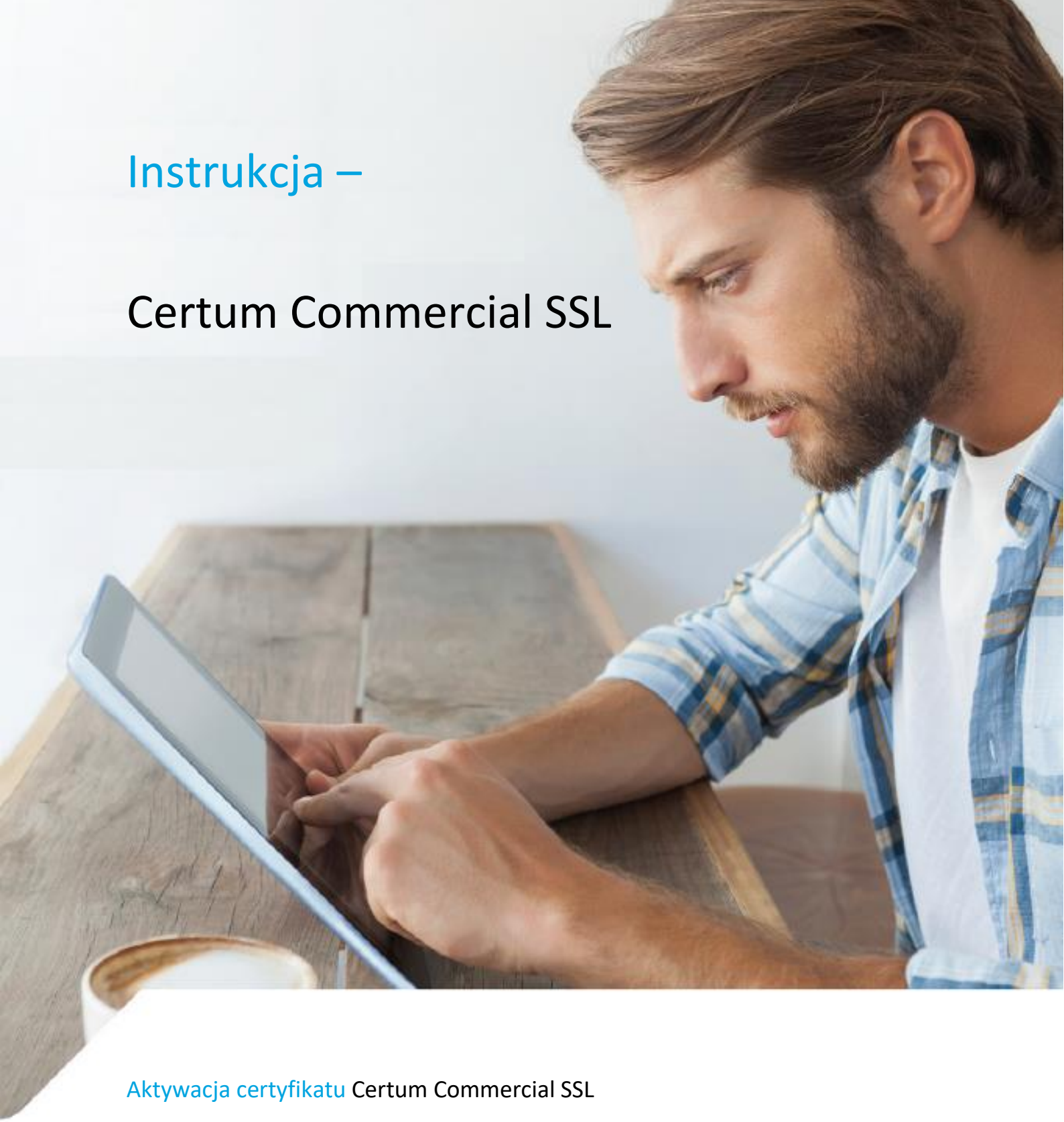


Instrukcja –

Certum Commercial SSL

Aktywacja certyfikatu Certum Commercial SSL

wersja 1.4

Certum by asseco

Spis treści

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.

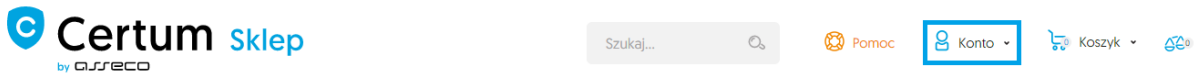
2. Aktywacja produktu

Instrukcja przygotowana jest na przykładzie przeglądarki Google Chrome i dotyczy procesu aktywacji certyfikatu Certum Commercial SSL.

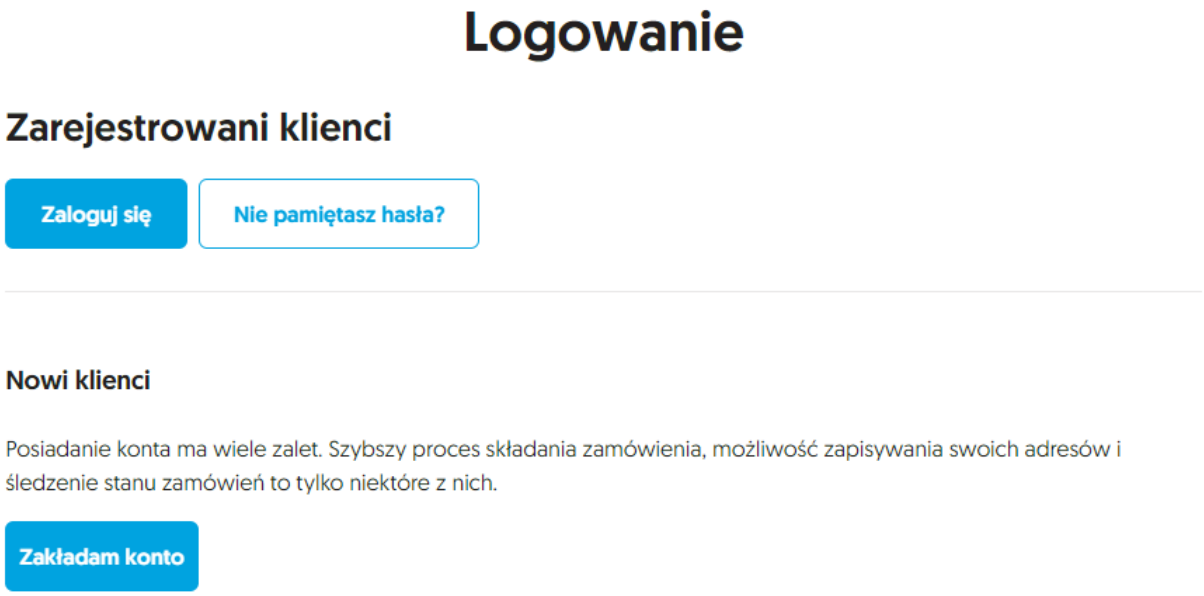
Po złożonym zamówieniu w sklepie Certum aktywacja dostępna będzie z poziomu konta w zakładce Aktywacja certyfikatów (patrz rozdział 2.2).

2.1. Dodanie kodu aktywacyjnego

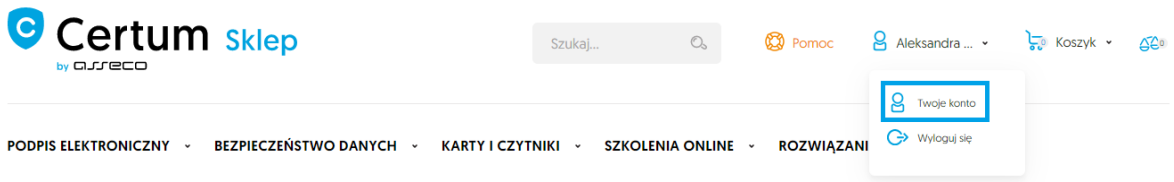
Jeżeli chcesz aktywować produkt z otrzymanego np. na adres email kodu elektronicznego – przed rozpoczęciem aktywacji kod dodaj w zakładce Kody elektroniczne. W tym celu zaloguj się do konta na stronie https://sklep.certum.pl



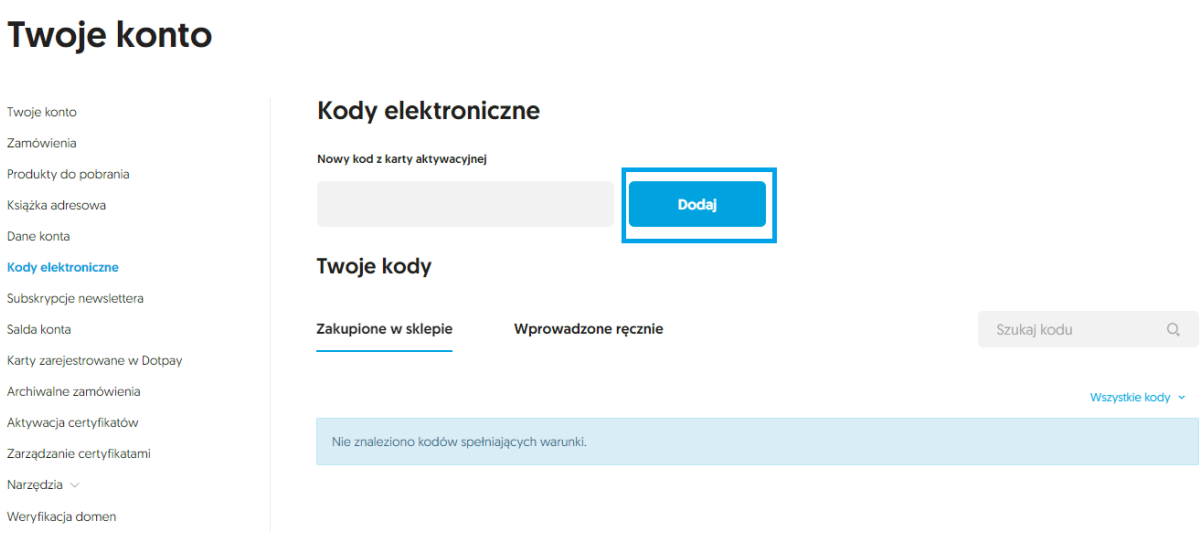
W przypadku gdy nie posiadasz konta kliknij na przycisk Zakładam konto, dzięki temu utworzysz nowe konto. Jeżeli posiadasz już konto wybierz opcję Zaloguj się.



Po zalogowaniu się kliknij na panel klienta – Twoje konto.



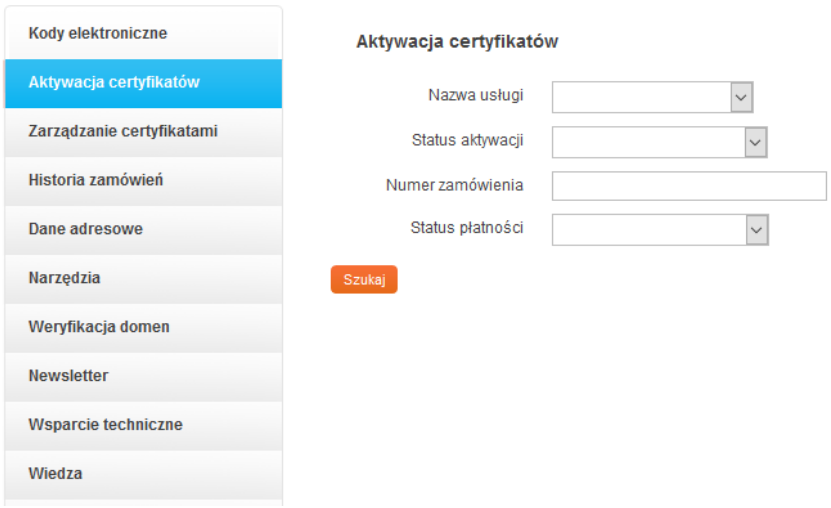
Aby dodać kod należy wybrać zakładkę Kody elektroniczne. W polu Nowy kod z karty aktywacyjnej wpisz posiadany kod i kliknij Dodaj.
Uwaga! Pamiętaj, że kod aktywacyjny składa się z 16 znaków. Po wpisaniu lub skopiowaniu kodu sprawdź czy ilość znaków się zgadza.



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.



Odszukaj na liście odpowiedni certyfikat i kliknij 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:

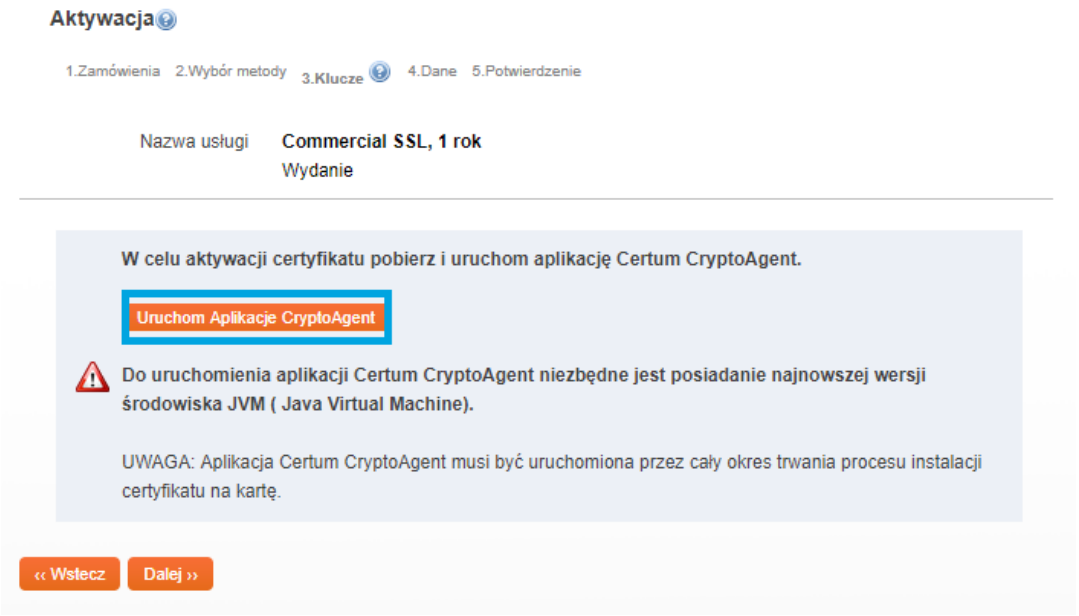
- przez administratora serwera
  lub
- za pomocą generatora CSR, dostępnego na koncie użytkownika sklepu Certum

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

2.2.1. Metoda aktywacji – generowanie pary kluczy

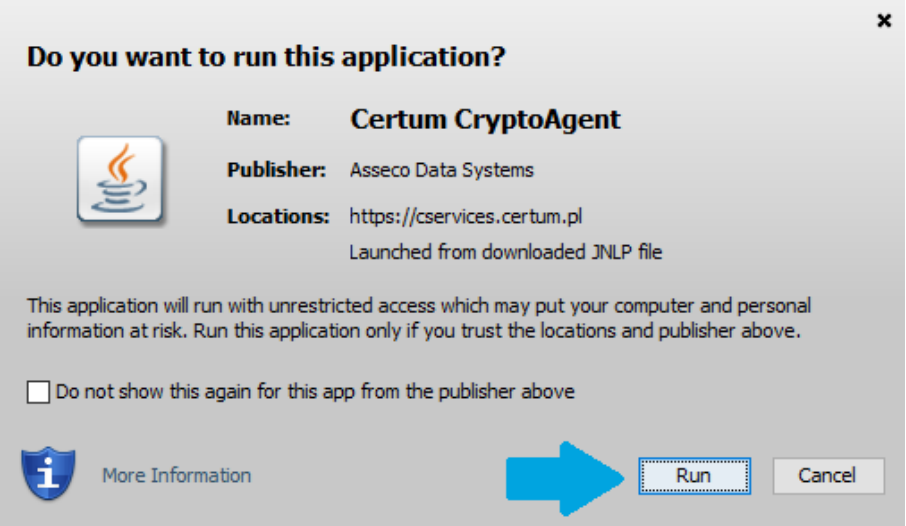
Jeżeli aktywację chcesz wykonać metodą generowania pary kluczy kliknij na przycisk Dalej.

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/).

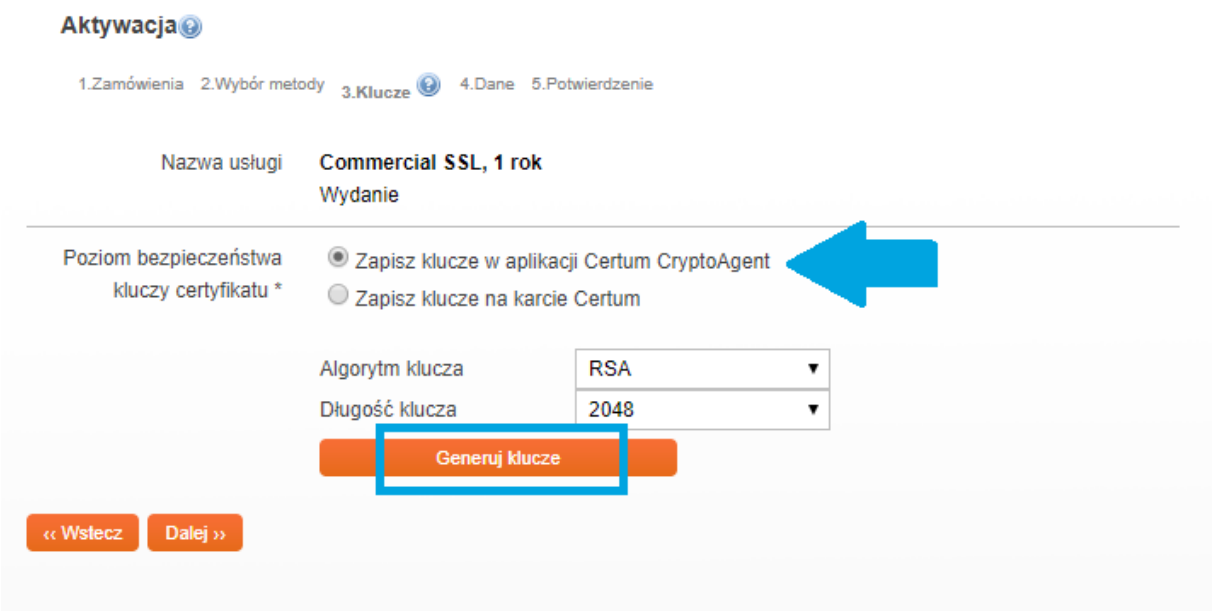


Na dolnym pasku przeglądarki pojawi się komunikat ostrzegawczy, przy którym kliknij na przycisk Zachowaj, aby pobrać aplikację Certum.

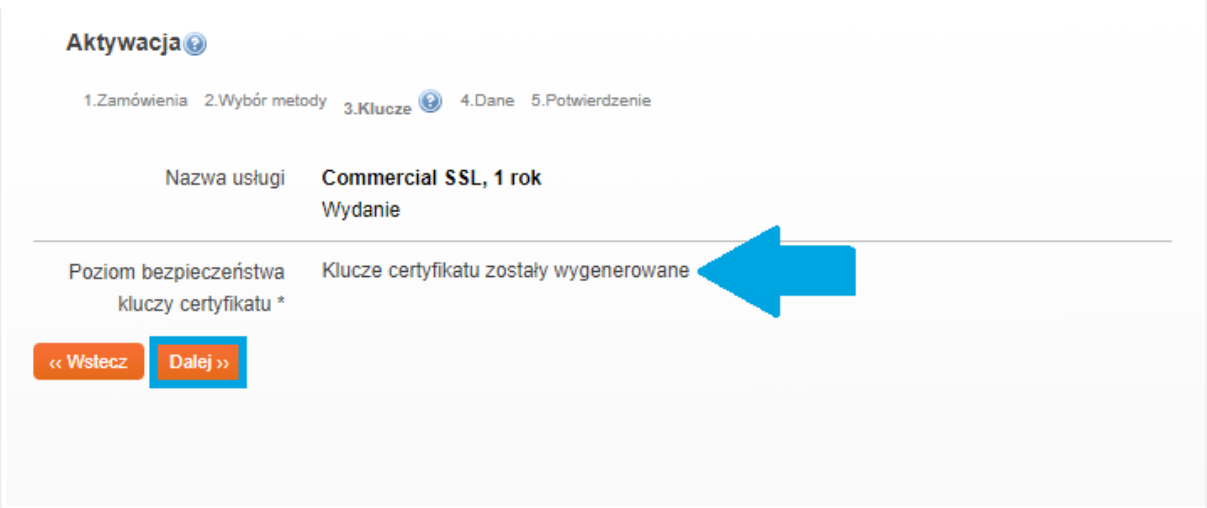
Gdy pojawi się okno Certum CryptoAgent włącz aplikację klikając na Run.



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.



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).



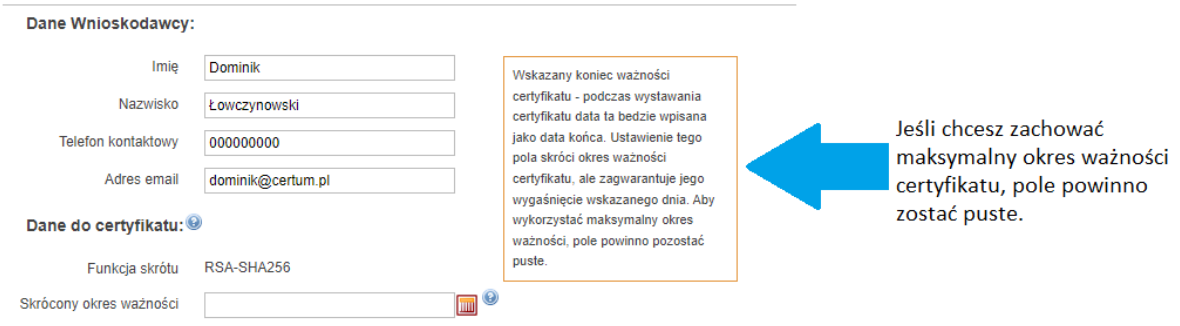
2.2.2. Metoda aktywacji – żądanie CSR

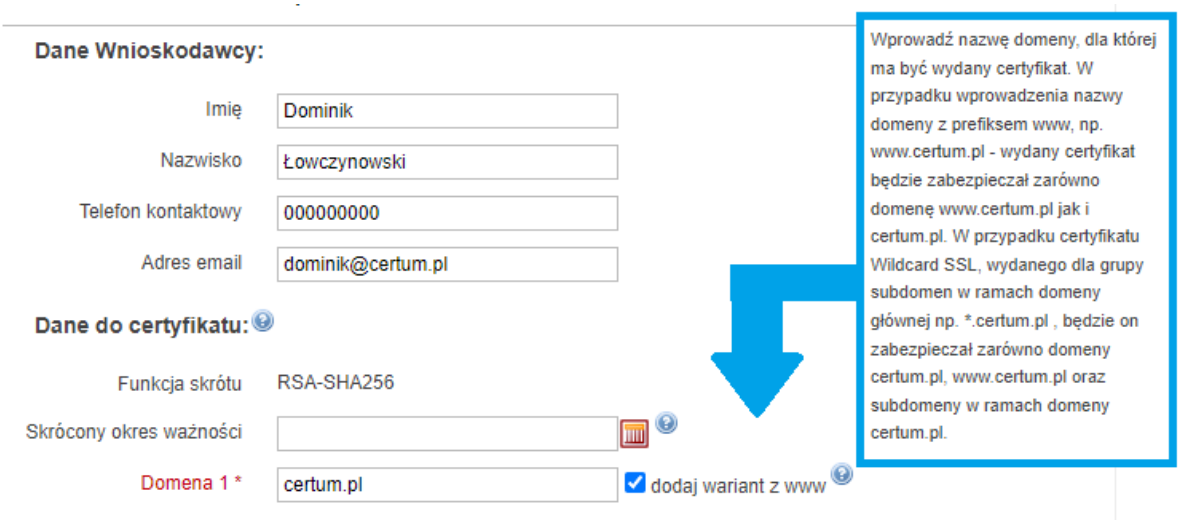
Jeśli chcesz wydać certyfikat metodą CSR skorzystaj z dowolnego spełniającego Twoje potrzeby generatora CSR lub rekomendowanego przez Certum narzędzia Open SSL. Czytaj więcej: https://pomoc.certum.pl/pl/czym-jest-csr/.

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



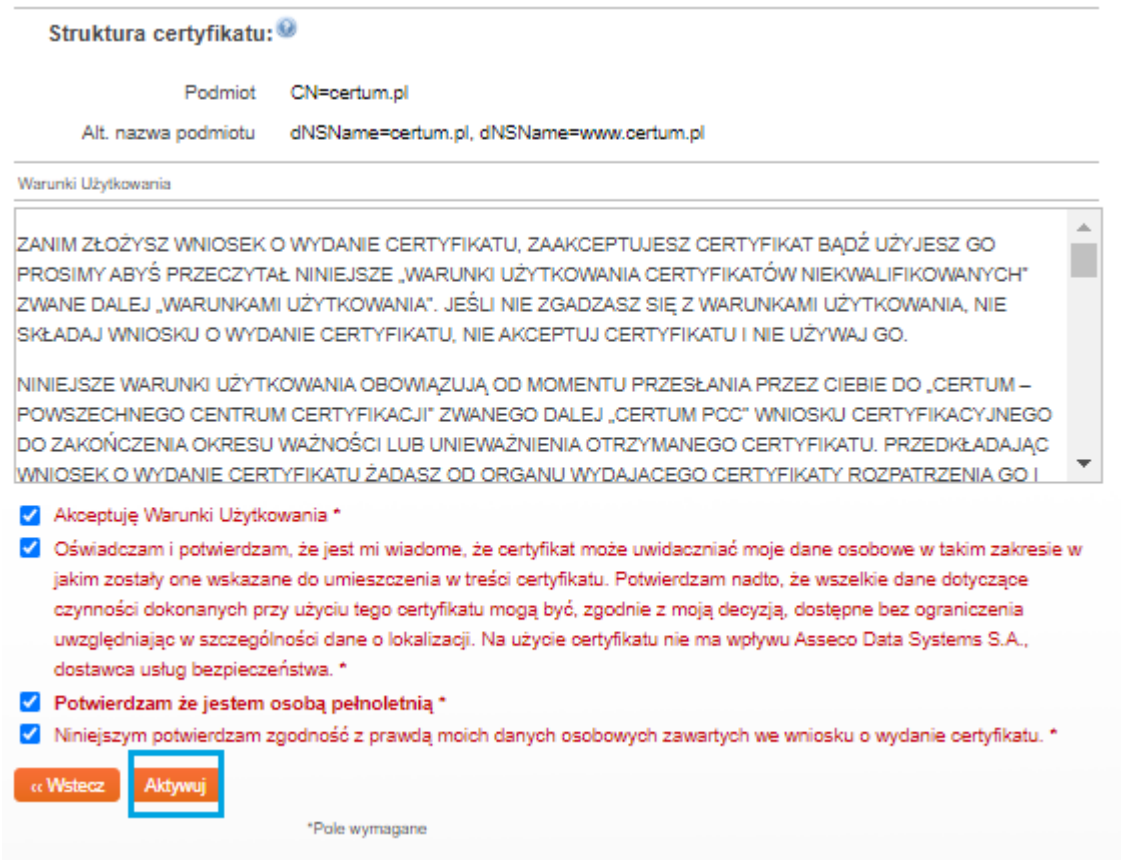


Uwaga! Jeżeli chcesz, aby certyfikat zabezpieczał dwa warianty domeny (twojadomena.pl i www.twojadomena.pl) w polu Domena 1, wpisz samą nazwę strony i po prawej zaznacz checkbox dodaj wariant z www.

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.



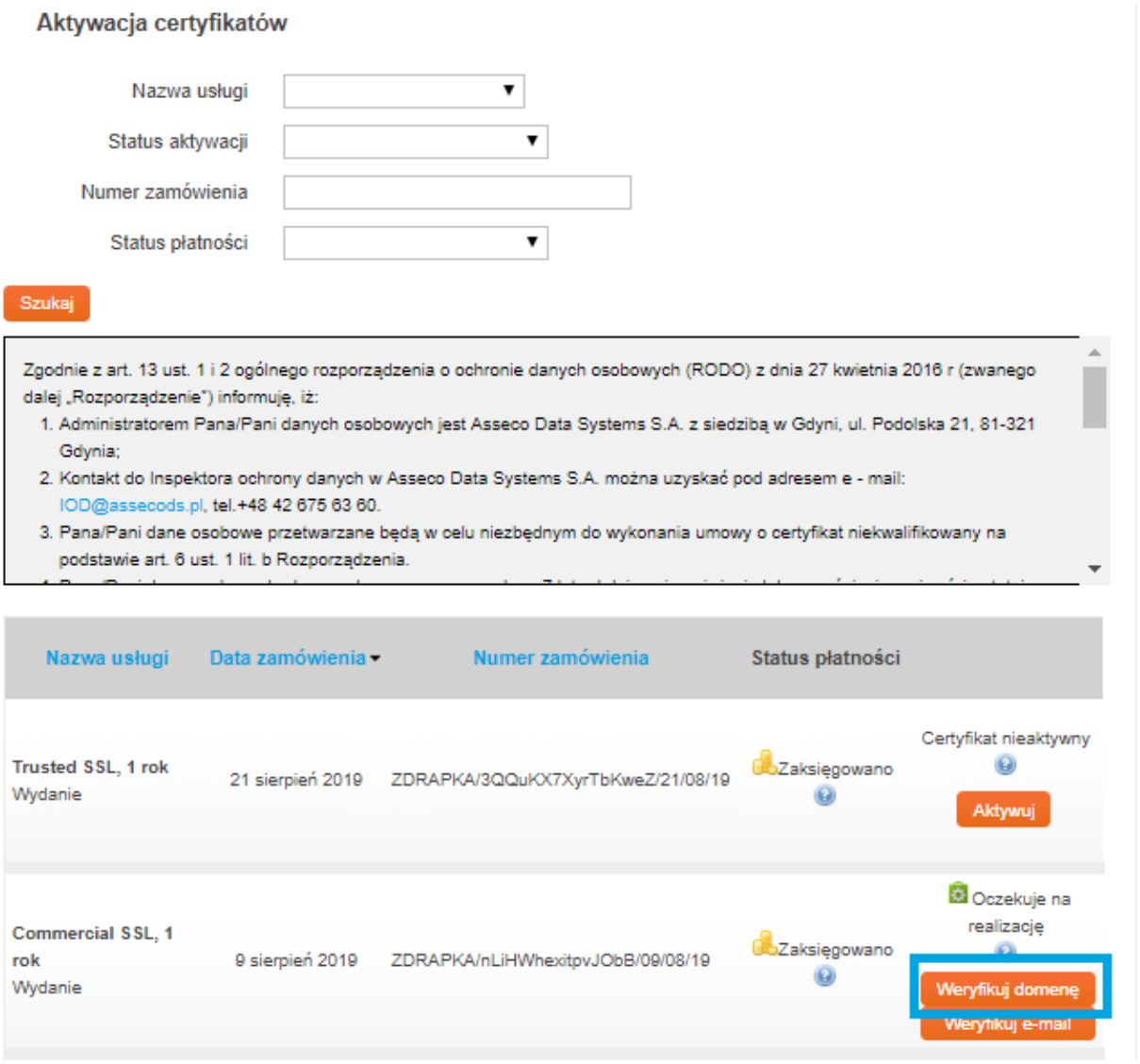
4. Weryfikacja dostępu do domeny

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:

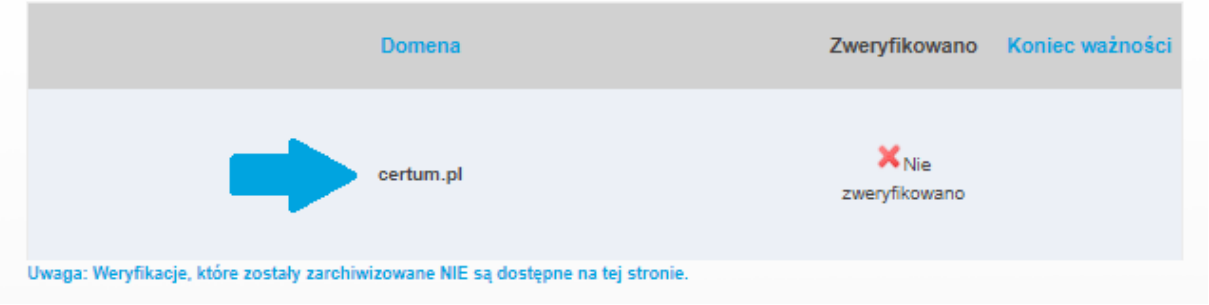
- weryfikacja administratorskiego adresu e-mail przez potwierdzenie linka weryfikacyjnego, który wysyłany będzie przez Certum na adres administratora (np.: admin@twojadomena.pl, administrator@twojadomena.pl, webmaster@twojadomena.pl, postmaster@twojadomena.pl, hostmaster@twojadomena.pl),
- weryfikacja 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.



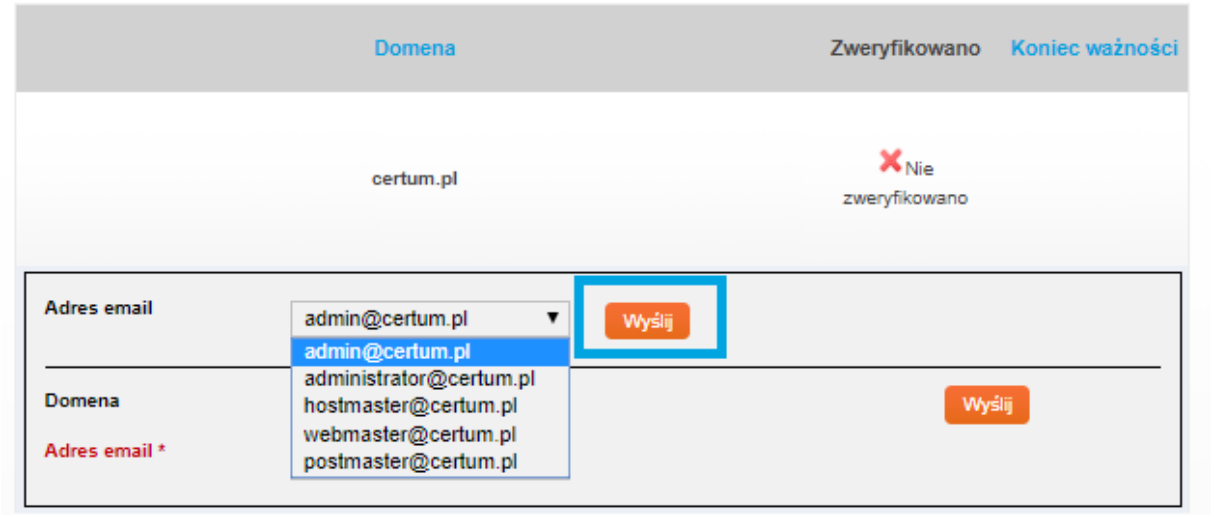
W kolejnym kroku wyświetli się lista domen do zweryfikowania. Kliknij na nazwę domeny, którą chcesz zweryfikować.



Po kliknięciu na domenę wyświetlą się metody weryfikacji do wyboru.

4.1. Weryfikacja administratorskiego adresu email

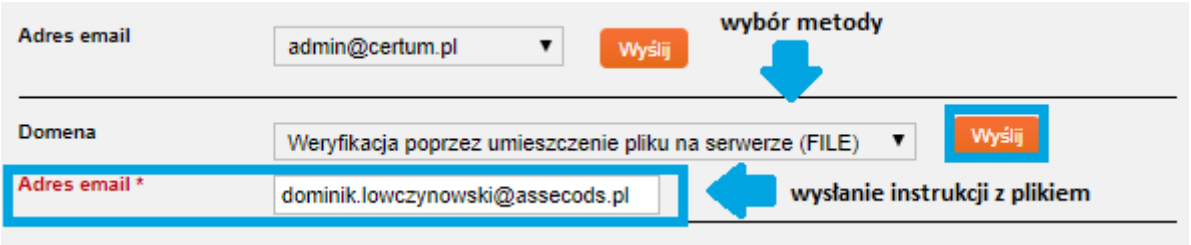
Używając tej metody należy wybrać z listy jeden z dostępnych adresów i wysłać na niego link weryfikacyjny. Po wyborze adresu, do którego mamy dostęp klikamy na przycisk Wyślij. W otrzymanym mailu znajdować się będzie link weryfikacyjny, na który wystarczy kliknąć w celu weryfikacji dostępu do domeny.



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.

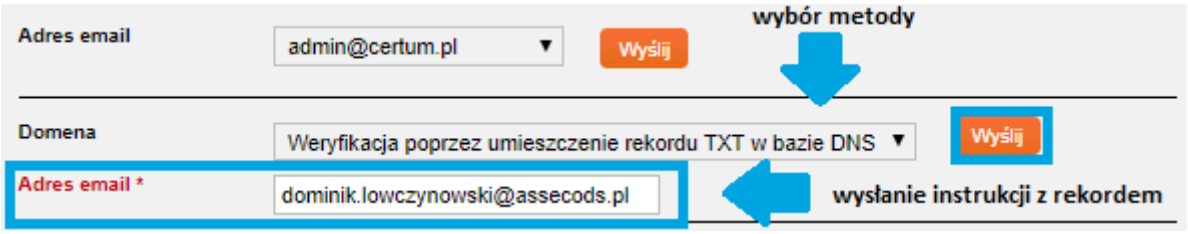
W sekcji Domena wybierz weryfikację poprzez umieszczenie pliku na serwerze (FILE), wpisz swój dowolny adres email, na który zostanie wysłana instrukcja.



Umieść plik (otrzymany na adres email) na swojej stronie w obszarze /.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.



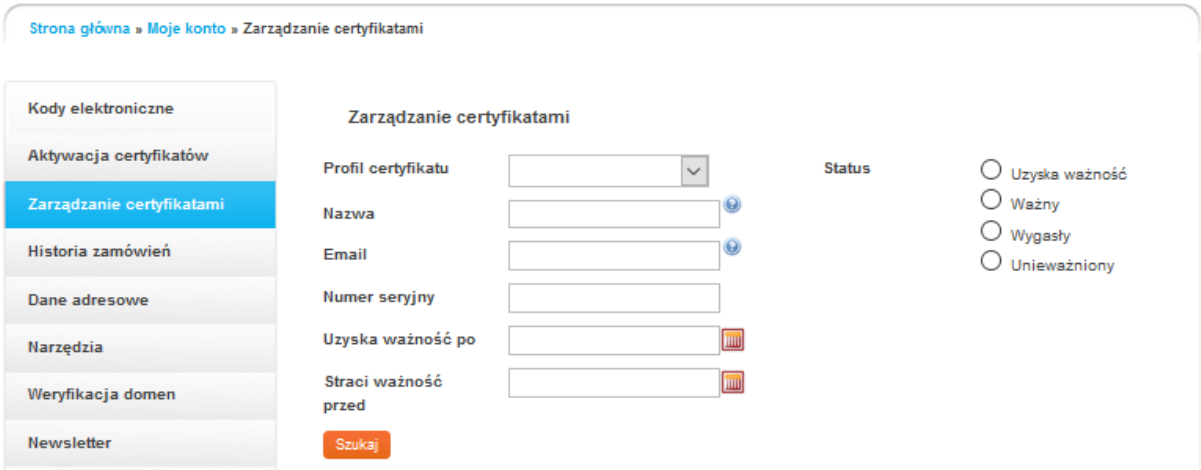
W otrzymanej wiadomości email będzie opis umieszczenia odpowiedniego wpisu do rekordu TXT w bazie DNS dla certyfikowanej domeny i potwierdzenie dokonanej zmiany przez kliknięcie odnośnika zamieszczonego w wiadomości.
Należy pamiętać, że odświeżenie/ aktualizacja wpisów DNS może trwać do 24 godzin**.**

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.

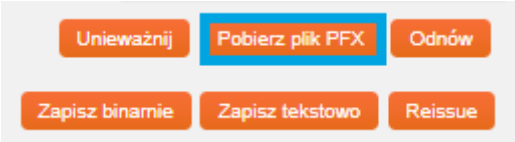
Aby pobrać plik certyfikatu zaloguj się na www.sklep.certum.pl. Wydane certyfikaty znajdują się w zakładce Zarządzanie certyfikatami.



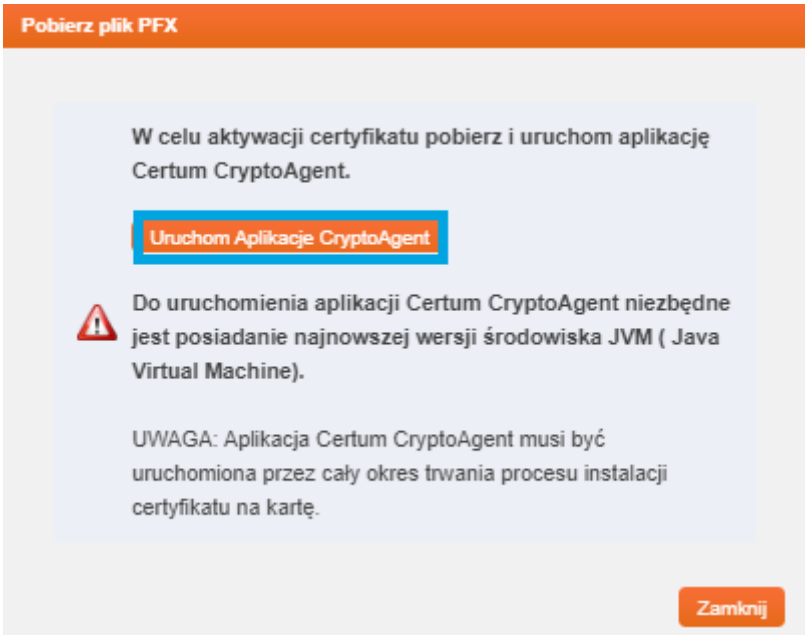
Na dole strony znajduje się lista wydanych certyfikatów. Po kliknięciu na wybrany certyfikat rozwiną się dostępne opcje związane z certyfikatem.

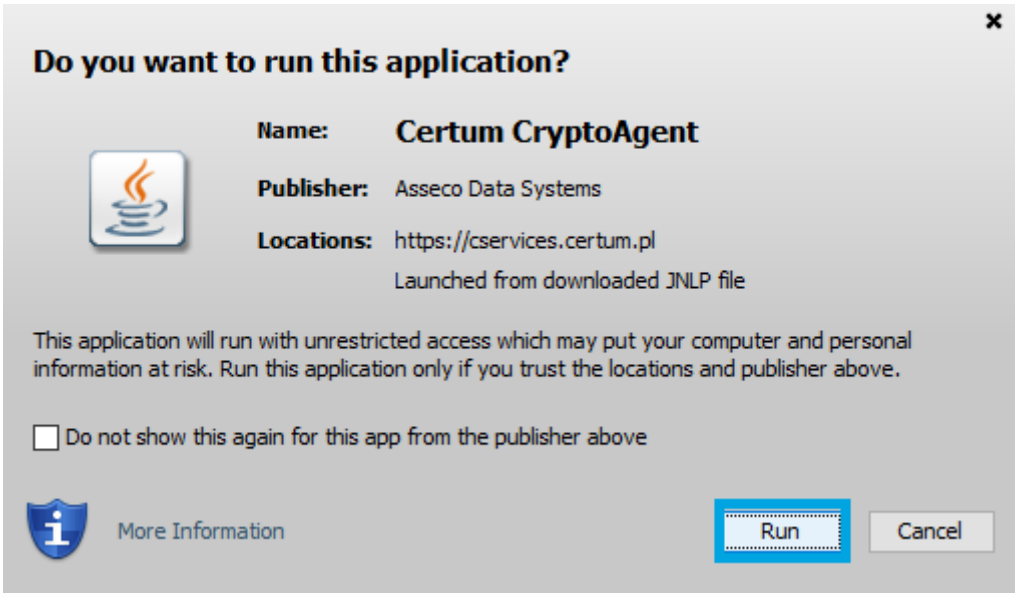
5.1. Pobranie pliku pfx/p12, po wykonaniu aktywacji metodą generowania pary kluczy

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

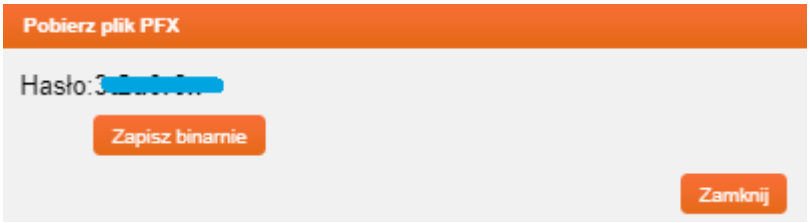


W kolejnym kroku uruchom aplikację CryptoAgent.



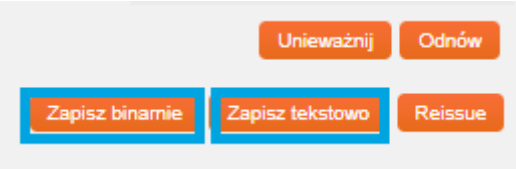


Aplikacja uruchomi się w tle, a na stronie pojawi się możliwość pobrania certyfikatu. Do pliku wygeneruje się również hasło, które należy zapisać, aby móc korzystać z pliku. Pobranie certyfikatu nastąpi po kliknięciu na przycisk Zapisz binarnie.



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.