAgent musi być uruchomiona przez cały okres trwania procesu instalacji certyfikatu na kartę.

<< Wstecz

Dalej >>

Na dolnym pasku przeglądarki pojawi się komunikat ostrzegawczy, przy którym kliknij na przycisk [Zachowaj](#), aby pobrać aplikację [Certum](#).

Gdy pojawi się okno [Certum CryptoAgent](#) włącz aplikację klikając na [Run](#).



Po krótkiej chwili aplikacja uruchomi się w tle, a przy procesie aktywacji pojawi się możliwość zapisania kluczy w aplikacji [Certum](#). Domyślne ustawienia, czyli algorytm klucza RSA (możliwa zmiana na EC) i długość klucza 2048 są poprawne do działania certyfikatu SSL.

Aktywacja ⓘ

1. Zamówienia 2. Wybór metody 3. Klucze ⓘ 4. Dane 5. Potwierdzenie

Nazwa usługi **Commercial SSL, 1 rok**
Wydanie

Poziom bezpieczeństwa kluczy certyfikatu *

Zapisz klucze w aplikacji Certum CryptoAgent ←

Zapisz klucze na karcie Certum

Algorytm klucza RSA ▼

Długość klucza 2048 ▼

Generuj klucze

« Wstecz Dalej »

Po kliknięciu na przycisk [Generuj klucze](#) wyświetli się komunikat, że klucze certyfikatu zostały wygenerowane. Klikając na przycisk [Dalej](#), przejdziesz do kolejnego etapu aktywacji (patrz rozdział 3 - Wypełnienie formularza przy aktywacji).

Aktywacja

1.Zamówienia 2.Wybór metody 3.Klucze 4.Dane 5.Potwierdzenie

Nazwa usługi	Commercial SSL, 1 rok Wydanie
Poziom bezpieczeństwa kluczy certyfikatu *	Klucze certyfikatu zostały wygenerowane

« Wstecz Dalej »

2.2.2. Metoda aktywacji – żądanie CSR

Jeśli chcesz wydać certyfikat metodą CSR skorzystaj z dowolnego spełniającego Twoje potrzeby generatora CSR lub rekomendowanego przez Certum narzędzia Open SSL. Czytaj więcej: <https://pomoc.certum.pl/pl/czym-jest-csr/>.

3. Wypełnienie formularza przy aktywacji

Na tym etapie wypełnij formularz z danymi Subskrybenta i danymi do certyfikatu. W przypadku wykorzystania metody CSR dane wpisane w żądaniu wypełnią automatycznie dane do certyfikatu. Pola z gwiazdką (*) są obowiązkowe.

Pole "skrótowy okres ważności" uzupełnij tylko wtedy, kiedy chcesz aby certyfikat kończył się przed upływem jego ważności.

Dane Wnioskodawcy:

Imię

Nazwisko

Telefon kontaktowy

Adres email

Dane do certyfikatu:

Funkcja skrótu RSA-SHA256

Skrócony okres ważności

Wskazany koniec ważności certyfikatu - podczas wystawiania certyfikatu data ta będzie wpisana jako data końca. Ustawienie tego pola skróci okres ważności certyfikatu, ale zagwarantuje jego wygaśnięcie wskazanego dnia. Aby wykorzystać maksymalny okres ważności, pole powinno pozostać puste.

Jeśli chcesz zachować maksymalny okres ważności certyfikatu, pole powinno zostać puste.

Dane Wnioskodawcy:

Imię:

Nazwisko:

Telefon kontaktowy:

Adres email:

Dane do certyfikatu:

Funkcja skrótu: RSA-SHA256

Skrócony okres ważności:

Domena 1 * dodaj wariant z www

Wprowadź nazwę domeny, dla której ma być wydany certyfikat. W przypadku wprowadzenia nazwy domeny z prefiksem www, np. www.certum.pl - wydany certyfikat będzie zabezpieczał zarówno domenę www.certum.pl jak i certum.pl. W przypadku certyfikatu Wildcard SSL, wydanego dla grupy subdomen w ramach domeny głównej np. *.certum.pl, będzie on zabezpieczał zarówno domeny certum.pl, www.certum.pl oraz subdomeny w ramach domeny certum.pl.

Uwaga! Jeżeli chcesz, aby certyfikat zabezpieczał dwa warianty domeny (twojadomena.pl i www.twojadomena.pl) w polu **Domena 1**, wpisz samą nazwę strony i po prawej zaznacz checkbox **dodaj wariant z www**.

Uwaga: Od października 2021 roku metoda weryfikacji FILE jest dostępna tylko dla certyfikatów zawierających tylko jedną domenę w zamówieniu. Metoda ta nie jest dostępna dla certyfikatów typu Wildcard oraz dla certyfikatów jednodomenowych z zaznaczonych checkboxem „www”. Jeśli zaznaczyłeś checkbox przy polu „Dodaj wariant www”, dostępna będzie metoda e-mail lub DNS.

Czytaj więcej: <https://pomoc.certum.pl/pl/ogloszenia-techniczne/zmiany-w-weryfikacji-domen/>

W przypadku certyfikatu Wildcard SSL wydanego dla grupy subdomen w ramach domeny głównej np. *.certum.pl, będzie on zabezpieczał zarówno domeny certum.pl, www.certum.pl (bez zaznaczania checkboxa) oraz subdomeny w ramach domeny certum.pl. Należy pamiętać, aby nazwę domeny rozpocząć od *.twojadomena.pl.

Po wypełnieniu danych klikamy na przycisk **Dalej**.

W ostatnim kroku (Potwierdzeniu) zweryfikuj czy wpisane dane są poprawne i zaznacz wymagane akceptacje oraz oświadczenia, po czym kliknij **Aktywuj**.

Struktura certyfikatu:

Podmiot	CN=certum.pl
Alt. nazwa podmiotu	dNSName=certum.pl, dNSName=www.certum.pl

Warunki Użytkowania

ZANIM ZŁOŻYSZ WNIOSEK O WYDANIE CERTYFIKATU, ZAAKCEPTUJESZ CERTYFIKAT BĄDŹ UŻYJESZ GO PROSIMY ABYŚ PRZECZYTAŁ NINIEJSZE „WARUNKI UŻYTKOWANIA CERTYFIKATÓW NIEKWALIFIKOWANYCH” ZWANE DALEJ „WARUNKAMI UŻYTKOWANIA”. JEŚLI NIE ZGADZASZ SIĘ Z WARUNKAMI UŻYTKOWANIA, NIE SKŁADAJ WNIOSKU O WYDANIE CERTYFIKATU, NIE AKCEPTUJ CERTYFIKATU I NIE UŻYWAJ GO.

NINIEJSZE WARUNKI UŻYTKOWANIA OBOWIĄZUJĄ OD MOMENTU PRZESŁANIA PRZEZ CIEBIE DO „CERTUM – POWSZECHNEGO CENTRUM CERTYFIKACJI” ZWANEGO DALEJ „CERTUM PCC” WNIOSKU CERTYFIKACYJNEGO DO ZAKOŃCZENIA OKRESU WAŻNOŚCI LUB UNIEWAŻNIENIA OTRZYMANEGO CERTYFIKATU. PRZEDKŁADAJĄC WNIOSEK O WYDANIE CERTYFIKATU ŻADASZ OD ORGANU WYDAJĄCEGO CERTYFIKATY ROZPATRZENIA GO I

- Akceptuję Warunki Użytkowania *
- Oświadczam i potwierdzam, że jest mi wiadome, że certyfikat może uwidaczniać moje dane osobowe w takim zakresie w jakim zostały one wskazane do umieszczenia w treści certyfikatu. Potwierdzam nadto, że wszelkie dane dotyczące czynności dokonanych przy użyciu tego certyfikatu mogą być, zgodnie z moją decyzją, dostępne bez ograniczenia uwzględniając w szczególności dane o lokalizacji. Na użycie certyfikatu nie ma wpływu Asseco Data Systems S.A., dostawca usług bezpieczeństwa. *
- Potwierdzam że jestem osobą pełnoletnią *
- Niniejszym potwierdzam zgodność z prawdą moich danych osobowych zawartych we wniosku o wydanie certyfikatu. *

« Wstecz **Aktywuj**

*Pole wymagane

4. Weryfikacja dostępu do domeny

Aby **Certum** mogło wydać certyfikat SSL użytkownik powinien udowodnić, że posiada dostęp do domeny, która ma być zabezpieczona. Weryfikację należy wykonać na JEDEN z TRZECH sposobów:

- weryfikacja administratorskiego adresu e-mail przez potwierdzenie linka weryfikacyjnego, który wysłany będzie przez **Certum** na adres administratora (np.: admin@twojadomena.pl, administrator@twojadomena.pl, webmaster@twojadomena.pl, postmaster@twojadomena.pl, hostmaster@twojadomena.pl),
- weryfikacja dostępu do domeny przez umieszczenie na serwerze pliku, którego nazwę użytkownik otrzyma od **Certum**,
- weryfikacja dostępu do domeny przez stworzenie odpowiedniego rekordu TXT w zasobach DNS, którego nazwę użytkownik otrzyma od **Certum**

Wybór metody weryfikacji dostępu do domeny jest możliwy w zakładce **Aktywacja certyfikatów**. Z listy należy wybrać odpowiedni nas certyfikat i kliknąć na przycisk **Weryfikuj domenę**.

Uwaga! Opcja weryfikowania dostępu do domeny będzie możliwa dopiero po przejściu przez aktywację produktu. Kod weryfikacyjny jest ważny 72 godziny od momentu wysłania, w przypadku jeśli link straci ważność masz możliwość wysłania kodu ponownie analogicznie jak przy wysłaniu pierwszego kodu.

Aktywacja certyfikatów

Nazwa usługi

Status aktywacji

Numer zamówienia

Status płatności

Zgodnie z art. 13 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych osobowych (RODO) z dnia 27 kwietnia 2016 r (zwanego dalej „Rozporządzenie”) informuję, iż:

1. Administratorem Pana/Pani danych osobowych jest Asseco Data Systems S.A. z siedzibą w Gdyni, ul. Podolska 21, 81-321 Gdynia;
2. Kontakt do Inspektora ochrony danych w Asseco Data Systems S.A. można uzyskać pod adresem e - mail: IOD@assecods.pl, tel.+48 42 675 63 60.
3. Pana/Pani dane osobowe przetwarzane będą w celu niezbędnym do wykonania umowy o certyfikat niekwalifikowany na podstawie art. 6 ust. 1 lit. b Rozporządzenia.

Nazwa usługi	Data zamówienia	Numer zamówienia	Status płatności	
Trusted SSL, 1 rok Wydanie	21 sierpień 2019	ZDRAPKA/3QQuKX7XyrTbKweZ/21/08/19	Zaksięgowano	Certyfikat nieaktywny <input type="button" value="Aktywuj"/>
Commercial SSL, 1 rok Wydanie	9 sierpień 2019	ZDRAPKA/nLiHWhexitpwJObB/09/08/19	Zaksięgowano	Oczekuje na realizację <input type="button" value="Weryfikuj domenę"/> <input type="button" value="Weryfikuj e-mail"/>

W kolejnym kroku wyświetli się lista domen do zweryfikowania. Kliknij na nazwę domeny, którą chcesz zweryfikować.

Domena	Zweryfikowano	Koniec ważności
 certum.pl	 Nie zweryfikowano	

Uwaga: Weryfikacje, które zostały zarchiwizowane NIE są dostępne na tej stronie.

Po kliknięciu na domenę wyświetlą się metody weryfikacji do wyboru.

4.1. Weryfikacja administratorskiego adresu email

Używając tej metody należy wybrać z listy jeden z dostępnych adresów i wysłać na niego link weryfikacyjny. Po wyborze adresu, do którego mamy dostęp klikamy na przycisk **Wyślij**. W otrzymanym mailu znajdować się będzie link weryfikacyjny, na który wystarczy kliknąć w celu weryfikacji dostępu do domeny.

Domena	Zweryfikowano	Koniec ważności
certum.pl	✗ Nie zweryfikowano	

Adres email: **Wyślij**

Domena: **Wyślij**

Adres email *

4.2. Weryfikacja dostępu do domeny przez umieszczenie na serwerze pliku

Metoda polega na umieszczeniu specjalnej strony WWW na serwerze obsługującym certyfikowaną domenę, a następnie potwierdzenie dokonanej zmiany przez kliknięcie odnośnika zamieszczonego w wysłanej wiadomości na podany adres email.

W sekcji **Domena** wybierz weryfikację poprzez umieszczenie pliku na serwerze (FILE), wpisz swój dowolny adres email, na który zostanie wysłana instrukcja.

Adres email: **Wyślij**

wybór metody

Domena: **Wyślij**

Adres email * ← wysłanie instrukcji z plikiem

Umieść plik (otrzymany na adres email) na swojej stronie w obszarze [./well-known/pki-validation/](https://www.certum.pl/.well-known/pki-validation/)
Po wykonaniu powyższej czynności w celu weryfikacji poprawnego umieszczenia pliku należy kliknąć na link weryfikacyjny z maila- [Weryfikuj domenę](#).

4.3. Weryfikacja dostępu do domeny przez stworzenie odpowiedniego rekordu TXT w zasobach DNS

Metoda polega na umieszczeniu odpowiedniego wpisu do rekordu TXT w bazie DNS dla certyfikowanej domeny, następnie potwierdzenie dokonanej zmiany przez kliknięcie odnośnika zamieszczonego w wysłanej wiadomości email.

W sekcji [Domena](#) należy wybrać weryfikację poprzez umieszczenie rekordu TXT w bazie DNS, następnie wpisać swój dowolny adres email, na który wysłana będzie instrukcja.

W otrzymanej wiadomości email będzie opis umieszczenia odpowiedniego wpisu do rekordu TXT w bazie DNS dla certyfikowanej domeny i potwierdzenie dokonanej zmiany przez kliknięcie odnośnika zamieszczonego w wiadomości.

Należy pamiętać, że odświeżenie/ aktualizacja wpisów DNS może trwać do 24 godzin.

5. Pobranie certyfikatu

Po poprawnej weryfikacji należy oczekiwać na wydanie certyfikatu.

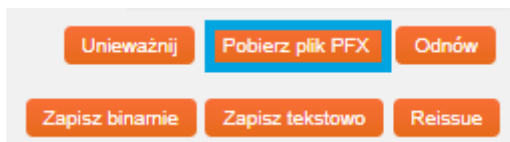
Ważna informacja! W przypadku złożenia zamówienia przez przelew tradycyjny do wydania certyfikatu niezbędne jest również zaksięgowanie wpłaty.

Aby pobrać plik certyfikatu zaloguj się na www.sklep.certum.pl. Wydane certyfikaty znajdują się w zakładce [Zarządzanie certyfikatami](#).

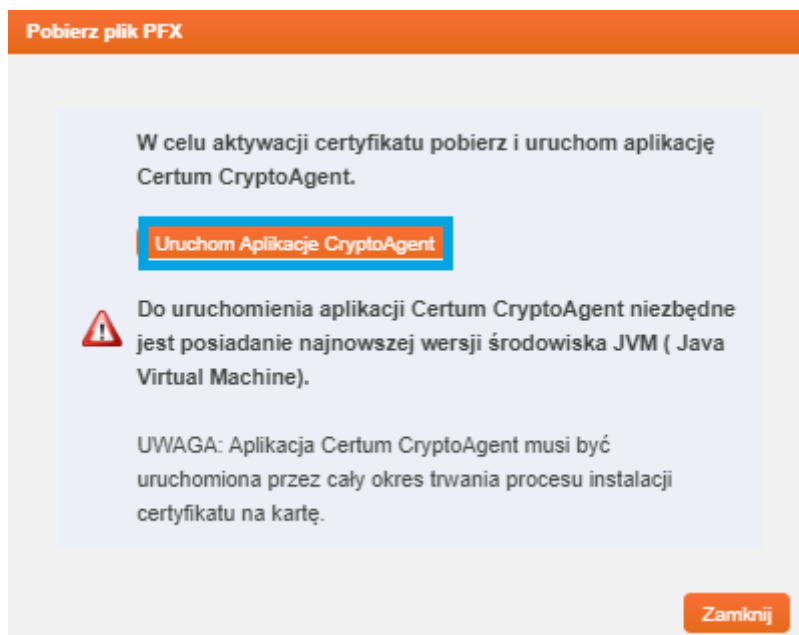
Na dole strony znajduje się lista wydanych certyfikatów. Po kliknięciu na wybrany certyfikat rozwiną się dostępne opcje związane z certyfikatem.

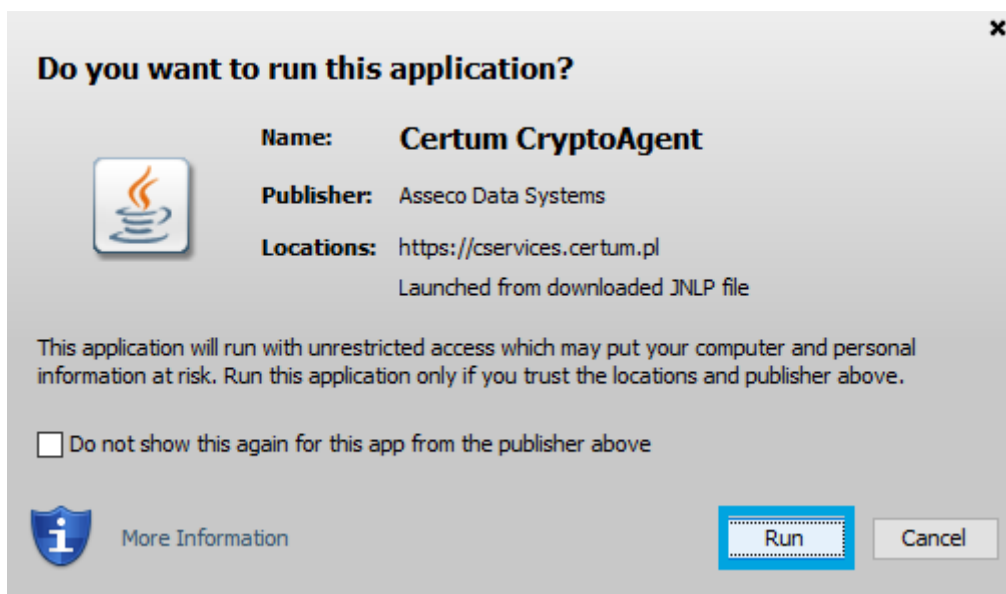
5.1. Pobranie pliku pfx/p12, po wykonaniu aktywacji metodą generowania pary kluczy

Jeżeli aktywację certyfikatu przeprowadziłeś metodą generowania pary kluczy, po wyborze certyfikatu w [Zarządzaniu certyfikatami](#) kliknij na przycisk [Pobierz plik PFX](#).

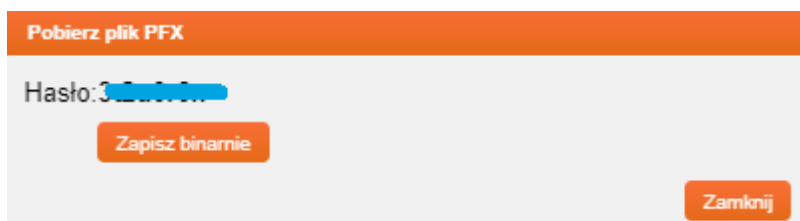


W kolejnym kroku uruchom aplikację [CryptoAgent](#).



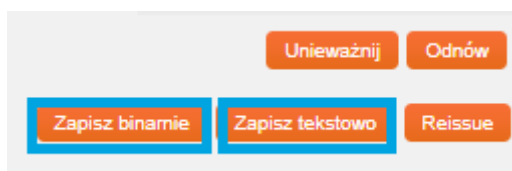


Aplikacja uruchomi się w tle, a na stronie pojawi się możliwość pobrania certyfikatu. Do pliku wygeneruje się również hasło, które należy zapisać, aby móc korzystać z pliku. Pobranie certyfikatu nastąpi po kliknięciu na przycisk [Zapisz binarnie](#).



5.2. Pobranie pliku certyfikatu i klucza prywatnego (metoda CSR)

Jeżeli aktywację przeprowadziłeś metodą CSR to plik certyfikatu (część publiczną) pobiera się bezpośrednio z zakładki [Zarządzanie certyfikatami](#) w formie binarnej (.cer – przycisk [Zapisz binarnie](#)) lub tekstowej (.pem – przycisk [Zapisz tekstowo](#)).



Przy tej aktywacji do implementacji certyfikatu na serwerze jest niezbędny również plik klucza prywatnego (privateKey.pem), który wygenerował się wcześniej wraz z CSR-em. W przypadku zagubienia klucza należy wykonać opcję [Reissue](#). Jest to ponowne wydanie certyfikatu.