



KSeF connector for Creatio



Table of Contents

Configuration guide	3
Custom system settings.....	4
Obtain a KSeF access token	5
Obtain the Ministry of Finance Public Keys	6
Generating a Certificate for Link Signing	7



Configuration guide

This section provides a step-by-step guide on how to install and configure the KSeF integration extension.

Prerequisites:

- The Customer 360 app must be installed.
- The Order and Contract Management app must be installed.

Installation steps:

1. Go to Settings → Application Management → Application Hub.
2. Click New application.
3. Select Marketplace powered.
4. Search for “KSeF connector for Creatio” and click Install.

There are three **KSeF environments** available. The table below shows the addresses for the taxpayer application, the QR code visualization application, and the API endpoints for each environment. By default, the system is configured with the **test API address**. If you are using a different environment, this address must be updated to the corresponding value from the table.

Environment	API	QR Code Visualization Application	Taxpayer Application*
Test Environment (TE)	https://api-test.ksef.mf.gov.pl	https://qr-test.ksef.mf.gov.pl	https://ap-test.ksef.mf.gov.pl
Demonstration / Pre-production Environment (TR)	https://api-demo.ksef.mf.gov.pl	https://qr-demo.ksef.mf.gov.pl	https://ap-demo.ksef.mf.gov.pl
Production Environment (PRD)	https://api.ksef.mf.gov.pl	https://qr.ksef.mf.gov.pl	https://ap.ksef.mf.gov.pl

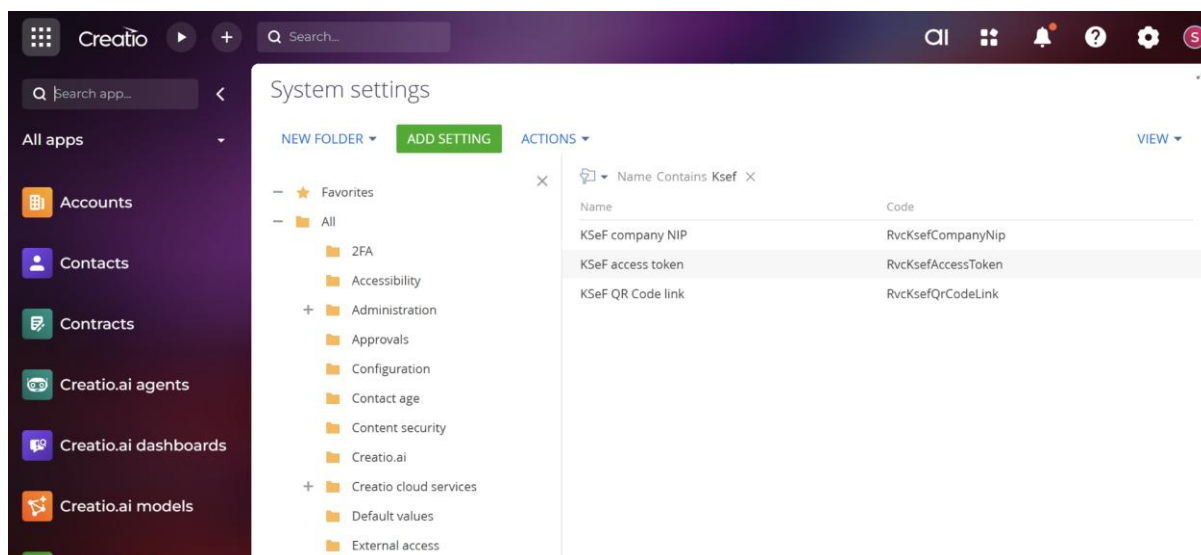


Custom system settings

To configure the KSeF integration, the system administrator must set up the following system settings.

Administrators can configure the system settings as follows:

1. Open the [System settings] section.
2. Filter by the [Code] field.
3. Enter the desired value.



Name	Code	Description
KSeF company NIP	RvcKsefCompanyNip	Company NIP (invoice issuer)
KSeF access token	RvcKsefAccessToken	Access token generated in the taxpayer portal
KSeF QR Code link	RvcKsefQrCodeLink	URL to verify the issuer certificate
TE: qr-test.ksef.mf.gov.pl TR: qr-demo.ksef.mf.gov.pl PRD: qr.ksef.mf.gov.pl		



To generate the token, follow these steps:

1. Log in to the Taxpayer Portal.
2. Open the [Tokens] section.
3. Select [Generate Token].
4. Enter the token name.
5. Select permissions for issuing and viewing invoices.
6. Click [Generate Token].

KSeF access token.



realvalue
No Code. High Value



Obtain the Ministry of Finance Public Keys

In order to ensure proper operation of the integration with the KSeF system, it is necessary to store the public keys provided by the Ministry of Finance in the system.

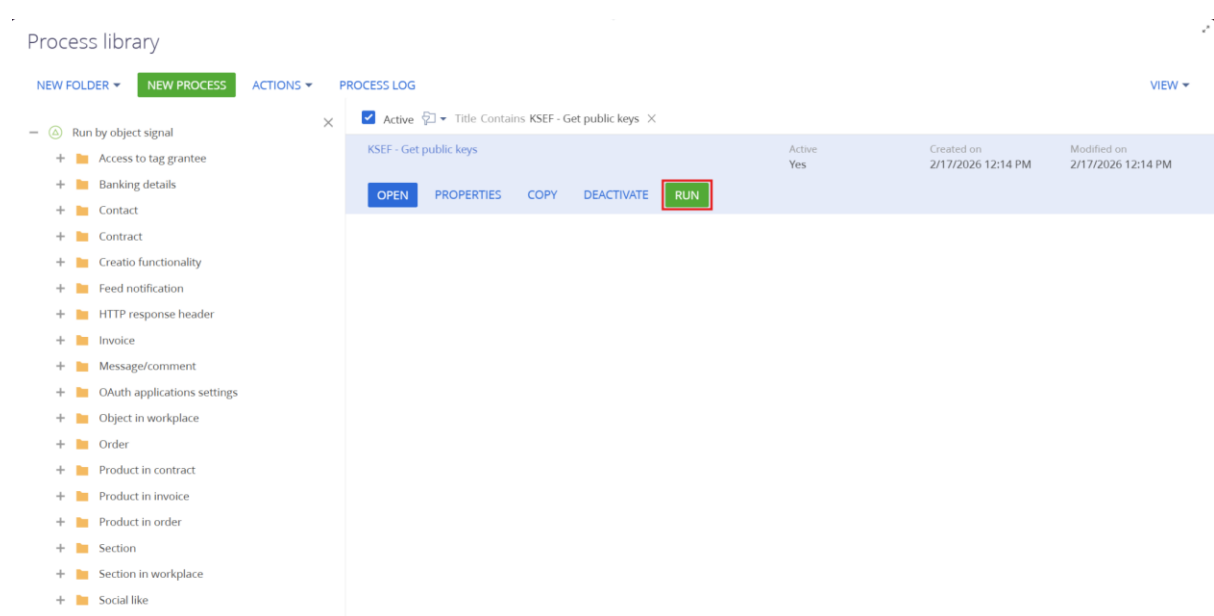
The keys are stored in the lookup KSeF key/certificate storage and are named: **Symmetric Key Encryption** and **KSEF Token Encryption**.

To simplify the process of saving the keys, a dedicated process named **KSEF - Get public keys** has been created.

The system administrator should run this process to retrieve the keys. This process can also be used to update the keys if they expire.

The Administrator can start the process as follows:

1. Open the [Process Library] section.
2. Filter by the [Code] field.
3. Run the process.





Generating a Certificate for Link Signing

The certificate is used to sign the link on invoices issued in offline mode.
To generate the certificate, follow these steps:

1. Log in to the Taxpayer Portal.
2. Open the [Certificates] section.
3. Select [Apply for a certificate].
4. Fill in the certificate name and password fields.
5. Click the [Generate] button.
6. On the next screen, select the certificate purpose:
Link signature for issuer verification and set the certificate validity date.
7. Download the certificate.

The screenshot shows the 'Generowanie klucza i wniosku o wydanie certyfikatu' (Generating key and application for certificate issuance) form. The form is part of the 'Krajowy System e-Faktur - Aplikacja Podatnika KSeF Środowisko Testowe' (National e-Invoice System - Taxpayer Application KSeF Test Environment). The form is titled '1 z 2 Generowanie klucza i wniosku o wydanie certyfikatu' and 'Wniosek o certyfikat'.

The form contains the following fields and sections:

- Nazwa certyfikatu *** (Certificate name): A text input field with the value 'Creatio Link Signing'. Below the field, it says 'Pod nadaną przez Ciebie nazwą zapiszemy klucz prywatny oraz certyfikat' (We will save the private key and certificate under the name you provided) and 'Wpisz od 5 do 100 znaków' (Enter from 5 to 100 characters).
- Hasło *** (Password): A password input field with a strength indicator. Below the field, it lists requirements: 'Musí zawierać minimum:' (Must contain minimum) and 'Nie może zawierać:' (Must not contain).
 - Musi zawierać minimum:**
 - 15 znaków
 - 1 wielką literę
 - 1 małą literę
 - 1 cyfrę
 - 1 znak specjalny: !@#\$%^&*()_-=+
 - Nie może zawierać:**
 - więcej niż 32 znaków
 - polskich znaków
 - innych znaków specjalnych
- Powtórz hasło *** (Repeat password): A second password input field for confirmation.
- Generuj** (Generate): A blue button at the bottom of the form.

The left sidebar shows the navigation menu with options: Faktury, Historia sesji, Uprawnienia, Tokeny, Certyfikaty, and Wniosek o certyfikat (selected). The top right corner shows the user ID '5252787769'.



Menu

Krajowy System **e-Faktur** - Aplikacja Podatnika KSeF Środowisko Testowe

5252787769

- Faktury
- Historia sesji
- Uprawnienia
- Tokeny
- Certyfikaty
 - Wniosek o certyfikat
 - Lista certyfikatów



Przesłanie wniosku

Wniosek o certyfikat



Wygenerowano klucz prywatny

Wygenerowany klucz jest zapisany na Twoim urządzeniu pod nazwą Creatio Link Signing i zabezpieczony hasłem

Przeznaczenie certyfikatu *

- ☒ Podpis linku do weryfikacji wystawcy
- ☐ Uwierzytelnienie w systemie KSeF

Certyfikat ważny od *

Możesz zmienić datę, od której będzie ważny Twój certyfikat. Certyfikat będzie ważny przez 2 lata od podanej daty.

18.02.2026

Wyślij wniosek o wydanie certyfikatu



As a result, two files are generated: the **certificate** and the **private key**.

To use them in Creatio, the private key must be decrypted using the following command:

- *openssl pkcs8 -in encrypted_key.key -out decrypted_key.key*

Next, the system administrator should add a new record to the **RvcKsefPublicKeysStorage** object and fill in the following fields:

- **Certificate** – content of the .crt file
- **Private Key** – content of the .key file
- **Decrypted Private Key** – content of the decrypted_key.pem file
- **Certificate Password** – password defined for the certificate in the taxpayer portal
- **Usage Type** – Offline Certificate
- **Active** – Yes / True
- **Valid From and Valid To** – values as provided in the taxpayer portal