

Emp@tia administracja

Certyfikaty



COIG SA

Grupa Kapitałowa

WASKO®



40-065 KATOWICE
ul. Mikołowska 100
www.coig.pl
coig@coig.pl

lipiec 2024 r.

Copyright © COIG SA
Wszelkie prawa zastrzeżone



Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji, w jakiegokolwiek postaci, jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Niniejsza dokumentacja stanowi tajemnicę przedsiębiorstwa COIG SA w rozumieniu art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz. U. z 2003 r. nr 153, poz. 1503 ze zm.).

COIG, logo COIG są znakami zastrzeżonymi firmy COIG SA.

Spis treści

Spis treści	3
Wstęp	4
Certyfikaty	5
Generowanie/odnowienie certyfikatu komunikacyjnego (CSR)	6
Obsługa certyfikatów	7

Wstęp

Niniejszy dokument omawia zagadnienia związane z obsługą certyfikatów w ramach komponentu Emp@tia Komputerowego Systemu dla Administracji Terenowej KSAT2000.

Obsługa certyfikatów jest taka sama w ramach obszarów SR/FA/SW.

Certyfikaty

Aby móc nawiązywać bezpieczne połączenia z serwisem Emp@tia, system dziedziny obsługiwany przez system KSAT2000 musi mieć dostęp do odpowiednich certyfikatów.

Wykorzystując formularz Emp@tia certyfikaty, należy zapisać udostępnione certyfikaty wraz z kompletem informacji ich dotyczących w bazie systemu KSAT2000.

Dodawanie certyfikatu

Aktualny Typ certyfikatu

Identyfikator systemu

Alias certyfikatu

Data od 21-09-2014 Data do Cel certyfikatu

Hasło klucza Hasło klucza magazynu

Nazwa pliku źródłowego

Anuluj Zapisz

Istotne jest, aby podczas dodawania tych certyfikatów w polu Typ certyfikatu podać wartość Root CA. Dzięki temu, podczas generowania pliku CSR (żądania podpisu certyfikatu) zostaną one automatycznie zaimportowane do przygotowanego keystore (magazynu kluczy).

Należy również zwrócić uwagę na to, czy udostępnione certyfikaty zawierają pełną ścieżkę certyfikacji do zaufanego wydawcy certyfikatów, w przeciwnym razie proces generowania CSR oraz importowania odpowiedzi na niego nie powiedzie się.

Istnieje też możliwość aktualizacji wybranych certyfikatów, np. w celu modyfikacji pliku binarnego certyfikatu, w celu ustawienia jego aktualności.

Modyfikowanie certyfikatu

Aktualny Typ certyfikatu

Identyfikator systemu

Alias certyfikatu

Data od 31-10-2014 Data do Cel certyfikatu Nieokreślony

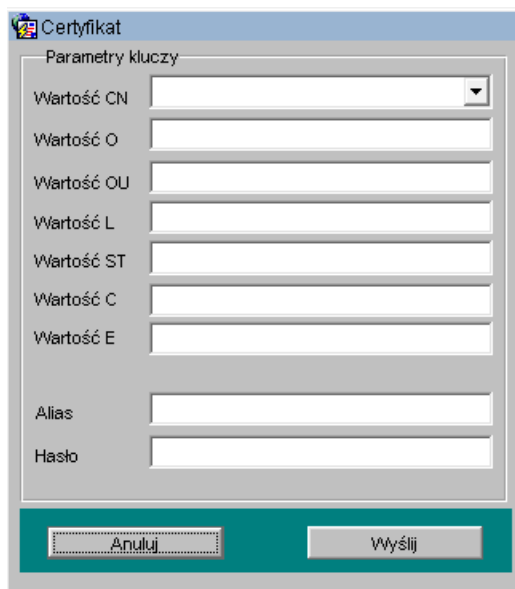
Hasło klucza Hasło klucza magazynu

Nazwa pliku źródłowego coig.truststore

Anuluj Zapisz

Generowanie/odnowienie certyfikatu komunikacyjnego (CSR)

Generowanie/odnowienie certyfikatu CSR odbywa z poziomu poniższego formularza (Emp@tia ⇒ Operacje ⇒ Generuj CSR):



Gdzie:

Wartość CN – (common name) – należy wybrać z listy wartości identyfikator systemu, który został nadany w momencie rejestracji systemu dziedzicznego.

Wartość O – (organization) – należy podać nazwę jednostki terenowej, dla której został utworzony system dziedziczny np. OPS Suchy Las.

Wartość OU – (organizational unit name) – należy podać nazwę jednostki organizacyjnej

Wartość L – (locality) – należy podać nazwę miejscowości gdzie znajduje się jednostka terenowa, dla której został utworzony system dziedziczny np. Suchy Las.

Wartość ST – (state Or province) – należy podać nazwę województwa gdzie mieści się jednostka terenowa, dla której został utworzony system dziedziczny np. Wielkopolskie

Wartość C – (country) – należy podać dwuliterowy kod kraju zawierającego jednostkę np. PL (kod musi być zapisany wielkimi literami)

Wartość E – (email) – należy podać adres poczty elektronicznej

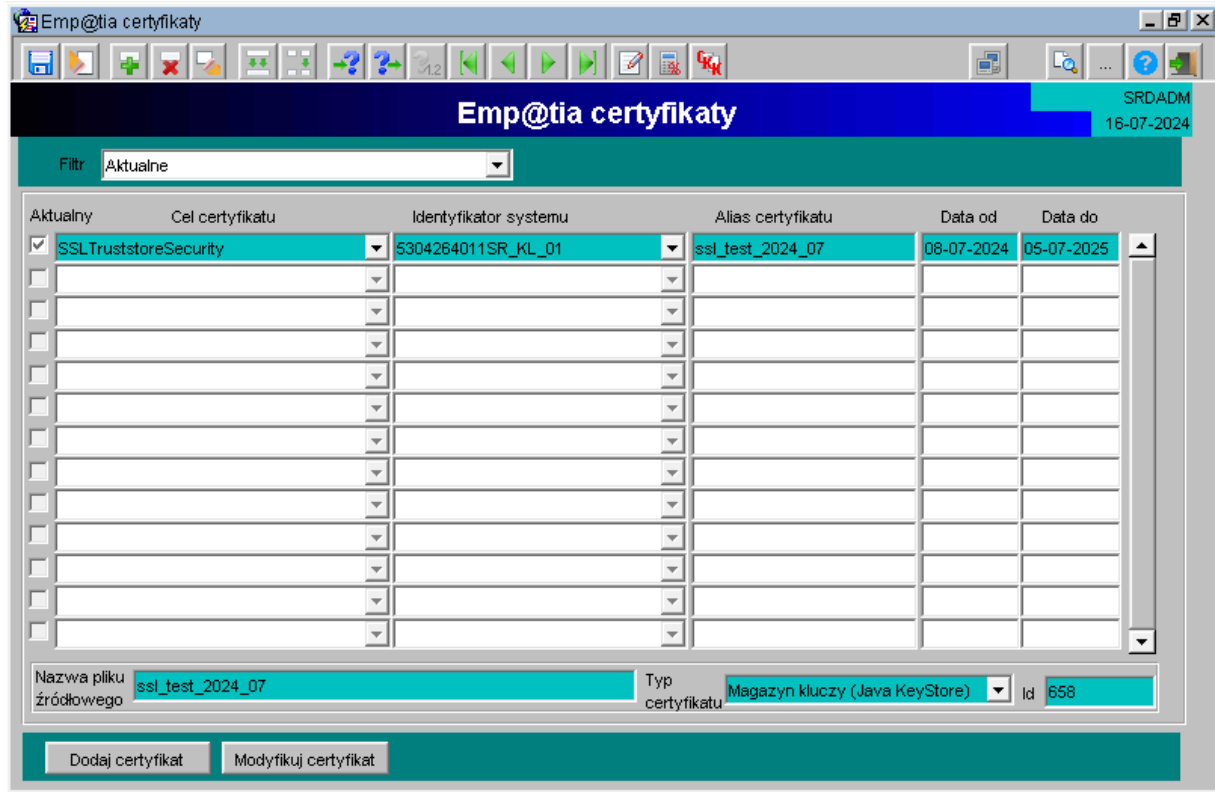
Alias – nazwa aliasu dla przygotowanego keystore (magazynu kluczy)

Hasło – hasło do przygotowanego keystore (pole korzysta ze znaków maskujących)

W wyniku naciśnięcia przycisku **Wyślij**, zostanie wysłane żądanie CSR do serwisu Emp@tia, a otrzymany wynik zaimportowany (podobnie jak wcześniej opisane certyfikaty Root CA) do utworzonego keystore. Po poprawnym zakończeniu operacji, będzie możliwa komunikacja ze wszystkimi serwisami zewnętrznymi udostępnionymi w ramach systemu Emp@tia.

Obsługa certyfikatów

Formularz prezentuje informacje o certyfikatach wykorzystywanych w procesie komunikacji z systemem Emp@tia. Na liście przedstawione są zapisane w systemie KSAT certyfikaty wraz z określeniem ich aktualności, dat obowiązywania, nazw plików źródłowych. Podczas wykonywania operacji *Generuj CSR* odpowiednie certyfikaty są automatycznie dodawane do tej listy. Z poziomu tego formularza dostępne są operacje dodania i modyfikacji certyfikatu.



Aktualny	Cel certyfikatu	Identyfikator systemu	Alias certyfikatu	Data od	Data do
<input checked="" type="checkbox"/>	SSLTruststoreSecurity	5304264011SR_KL_01	ssl_test_2024_07	08-07-2024	05-07-2025
<input type="checkbox"/>					
<input type="checkbox"/>					
<input type="checkbox"/>					
<input type="checkbox"/>					
<input type="checkbox"/>					
<input type="checkbox"/>					
<input type="checkbox"/>					
<input type="checkbox"/>					
<input type="checkbox"/>					
<input type="checkbox"/>					

Nazwa pliku źródłowego: ssl_test_2024_07 Typ certyfikatu: Magazyn kluczy (Java KeyStore) Id: 656