

ePUAP

Konfiguracja w zakresie integracji

Wersja 2.0

**Projekt współfinansowany ze środków Europejskiego
Funduszu Rozwoju Regionalnego
w ramach Programu Operacyjnego Innowacyjna Gospodarka**

Konfiguracja w zakresie integracji

SPIS TREŚCI

SPIS TREŚCI	2
1 Wprowadzenie.....	3
2 Podział usług na zabezpieczone i nie zabezpieczone	4
2.1 Usługi zabezpieczone.....	4
2.2 Usługi niezabezpieczone	5
3 Powiązanie z usługami systemu PZ.....	6
4 Konfiguracja systemu w ePUAP	9
5 Konfiguracja udostępniania usług, skrytki i elementów formularza.	13
5.1 Konfiguracja trybu pracy.....	13
5.2 Konfiguracja ustawień transmisji	14
5.3 Konfiguracja formularza w zakresie komunikacji z web serwisem.....	15
5.3.1 Elementy konfiguracyjne kontrolki Pobierz XML	16

1 Wprowadzenie

Jedną z funkcjonalności pozwalających na pełne wykorzystanie ePUAP, jest możliwość integracji z systemami zewnętrznymi zarówno usługodawców, jak i usługobiorców. Integracja umożliwia łączenie ze sobą różnorodnych aplikacji i tym samym automatyzację i uproszczenie wymiany danych. Aby wymiana danych przebiegała prawidłowo należy dokonać odpowiedniej konfiguracji zarówno od strony systemu zewnętrznego, jak i ePUAP. W niniejszej instrukcji zostały przedstawione podstawowe informacje dotyczące konfiguracji ePUAP.

2 Podział usług na zabezpieczone i nie zabezpieczone

2.1 Usługi zabezpieczone

W komunikacji pomiędzy ePUAP, a systemami zewnętrznymi, stosowany jest standardowy mechanizm WS-Security.

Dopuszczalne algorytmy używane w WS-Security to:

- skrótu - <http://www.w3.org/2001/04/xmlenc#sha256>
- podpisu - <http://www.w3.org/2001/04/xmldsig-more#rsa-sha256>
- kanonikalizacji - <http://www.w3.org/2001/10/xml-exc-c14n#>

Przykładowy nagłówek

```
<soapenv:Envelope xmlns:fil="http://wsdl.epuap.gov.pl/filerepocore/"
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header>
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">
      <wsse:BinarySecurityToken EncodingType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary"
      ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3" wsu:Id="X509-827A7F52E3D7B6731E154340469572511">
        MIID0zCCArugAwIBAgIIBuyFErafp...
      </wsse:BinarySecurityToken>
      <ds:Signature Id="SIG-827A7F52E3D7B6731E154340469572615"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#">
            <ec:InclusiveNamespaces PrefixList="fil soapenv"
              xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </ds:CanonicalizationMethod>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256" />
            <ds:Reference URI="#id-827A7F52E3D7B6731E154340469572514">
              <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                  <ec:InclusiveNamespaces PrefixList="fil"
                    xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
                  </ds:Transform>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
              </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>anzFaB9pqAOIOJ0IfQHQ6PPAN...</ds:SignatureValue>
            <ds:KeyInfo Id="KI-827A7F52E3D7B6731E154340469572512">
              <wsse:SecurityTokenReference wsu:Id="STR-
827A7F52E3D7B6731E154340469572513">
                <wsse:Reference URI="#X509-827A7F52E3D7B6731E154340469572511"
                  ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3" />
              </wsse:SecurityTokenReference>
            </ds:KeyInfo>
          </ds:SignatureValue>
        </ds:Signature>
      </wsse:Security>
    </soapenv:Header>
  </soapenv:Envelope>
```

Konfiguracja w zakresie integracji

```
</wsse:SecurityTokenReference>
  </ds:KeyInfo>
</ds:Signature>
</wsse:Security>
</soapenv:Header>
<soapenv:Body>
  ....
</soapenv:Body>
</soapenv:Envelope>
```

Usługi sieciowe ePUAP wymagają, aby element soap:body przesyłanej wiadomości, stanowiącej wywołania operacji, podpisany był certyfikatem zarejestrowanym w systemie ePUAP. Certyfikat musi być:

- w standardzie X.509 v.3.,
- wydany przez zaufane centrum certyfikacji.

Do usług, które wymagają podpisu certyfikatem należą:

- Skrytka,
- Doreczyciel,
- pull,
- FileRepoService,
- obsługaUpp,
- SłownikiReferencyjne,
- ValidatorWS,
- OrganizationExtService,
- KupWebServices,
- KupWebServicesExt,
- PLService,
- Płatności,
- Podmioty,
- ZarządzanieDokumentami,

2.2 Usługi niezabezpieczone

Usługa SłownikiReferencyjnePublic nie wymaga, aby wiadomość stanowiąca wywołanie operacji była podpisana certyfikatem.

3 Powiązanie z usługami systemu PZ

Funkcjonalności podpisywania przy pomocy Profilu Zaufanego oraz logowania SSO do ePUAP w systemie zewnętrznym nie jest realizowana w systemie epuap.gov.pl tylko w systemie pz.gov.pl. Wymaga ponadto dodania certyfikatu oraz nadania uprawnień dla systemu zewnętrznego w systemie pz.gov.pl (podsystem PZ oraz DT). Uprawnienia są dodawane oraz aktualizowane **tylko przez Administratorów COI**.

Należy pamiętać, że w zakresie usług realizowanych przez system ePUAP, system zewnętrzny integruje się z ePUAP i Administrator podmiotu samodzielnie wgrywa certyfikat.

W zakresie usług realizowanych przez system PZ oraz DT system zewnętrzny integruje się z systemem pz.gov.pl i certyfikat i uprawnienia są dodawane tylko przez Administratorów COI.

Do integracji do w/w systemów **może być wykorzystywany ten sam certyfikat**.

Dla systemów zewnętrznych, które integrują się tylko z systemem pz.gov.pl procedura wnioskowania o uprawnienia w systemie PZ dostępna jest na stronie:

<http://mc.bip.gov.pl/departament-utrzymania-i-rozwoju-systemow/integracja-systemow-z-profilem-zaufanym.html>

Dla systemów, które integrują się z ePUAP, PZ oraz DT zalecaną ścieżką jest dodanie certyfikatu przez Administratora podmiotu w ePUAP, a następnie należy drogą mailową przekazać zgłoszenie do Centralnego Ośrodka Informatyki na adres mailowy: epuap-pomoc@coi.gov.pl

Zgłoszenie **musi** zawierać w treści:

Temat wiadomości:	Wgranie certyfikatu do integracji
Nazwa systemu:	<i>Tutaj nazwa systemu, który ma się integrować</i>
Identyfikator podmiotu na ePUAP:	<i>Identyfikator podmiotu</i>
Certyfikat	<i>Certyfikat X.509 zakodowany algorytmem Base-64(.CER) lub dane certyfikatu (DN)</i>

Podstawowy zakres usług, z których będzie mógł korzystać zintegrowany system znajduje się poniżej:

- SignatureVerification.verifySignature
- TpSigning.addDocumentToSigning
- TpSigning.getSignedDocument
- TpSigning.hasTrustedProfileInstitution
- TpSigning.hasTrustedProfilePerson

Konfiguracja w zakresie integracji

- TpSigning.verifySignedDocument
- TpUserInfo.getTpUserInfo

Dodatkowo system zewnętrzny może korzystać z usług:

- TpSigning3.addDocumentToSigning
- TpSigning3.getSignedDocument
- TpMultisign.addDocumentToSigning
- TpMultisign.getSignedDocument
- TpAuthorizationMethodsInfo.getAuthorizationMethodsInfo
- TpConfirmationPointsInfo.getConfirmationPointAddresses

Pozostałe usługi systemu opisane w dokumentacji:

[Szczegółowy opis usług Profilu Zaufanego](#)

używane są przez integracje wewnętrzne oraz systemy centralne.

W celu realizacji logowania SSO musi być utworzony system kliencki w systemie DT. W tym celu należy podać dodatkowo następujące parametry:

Nazwa SAML (Issuer)	<i>Przy wnioskowaniu dla nowego systemu zalecane jest podanie URL, pod którym dostępny jest system zewnętrzny, np. https://domena.pl (Nazwa jest unikalna)</i>
Adres zwrotny dla usługi SSO	<i>Lista prefiksów adresów URL oddzielonych spacjami, od których musi rozpoczynać się adres URL w polu AssertionConsumerServiceURL w komunikacie SAML AuthnRequest pochodzącym z systemu klienckiego i na który DT wysyła Artefact SAML po poprawnym uwierzytelnieniu użytkownika w DT</i>
Adres zwrotny dla usługi SLO	<i>Adres zwrotny dla usługi Single Logout – Adres URL w systemie klienckim, na który DT wysyła komunikaty SAML LogoutRequest otrzymany z systemu klienckiego (wylogowanie użytkownika inicjowane przez system kliencki), jeżeli będzie realizowane wylogowanie.</i>
Uprawnienie w systemie DT	<i>Dostęp do usług Single Sign-On i Single Logout</i>

Konfiguracja w zakresie integracji

Podstawowe informacje na temat realizacji logowania do systemu PZ, podpisywania dokumentu i pobierania danych użytkownika sesji zostały opisane w dokumencie:

https://pz.gov.pl/Instrukcja_dla_Integratora_PZ_logowanie.pdf

4 Konfiguracja systemu w ePUAP

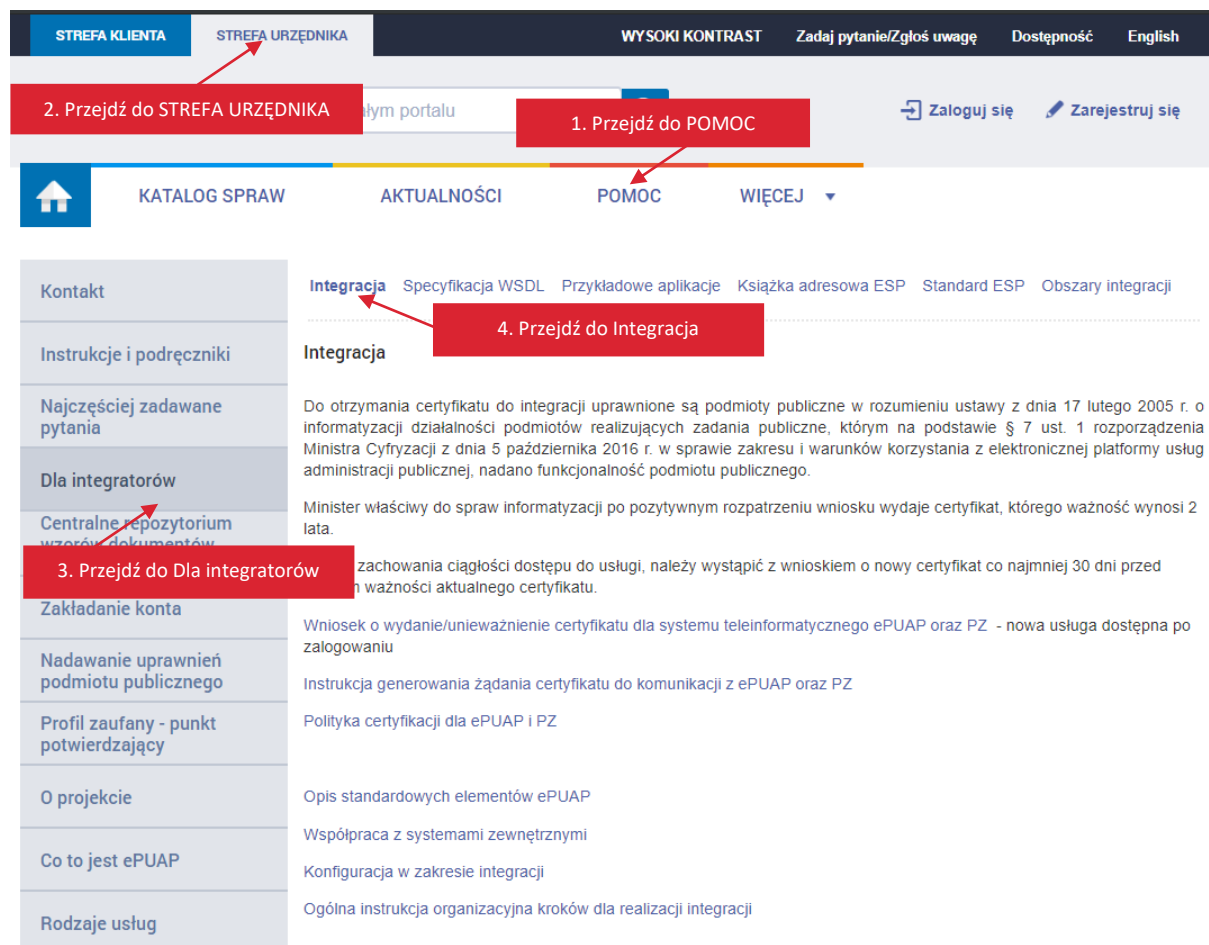
System – byt odpowiadający użytkownikowi, który może mieć nadawany dostęp do aplikacji poprzez mechanizm ról i uprawnień. System w systemie ePUAP reprezentowany jest przez certyfikat. Certyfikat należy zainstalować w systemie operacyjnym, a następnie zarejestrować w systemie zewnętrznym oraz w ePUAP.



Szczegółowych informacji na temat konfiguracji systemu zewnętrznego dostarcza dostawca tego systemu.

Aby zarejestrować system w ePUAP przygotuj plik certyfikat.txt otrzymany z centrum certyfikacji w odpowiedzi na wniosek wysłany za pomocą usługi udostępnionej na ePUAP. Szczegółowe informacje o usłudze znajdują się w POMOCY ePUAP, zakładka STREFA URZĘDNIKA, Dla integratorów, Integracja.

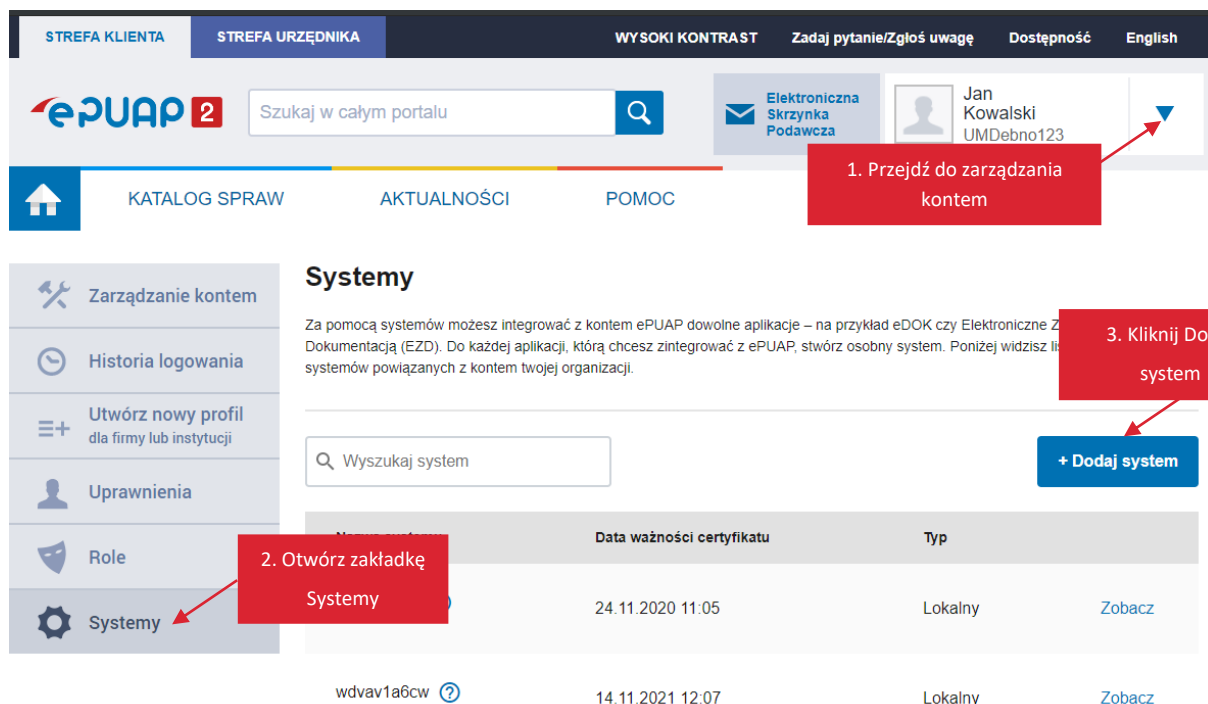
Konfiguracja w zakresie integracji



The screenshot shows the ePUAP portal interface. At the top, there is a navigation bar with 'STREFA KLIENTA' and 'STREFA URZĘDNIKA'. Below it, a secondary bar contains '2. Przejdź do STREFA URZĘDNIKA', 'WYSOKI KONTRAST', 'Zadaj pytanie/Zgłoś uwagę', 'Dostępność', and 'English'. The main navigation menu includes 'KATALOG SPRAW', 'AKTUALNOŚCI', 'POMOC', and 'WIĘCEJ'. The left sidebar lists various categories, with 'Dla integratorów' highlighted. The main content area shows the 'Integracja' section, which includes links to 'Specyfikacja WSDL', 'Przykładowe aplikacje', 'Książka adresowa ESP', 'Standard ESP', and 'Obszary integracji'. Red arrows and boxes indicate the following steps: 1. Click 'POMOC' in the top menu. 2. Click 'STREFA URZĘDNIKA' in the top navigation bar. 3. Click 'Dla integratorów' in the left sidebar. 4. Click 'Integracja' in the main content area.

Do ePUAP zaloguj się na podmiot organizacji, dla której został wystawiony certyfikat. Rozwiń menu i przejdź do **Zarządzania kontem**, następnie otwórz zakładkę **Systemy**. W zakładce Systemy wyświetli się ekran, który umożliwi ci dodanie nowego systemu. Kliknij w prawym górnym rogu przycisk **Dodaj system**.

Konfiguracja w zakresie integracji



Systemy

Za pomocą systemów możesz integrować z kontem ePUAP dowolne aplikacje – na przykład eDOK czy Elektroniczne Zgłoszenie (EZD). Do każdej aplikacji, którą chcesz zintegrować z ePUAP, stwórz osobny system. Poniżej widzisz listę systemów powiązanych z kontem twojej organizacji.

Wyszukaj system

	Data ważności certyfikatu	Typ	
Systemy	24.11.2020 11:05	Lokalny	Zobacz
wdvav1a6cw	14.11.2021 12:07	Lokalny	Zobacz

Wyświetli się formularz System. Wypełnij pola:

- Opisz system** – wpisz informacje, dzięki którym będzie wiadomo jaki system integrujesz z ePUAP.
- Certyfikat** – otwórz plik certyfikat.txt otrzymany z centrum certyfikacji w dowolnym edytorze tekstu. Skopiuj pierwszy certyfikat. Skopiowana część powinna zawierać:

-----BEGIN CERTIFICATE-----

(Ciąg znaków)

-----END CERTIFICATE-----

Pozostałe trzy certyfikaty to certyfikaty pośrednie (Root CA) .

- Role** – nadaj role w zależności od potrzeb usług sieciowych, z których korzysta system integrujący się z ePUAP. Najczęściej wystarczy nadanie roli **Rola domyślna**, część usług wymaga roli **Instytucja Publiczna**. Możesz również nadać inną rolę jeśli takie wymaganie poda dostawca systemu integrującego się z ePUAP.

Konfiguracja w zakresie integracji

Zarządzanie kontem

Historia logowania

Utwórz nowy profil dla firmy lub instytucji

Uprawnienia

Role

Systemy

System

Nazwa i opis systemu

Nazwa systemu jest generowana automatycznie – nie możesz jej nadać ani zmienić. Dlatego opisz system tak, aby łatwo go rozpoznać. W opisie koniecznie podaj nazwę aplikacji, z którą integrujesz ePUAP.

Nazwa systemu (automatycznie)

Opisz system

eDOK

1. Opisz system

Certyfikat

Certyfikat dostaniesz e-mailem z centrum certyfikacji (znajdziesz go w pliku .txt). Skopiuj część publiczną certyfikatu (od BEGIN CERTIFICATE do END CERTIFICATE) i wklej w pole poniżej.

2. Wklej certyfikat

```
-----BEGIN CERTIFICATE-----
MIIDbDCCAlSgAwIBAgIlecmVoLKw5eAwDQYJKoZIhvcNAQELBQAwFz
EVBMBGA1UE
AwWMSU5UX2VQVUFQaVBaMB4XDTE5MDIxMTEzNDMxMFoXDTE5MDIxM
```

Dane certyfikatu

Podmiot

Wystawca

Numer seryjny 79c995a0b2b0e5e0

Ważny od 11.02.2019 14:43

Ważny do 10.02.2021 14:43

Powyższe informacje zostaną zapisane po kliknięciu przycisku Dodaj system, wtedy też nastąpi ostateczna walidacja tych danych.

Role

Poniżej widzisz listę ról dostępnych dla tego systemu. Wybierz którą chcesz mu nadać.

3. Zaznacz niezbędne role

4. Kliknij Dodaj system

☒ Instytucja_Publiczna

☒ Rola domyślna

Anuluj Dodaj system

Gdy wypełnisz pola, kliknij **Dodaj system**. Wyświetli się komunikat, że system został dodany.

✓ System został dodany.

5 Konfiguracja udostępniania usług, skrytki i elementów formularza.

W konfiguracji usług, w trakcie dodawania karty sprawy jest krok przypisania formularza do karty sprawy. W tym kroku należy również wskazać skrytkę, przez którą będą przechodziły wypełnione dokumenty. Jest to element, na który należy zwrócić uwagę w przypadku integracji systemu zewnętrznego z systemem ePUAP, ponieważ system zewnętrzny będzie się komunikował tylko ze skrytką, która będzie w nim zdefiniowana. Dlatego w tym kroku należy wskazać skrytkę skonfigurowaną do współpracy z systemem zewnętrznym.

W konfiguracji skrytki, która będzie się komunikować z systemami zewnętrznymi należy zwrócić uwagę na dwie zakładki konfiguracyjne na rysunku poniżej: Tryb pracy oraz Ustawienia transmisji.



5.1 Konfiguracja trybu pracy

W zakresie integracji w konfiguracji trybu pracy skrytki istotne są następujące elementy:

- Typ skrytki
 - synchroniczna – Skrytka wysyłająca dokument od razu na adres systemu. Wszystko zaczyna się i kończy w ramach jednej transakcji. Najważniejszą cechą skrytki synchronicznej jest to, że odpowiedź jest zwracana dopiero po uzyskaniu odpowiedzi od systemu docelowego,
 - asynchroniczna – Skrytka kolejująca dokumenty. Wysyła dopiero dokumenty na podany adres po pewnym czasie w zależności od dokumentów czekających w kolejce danej skrytki i od jej konfiguracji.
- Tryb pracy
 - PUSH – dokument po dotarciu na skrytkę jest automatycznie przekierowywany pod wskazany adres,
 - PULL – dokument jest zatrzymywany na skrytce aż do czasu ściągnięcia go na żądanie przez system zewnętrzny.
- Maksymalna liczba dokumentów w kolejce – Limit maksymalnej liczby dokumentów na skrytce. Po przekroczeniu limitu skrytka zostaje zablokowana.

Konfiguracja w zakresie integracji

Typ skrytki:

☐ synchroniczna
 ☐ asynchroniczna

Typ skrytki

Tryb pracy :

☐ PUSH
 ☐ PULL

Tryb pracy

Maksymalna liczba dokumentów w kolejce:

Maksymalna liczba dokumentów w kolejce

5.2 Konfiguracja ustawień transmisji

W zakresie integracji w konfiguracji ustawień transmisji skrytki istotne są następujące elementy:

- **Adres systemu odbiorcy dla dokumentów/UPP:**
 - **Moje dokumenty** – odbiór dokumentów/UPP odbywa się w jednym ze składów użytkownika, zdefiniowanym w ustawieniach mapowania,
 - **Koordinator** – dokumenty/UPP są wysyłane do zdefiniowanego procesu koordynatora,
 - **Własny** – dokumenty/UPP są wysyłane na adres systemu zewnętrznego. W tym miejscu należy wprowadzić prawidłowy adres systemu zewnętrznego.
- **Rodzaj transmisji dla systemu odbiorcy:**
 - **SOAP binarnie** – standardowe wywołanie web serwisu,
 - **HTTP POST** – wywołanie web serwisu metodą HTTP POST.

Konfiguracja w zakresie integracji

☐ Moje dokumenty  **Ustawienia mapowania**

Mapowanie adresów skrzytek na składy

Adres Skład

Adres systemu odbiorcy dla dokumentów:

☐ Koordynator

☐ własny:

☐ Moje dokumenty  **Ustawienia mapowania**

Mapowanie adresów skrzytek na składy

Adres Skład

Adres systemu odbiorcy dla UPP:

☐ Koordynator

☐ własny:

Rodzaj transmisji do systemu odbiorcy ☐ SOAP binarnie ☐ HTTP POST 

5.3 Konfiguracja formularza w zakresie komunikacji z web serwisem

W trakcie tworzenia formularza w edytorze formularzy możliwe jest zdefiniowanie kontrolki: Pobierz XML

Dodaj pole	Pokaż/Ukryj
Pole edycji	Pole tekstowe
Lista	Wybierz kilka
Wybierz jeden	Data
Załącznik	Wypełnij
Sekcja	Pobierz XML

Typ skrytki

Konfiguracja w zakresie integracji

Kontrolka Pobierz XML umożliwia komunikację z web serwisem przygotowanym przez użytkownika zewnętrznego. Np. z web serwisem, który zwraca adres firmy o zadanym numerze NIP. Aby komunikacja z web serwisem była możliwa należy taką kontrolkę odpowiednio skonfigurować.

5.3.1 Elementy konfiguracyjne kontrolki Pobierz XML

Warunkiem prawidłowego działania kontrolki Pobierz XML jest prawidłowe ustawienie właściwości tej kontrolki, czyli:

- Opis – tekst, który ma się pojawić na kontrolce (przycisku),
- Instancja wyjściowa – nazwa instancji, z której zostaną pobrane dane do wysłania na skrytkę,
- Instancja wejściowa – nazwa instancji, do której zostanie wstawiony wynik wysłany przez skrytkę,
- Adres skrytki – adres skrytki, na który mają zostać wysłane dane z instancji wyjściowej po naciśnięciu przycisku,
- Uruchom automatycznie – czy uruchomić automatycznie w momencie załadowania formularza.

