

PZ-Instrukcja logowania do systemu PZ, podpisywania dokumentu i pobierania danych użytkownika sesji

Spis treści

ZALOGOWANIE DO PROFILU ZAUFANEGO	2
POBRANIE IDENTYFIKATORA SESJI TGSID	2
PODPISANIE DOKUMENTU.....	2
POBRANIE DANYCH UŻYTKOWNIKA SESJI	3

1. Zalogowanie do Profilu Zaufanego

Do zalogowania użytkownika w Profilu Zaufanym używana jest usługa Single-Sign-On w systemie Dostawca Tożsamości o adresie sieciowym: <https://pz.gov.pl/dt/SingleSignOnService>
Żądanie uwierzytelnienia SAML (<**AuthnRequest**>) do systemu Dostawca Tożsamości przekazywane jest poprzez przeglądarkę internetową przy użyciu formularza HTML.

W celu przygotowania formularza HTML należy wykonać następujące kroki:

- Utworzyć żądanie **AuthnRequest**
- Podpisać żądanie **AuthnRequest** zgodnie XML Schema SAML 2.0.
- Utworzyć wysłać do przeglądarki formularz HTML umożliwiający automatyczne wywołanie systemu Dostawca Tożsamości zawierający zakodowane w Base64 żądanie **AuthnRequest**

2. Pobranie identyfikatora asercji

Do pobrania asercji służy usługa **ArtifactResolution** Systemu **Dostawca Tożsamości** o adresie sieciowym: <https://pz.gov.pl/dt-services/idpArtifactResolutionService>

- Utworzyć żądanie SAML **ArtifactResolve** podając wstawiając identyfikatora wystawcy SAML jako wartość znacznika <**Issuer**> oraz wartość artefaktu uzyskanego z logowania do systemu Dostawca Tożsamości do znacznika <**Artifact**>.
- Podpisać żądanie metodą **Enveloped** używając certyfikatu zawierającego klucz prywatny (certyfikatu przypisanego do systemu zewnętrznego wywołującego usługę)
- Wysłać podpisane żądanie do usługi: <https://pz.gov.pl/dt-services/idpArtifactResolutionService>
- Zweryfikować podpis cyfrowy odpowiedzi (*response*) z usługi przy użyciu certyfikatu z kluczem publicznym do weryfikacji odpowiedzi z PZ (certyfikat można poprać ze strony <https://pz.gov.pl> - zakładka „Pomoc”)
- Z otrzymanej odpowiedzi pobrać wartość identyfikatora asercji (wartość atrybutu **ID** węzła **Assertion**)

3. Podpisanie dokumentu

Do uwierzytelnienia użytkownika i powiązania z Profilem Zaufanym konieczne jest wykonanie podpisu dokumentu.

Podpisanie dokumentu wykonuje usługa **TpSigning** Systemu Profil Zaufany o adresie sieciowym: <https://pz.gov.pl/pz-services/tpSigning>

- Utworzyć żądanie **addDocumentToSigning**
- Podpisać żądanie **addDocumentToSigning** metodą **WSec** używając klucza prywatnego (klucza przypisanego do systemu zewnętrznego wywołującego usługę)
- Wysłać podpisane żądanie do usługi: <https://pz.gov.pl/pz-services/tpSigning>
- Zweryfikować podpis cyfrowy odpowiedzi (*response*) z usługi przy użyciu certyfikatu z kluczem publicznym do weryfikacji odpowiedzi z PZ (certyfikat można poprać ze strony <https://pz.gov.pl> - zakładka „Pomoc”).
- Obsłużyć wynik żądania **addDocumentToSigningResponse** (*link*) ze znacznika <**addDocumentToSigningReturn**>:
 - Przekierować na stronę uzyskaną w wyniku żądania addDocumentToSigning
 - Pobrać podpisany dokument

4. Pobranie danych użytkownika sesji

Do pobrania danych użytkownika sesji służy metoda **getTpUserInfo** wystawiana przez usługę PZ: <https://pz.gov.pl/pz-services/tpUserInfo>

Metoda zwraca następujące informacje dla danych osoby fizycznej:

- Adres e-mail
- Nazwisko
- Imię
- PESEL
- Identyfikator Profilu Zaufanego
- Identyfikator konta użytkownika

W celu pobrania danych należy wykonać następujące kroki

- Utworzyć komunikat (*request*) dla operacji **getTpUserInfo** wstawiając do znacznika **<tgsid>** wartość identyfikatora asercji
- Podpisać komunikat (*request*) metodą **WSSec** używając klucza prywatnego (*klucza przypisanego do systemu zewnętrznego wywołującego usługę*)
- Wysłać podpisany komunikat (*request*) na adres sieciowy <https://pz.gov.pl/pz-services/tpUserInfo>
- Zweryfikować podpis cyfrowy odpowiedzi (*response*) z usługi przy użyciu certyfikatu z kluczem publicznym do weryfikacji odpowiedzi z PZ (certyfikat można pobrać ze strony <https://pz.gov.pl> - zakładka „Pomoc”)
- Pobrać wymagane wartości z odpowiedzi.

Szczegółowe dane dotyczące typów danych, formatów żądań i odpowiedzi opisane są w dokumentach „*Instrukcja dla Integratora PZ*”, „*Instrukcja dla Integratora DT*” i „*Instrukcja dla Integratora DT - pliki WSDL*” znajdującej się na stronie <https://pz.gov.pl> - zakładka „Pomoc”.