



ePUAP

Konfiguracja w zakresie integracji

Wersja 2.1

**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	7
5 Konfiguracja udostępniania usług, skrytki i elementów formularza.	11
5.1 Konfiguracja trybu pracy.....	11
5.2 Konfiguracja ustawień transmisji	12
5.3 Konfiguracja formularza w zakresie komunikacji z web serwisem.....	13
5.3.1 Elementy konfiguracyjne kontrolki Pobierz XML	14

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:Transform>
                  </ds:Transforms>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                </ds:Reference>
              </ds:SignedInfo>
              <ds:SignatureValue>anzFaB9pqAOIOJ0IfQHQR6PPAN...</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:SignatureMethod>
          </ds:Signature>
        </ds:SignedInfo>
      </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 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. 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 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 z systemem pz.gov.pl instrukcje dostępne są na stronie:

<https://mc.bip.gov.pl/integracja-z-podpisem-zaufanym/e-podpis-tps5-dokumentacja-dotyczaca-integracji-z-podpisem-zaufanym-oraz-podpisem-osobistym.html>

4 Konfiguracja systemu w ePUAP

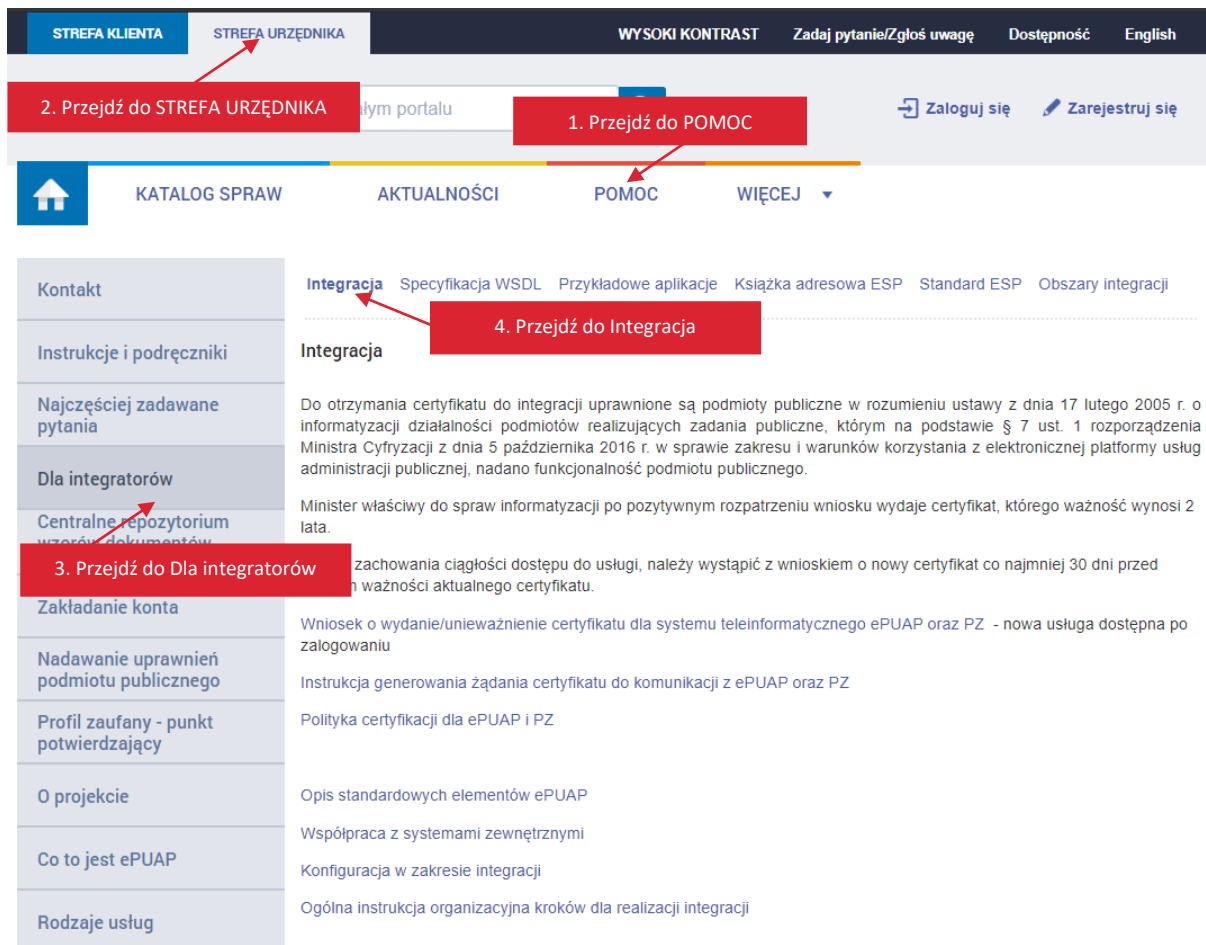
System – byt odpowiadający użytkownikowi, który może mieć nadawany dostęp do aplikacji poprzez mechanizm ról i uprawnień. System w systemie ePUAP reprezentowany jest przez certyfikat. Certyfikat należy zainstalować w systemie operacyjnym, a następnie zarejestrować w systemie zewnętrznym oraz w ePUAP.



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 are navigation tabs: 'STREFA KLIENTA' and 'STREFA URZĘDNIKA'. Below them is a header with 'WYSOKI KONTRAST', 'Zadaj pytanie/Zgłoś uwagę', 'Dostępność', and 'English'. A main navigation bar contains 'KATALOG SPRAW', 'AKTUALNOŚCI', 'POMOC', and 'WIĘCEJ'. A sidebar on the left lists various services. The main content area shows the 'Integracja' section, which is highlighted with a red box and an arrow labeled '4. Przejdź do Integracja'. Other red boxes and arrows indicate the path: '2. Przejdź do STREFA URZĘDNIKA' (pointing to the top navigation), '1. Przejdź do POMOC' (pointing to the 'POMOC' menu item), and '3. Przejdź do Dla integratorów' (pointing to the 'Dla integratorów' sidebar item).

Kontakt	Integracja Specyfikacja WSDL Przykładowe aplikacje Książka adresowa ESP Standard ESP Obszary integracji
Instrukcje i podręczniki	Integracja
Najczęściej zadawane pytania	Do otrzymania certyfikatu do integracji uprawnione są podmioty publiczne w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, którym na podstawie § 7 ust. 1 rozporządzenia Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej, nadano funkcjonalność podmiotu publicznego.
Dla integratorów	Minister właściwy do spraw informatyzacji po pozytywnym rozpatrzeniu wniosku wydaje certyfikat, którego ważność wynosi 2 lata.
Centralne repozytorium wzorów dokumentów	z zachowania ciągłości dostępu do usługi, należy wystąpić z wnioskiem o nowy certyfikat co najmniej 30 dni przed ważności aktualnego certyfikatu.
Zakładanie konta	Wniosek o wydanie/unieważnienie certyfikatu dla systemu teleinformatycznego ePUAP oraz PZ - nowa usługa dostępna po zalogowaniu
Nadawanie uprawnień podmiotu publicznego	Instrukcja generowania żądania certyfikatu do komunikacji z ePUAP oraz PZ
Profil zaufany - punkt potwierdzający	Polityka certyfikacji dla ePUAP i PZ
O projekcie	Opis standardowych elementów ePUAP
Co to jest ePUAP	Współpraca z systemami zewnętrznymi
Rodzaje usług	Konfiguracja w zakresie integracji
	Ogólna instrukcja organizacyjna kroków dla realizacji integracji

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

1. Przejdź do zarządzania kontem

2. Otwórz zakładkę Systemy

3. Kliknij Dodaj system

Systemy

Za pomocą systemów możesz integrować z kontem ePUAP dowolne aplikacje – na przykład eDOK czy Elektroniczne Z Dokumentacją (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

Wyświetlił 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.

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:

- Tryb 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,
 - Koordynator – 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 i
Ustawienia mapowania

Mapowanie adresów skrytek na sklady

Adres	Sklad
-------	-------

Adres systemu odbiorcy dla dokumentów:

Koordynator

własny:

Moje dokumenty i
Ustawienia mapowania

Mapowanie adresów skrytek na sklady

Adres	Sklad
-------	-------

Adres systemu odbiorcy dla UPP:

Koordynator

własny:

Rodzaj transmisji do systemu odbiorcy

SOAP binarnie
 HTTP POST i

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.