INSTRUKCJA DLA INTEGRATORA SYSTEMU DOSTAWCA TOŻSAMOŚCI

Spis treści

1. Cel i zakres dokumentu 3
1.1. Słownik pojęć i skrótów 3
2. Dostęp do usług sieciowych DT 4
2.1. WS-Security 4
2.2. Wspólny nagłówek żądania i odpowiedzi 6
2.3. Odpowiedź informująca o błędzie 8
3. Definicja usług sieciowych DT 10
3.1. Usługa `IdpIdentityManagement` 10
3.1.1. Operacja `createIdentity` 10
3.1.2. Operacja `modifyIdentity` 12
3.1.3. Operacja `isUserIdAvailable` 13
3.2. Usługa `IdpIdentityInfo` 15
3.2.1. Operacja `getUserInfo` 15
3.2.2. Operacja `resolveUserId` 17
4. Uwierzytelnienie przy pomocy SAML w systemie DT 19
5. SAML w komunikacji z Zewnętrznymi Dostawcami Tożsamości 24
5.1. Uwierzytelnienie w ZDT 24
5.2. Autoryzacja podpisu profilem zaufanym w ZDT 29
5.3. Reguły przetwarzania 32

1. Cel i zakres dokumentu

Niniejszy dokument opisuje usługi sieciowe systemu Dostawca Tożsamości na poziomie technicznym. Jest przeznaczony dla twórców systemów integrujących się z systemem DT na poziomie tych interfejsów.

1.1. Słownik pojęć i skrótów

Pojęcia i skróty użyte w dokumencie mają następujące znaczenie.

Pojęcie/skrót	Znaczenie
System DT	System Dostawca Tożsamości
System kliencki	System używający usług sieciowych systemu DT
Administrator systemu DT	Użytkownik systemu DT posiadający uprawnienie do zarządzania słownikiem systemów klienckich
Usługa sieciowa	Metoda komunikacji elektronicznej pomiędzy systemami informatycznymi; W Systemie DT usługi sieciowe zaimplementowane są z wykorzystaniem SOAP/HTTP
SOAP	Simple Object Access Protocol – protokół wymiany informacji ustrukturalizowanej w usłudze sieciowej (http://www.w3.org/TR/soap)
WSDL	Web Services Description Language (http://www.w3.org/TR/wsdl)
Operacja usługi sieciowej	Akcja SOAP w znaczeniu stosowanym w WSDL
WS-Security	Web Services Security – rozszerzenie SOAP w celu zabezpieczenia usług sieciowych. (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss)
SSO	Single sign-on – sposób organizacji kontroli dostępu do systemów informatycznych, gdzie uwierzytelnianiem użytkowników zajmuje się dedykowany system
SAML	Security Assertion Markup Language – standard wymiany danych służących do uwierzytelnienia i autoryzacji użytkowników. (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security)
Asercja	Pakiet informacji dotyczących bezpieczeństwa w SAML
Artefakt	Referencja do asercji SAML
Zewnętrzny Dostawca Tożsamości (ZDT)	System teleinformatyczny który pełni rolę dostawcy tożsamości dla systemu DT, również dla funkcji autoryzacji podpisu profilem zaufanym

INNOWACYJNA GOSPODARKA NARODOWA STRATEGIA SPÓJNOŚCI
ePUAP 2
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO
Centralny Ośrodek Informatyki ul. Suwak 3, 02-676 Warszawa tel: 22 250 28 83 mail: coi@coi.gov.pl | www.coi.gov.pl

2. Dostęp do usług sieciowych DT

Wszystkie usługi sieciowe systemu DT zabezpieczone są za pomocą protokołu WS-Security. Uzyskanie dostępu do usługi przez system kliencki związane jest ze spełnieniem wszystkich poniższych warunków:

- Żądanie wysyłane do systemu DT musi być podpisane certyfikatem klienckim. Podpis musi być zgodny z protokołem WS-Security.
- System kliencki musi być wpisany przez administratora systemu DT na listę znanych systemów klienckich w systemie DT.
- Certyfikat kliencki użyty przez system kliencki do podpisania żądania musi być dodany przez administratora systemu DT do listy certyfikatów systemu klienckiego w systemie DT.
- System kliencki musi być oznaczony przez administratora systemu DT jako aktywny w systemie DT.
- System kliencki musi mieć przyznane przez administratora systemu DT uprawnienie do wywoływania metody usługi sieciowej w systemie DT.

Dla zwiększenia bezpieczeństwa, system DT przy konstruowaniu odpowiedzi nie ujawnia, który z powyższych warunków nie został spełniony przez klienta. W każdym przypadku zwracana jest odpowiedź podobna do poniższej:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Header/>
  <soap:Body>
    <soap:Fault>
      <faultcode>soap:Server</faultcode>
      <faultstring>Brak uprawnień do wywołania metody.</faultstring>
      <detail>
        <ns4:errorFault callId="2913616646816870912" responseTimestamp="2014-06-30T12:01:05.373+02:00"
xmlns:ns2="http://www.cpi.gov.pl/dt/CommonSchema"
xmlns:ns4="http://www.cpi.gov.pl/dt/IdpIdentityManagementService">
          <ns2:code>401</ns2:code>
          <ns2:description>Brak uprawnień do wywołania metody.</ns2:description>
        </ns4:errorFault>
      </detail>
    </soap:Fault>
  </soap:Body>
</soap:Envelope>
```

2.1. WS-Security

Każde żądanie wysyłane przez system kliencki do systemu DT musi być podpisane zgodnie z rozszerzeniem SOAP: WS-Security. Szczegółowa specyfikacja tego rozszerzenia dostępna jest pod adresem http://www.oasis-open.org/committees/wss. System DT wymaga, aby w wiadomości SOAP podpisany był element `<soap:Body>`. System weryfikuje obecność w żądaniu binarnego tokenu bezpieczeństwa typu X509v3.

Przykładowe podpisane żądanie wygląda następująco (długie wartości elementów zakodowane w Base64 zostały skrócone dla przejrzystości):

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:idpi="http://www.cpi.gov.pl/dt/IdpIdentityManagementService">
  <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="X509-8D58A61A83EB7640661398960091579265">MIIDZTCCAk2gAwI(...)</wsse:BinarySecurityToken>
      <ds:Signature Id="SIG-176" 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="soapenv idpi" xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          </ds:CanonicalizationMethod>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
          <ds:Reference URI="#id-175">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                <ec:InclusiveNamespaces PrefixList="idpi" xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
              </ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>e3x8yAjaJoXfO058N0z05VjSP4Q=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>hN1LsCfXAgUfuMLji5Zk(...)</ds:SignatureValue>
        <ds:KeyInfo Id="KI-8D58A61A83EB7640661398960091579266">
          <wsse:SecurityTokenReference wsu:Id="STR-8D58A61A83EB7640661398960091579267">
            <wsse:Reference URI="#X509-8D58A61A83EB7640661398960091579265" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"/>
          </wsse:SecurityTokenReference>
        </ds:KeyInfo>
      </ds:Signature>
    </wsse:Security>
  </soapenv:Header>
  <soapenv:Body wsu:Id="id-175" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">
    <idpi:reqIsLoginAvailable callId="6347177294896046332" requestTimestamp="2014-06-30T12:01:30.128+02:00">
      <idpi:userId>user01</idpi:userId>
    </idpi:reqIsLoginAvailable >
  </soapenv:Body>
</soapenv:Envelope>
```

Odpowiedź serwera na powyższe przykładowe żądanie jest również podpisana zgodnie z protokołem WS-Security i wygląda następująco:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <wsse:Security soap:mustUnderstand="1" 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-
8ACEA668E7B1B1E54F1398960101010217">MIIDbzCCAlegAwIBAgII(...)</wsse:BinarySecurityToken>
```

```
    <ds:Signature Id="SIG-73" 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="soap" xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        </ds:CanonicalizationMethod>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <ds:Reference URI="#Id-15963761">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
              <ec:InclusiveNamespaces PrefixList="" xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transform>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <ds:DigestValue>azRca9fQn08cGOxF3jBi6pt2vFw=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>kbhy/woiLGiUrkp43Joh8Jm(…)</ds:SignatureValue>
      <ds:KeyInfo Id="KI-8ACEA668E7B1B1E54F1398960101010218">
        <wsse:SecurityTokenReference wsu:Id="STR-8ACEA668E7B1B1E54F1398960101010219">
          <wsse:Reference URI="#X509-8ACEA668E7B1B1E54F1398960101010217" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"/>
        </wsse:SecurityTokenReference>
      </ds:KeyInfo>
    </ds:Signature>
  </wsse:Security>
 </SOAP-ENV:Header>
 <soap:Body wsu:Id="Id-15963761" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">
   <ns3:respIsLoginAvailable callId="6347177294896046332" responseTimestamp="2014-06-30T12:01:41.004+02:00"
xmlns:ns2="http://www.cpi.gov.pl/dt/CommonSchema" xmlns:ns3="
http://www.cpi.gov.pl/dt/IdpIdentityManagementService">
     <available>false</available>
   </ns3:respIsLoginAvailable>
 </soap:Body>
</soap:Envelope>
```

W dalszej części dokumentu w przykładowych komunikatach usług sieciowych nagłówek SOAP wraz z podpisem WS-Security będzie pominięty dla przejrzystości.

2.2. Wspólny nagłówek żądania i odpowiedzi

Usługi sieciowe systemu Dostawca Tożsamości posiadają standardowe atrybuty dodawane do żądania i odpowiedzi, ułatwiające analizę poprawności i efektywności działania usług.

W żądaniu wymagane są przez system następujące atrybuty wymienione w tabeli:

Pole	Typ	Wymagane	Opis
callId	long	tak	Losowa liczba naturalna identyfikująca wywołanie usługi sieciowej; Dopuszczalne jest użycie przez klienta tego samego identyfikatora w różnych wywołaniach. Klient powinien jednak zadbać o możliwie największą unikalność tych identyfikatorów, np. przez losowanie identyfikatora z całego zakresu 0 – 2^63-1 aby prawdopodobieństwo powtórzenia się było jak najniższe.
requestTimestamp	dateTime	tak	Znacznik czasu możliwie najbliższy momentowi wysłania żądania od klienta do systemu DT. Możliwe odchylenie wartości podanej w polu requestTimestamp wynosi [maksymalne dopuszczalne przesunięcie w czasie (niedokładność) między zegarami systemów biorących udział w wymianie wiadomości protokołu SOAP] ± 3 minuty (wartość konfigurowalna).

W odpowiedzi system DT dołącza następujące atrybuty:

Pole	Typ	Wymagane	Opis
callId	long	tak	Identyfikator wywołania usługi sieciowej skopiowany z żądania
responseTimestamp	dateTime	tak	Znacznik czasu możliwie najbliższy momentowi wysłania odpowiedzi od systemu DT do klienta

Atrybuty te są dołączane przez system DT również w przypadku zwrócenia odpowiedzi typu fault.

Przykładowe atrybuty w żądaniu wyglądają następująco:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:idpi="http://www.cpi.gov.pl/dt/IdpIdentityManagementService">
  <soapenv:Header/>
  <soapenv:Body>
    <idpi:reqIsLoginAvailable callId="6347177294896046332" requestTimestamp="2014-06-30T12:01:30.128+02:00">
      <idpi:userId>user01</idpi:userId>
    </idpi:reqIsLoginAvailable >
  </soapenv:Body>
</soapenv:Envelope>
```

Odpowiedź serwera na powyższe żądanie wygląda następująco:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Header/>
  <soap:Body>
```

```
    <ns3:respIsLoginAvailable callId="6347177294896046332" responseTimestamp="2014-06-30T18:01:41.004+02:00"
xmlns:ns2="http://www.cpi.gov.pl/dt/CommonSchema" xmlns:ns3="
http://www.cpi.gov.pl/dt/IdpIdentityManagementService">
       <available>false</available>
    </ns3:respIsLoginAvailable>
  </soap:Body>
</soap:Envelope>
```

2.3. Odpowiedź informująca o błędzie

W przypadku, gdy system DT nie jest w stanie poprawnie obsłużyć żądania, w odpowiedzi zwracany jest element typu SOAP Fault. Przykładowa odpowiedź wygląda następująco:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Header/>
  <soap:Body>
    <soap:Fault>
      <faultcode>soap:Client</faultcode>
      <faultstring>Brak tożsamości o identyfikatorze użytkownika 'user011'.</faultstring>
      <detail>
        <errorFault callId="2044934600846446110" responseTimestamp="2014-06-30T12:27:07.331+02:00"
xmlns="http://www.cpi.gov.pl/dt/IdpIdentityInfoServiceSchema" xmlns:ns3="http://www.cpi.gov.pl/dt/CommonSchema">
          <ns3:code>600</ns3:code>
          <ns3:description>Brak tożsamości o identyfikatorze użytkownika 'user011'.</ns3:description>
        </errorFault>
      </detail>
    </soap:Fault>
    </soap:Body>
</soap:Envelope>
```

Odpowiedź zawiera elementy wymienione w poniższej tabeli:

Element	Odbiorca	Przeznaczenie
faultcode	System kliencki	Element przyjmuje następujące wartości, zgodne ze specyfikacją SOAP: • Client – oznacza że żądanie jest nieuprawnione, skonstruowane w sposób nieprawidłowy lub zawiera nieprawidłowe dane. Po otrzymaniu takiej odpowiedzi system kliencki nie powinien ponawiać żądania w niezmienionej postaci, gdyż jego obsługa nigdy się nie powiedzie. • Server – oznacza że wystąpił błąd na serwerze uniemożliwiający obsługę żądania. Po otrzymaniu takiej odpowiedzi system kliencki może (ale nie musi) ponowić żądanie w niezmienionej postaci natychmiast, lub po pewnym czasie, gdyż jest prawdopodobne, że jego obsługa w końcu się powiedzie.

Element	Odbiorca	Przeznaczenie
faultstring	Administrator systemu klienckiego	Opis powodu nieobsłużenia żądania w postaci tekstu zrozumiałego dla człowieka; Jest przeznaczony dla administratora systemu klienckiego do diagnozowania błędów w komunikacji między systemami. Element nie powinien być używany do automatycznego podejmowania decyzji przez system kliencki, gdyż komunikaty w nim zawarte mogą ulegać zmianie w momencie aktualizacji oprogramowania systemu DT.
code	System kliencki	Element przyjmuje wartości właściwe dla konkretnej operacji usługi sieciowej, wymienione w opisie tej usługi w tym dokumencie. Może być użyty do automatycznego podejmowania decyzji przez system kliencki.

3. Definicja usług sieciowych DT

Schemat XML usług sieciowych systemu DT zawarty jest w plikach dołączonych do dokumentu.

3.1. Usługa `IdpIdentityManagement`

Usługa służy do zarządzania kontami użytkowników w systemie DT. Możliwe jest dodawanie kont, modyfikacja ich danych oraz sprawdzenie, czy identyfikator użytkownika jest zajęty.

Usługa dostępna jest pod adresem https://pz.gov.pl/dt-services/idpIdentityManagementService .

Definicja usługi znajduje się w pliku idpIdentityManagementService.wsdl. Typy danych używane przez usługę zawarte są w plikach identityManagement.xsd i common.xsd.

3.1.1. Operacja `createIdentity`

Operacja służy do utworzenia nowego konta użytkownika.

Struktura danych wymagana do założenia konta jest następująca:

Pole	Typ	Wymagane	Uwagi
userId	string(255)	tak	Pole może zawierać cyfry, małe i duże litery łacińskie oraz znaki '-' i '_'. Pozostałe znaki nie są dopuszczalne.
email	string(255)	tak	Adres email użytkownika
phoneNumber	string(40)	tak	Numer telefonu użytkownika z funkcją odbierania SMS
password	string(255)	nie	Hasło w postaci niezaszyfrowanej; Podlega walidacji zgodnie z polityką haseł systemu DT. Jeśli pole jest puste, zostanie utworzone konto bez hasła.

Jeśli utworzenie nowego konta udało się, zwracany jest pusty element odpowiedzi. W przeciwnym razie zwracany jest komunikat typu fault, a w nim jeden z poniższych kodów błędów:

Kod	Znaczenie	Przyczyna
401	brak uprawnień	• system kliencki nie jest uprawniony do wywołania usługi
600	nieprawidłowy parametr wywołania	• walidacja danych nowego konta wykazała błędy
601	zajęty identyfikator użytkownika	• identyfikator użytkownika jest już zajęty

Kod	Znaczenie	Przyczyna
602	hasło niezgodne z polityką haseł	• hasło nie spełnia polityki haseł
680	nieprawidłowy parametr requestTimestamp	• zbyt duża różnica między parametrem requestTimestamp a czasem systemowym serwera
500	błąd wewnętrzny	• wystąpił nieoczekiwany błąd w systemie DT

Przykładowe wywołanie metody wygląda następująco:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:idp="http://www.cpi.gov.pl/dt/IdpIdentityManagementServiceSchema">
  <soapenv:Header/>
  <soapenv:Body>
    <idp:reqCreateIdentity callId="6955045684918848071" requestTimestamp="2014-06-30T12:04:09.439+02:00">
      <idp:userId>user02</idp:userId>
      <idp:email>tomasz.nowak@adres.pl</idp:email>
      <idp:phoneNumber>+48600123456</idp:phoneNumber>
      <idp:password>Haslo@123</idp:password>
    </idp:reqCreateIdentity>
  </soapenv:Body>
</soapenv:Envelope>
```

Jeśli powyższe żądanie jest prawidłowe to odpowiedź serwera wygląda następująco:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Header/>
  <soap:Body>
    <ns4:respCreateIdentity callId="6955045684918848071" responseTimestamp="2014-06-30T12:04:09.718+02:00"
xmlns:ns2="http://www.cpi.gov.pl/dt/CommonSchema"
xmlns:ns4="http://www.cpi.gov.pl/dt/IdpIdentityManagementServiceSchema"/>
  </soap:Body>
</soap:Envelope>
```

Odpowiedź serwera na powyższe żądanie w przypadku nieprawidłowego parametru wywołania jest następująca:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Header/>
  <soap:Body>
    <soap:Fault>
      <faultcode>soap:Server</faultcode>
      <faultstring>Identyfikator użytkownika 'user02' jest już zajęty.</faultstring>
      <detail>
        <ns4:errorFault callId="6955045684918848071" responseTimestamp="2014-06-30T12:04:09.702+02:00"
xmlns:ns2="http://www.cpi.gov.pl/dt/CommonSchema"
xmlns:ns4="http://www.cpi.gov.pl/dt/IdpIdentityManagementServiceSchema"/>
          <ns2:code>601</ns2:code>
          <ns2:description>Identyfikator użytkownika 'user02' jest już zajęty.</ns2:description>
```

```
        </ns4:errorFault>
      </detail>
    </soap:Fault>
  </soap:Body>
</soap:Envelope>
```

3.1.2. Operacja `modifyIdentity`

Operacja służy do modyfikacji danych konta użytkownika.

Struktura danych żądania modyfikacji konta jest następująca:

Pole	Typ	Wymagane	Uwagi
userId	string(255)	tak	
email	string(255)	tak	Nowy adres email użytkownika
phoneNumber	string(40)	tak	Nowy numer telefonu użytkownika z funkcją odbierania SMS

Jeśli modyfikacja danych konta udała się, zwracany jest pusty element odpowiedzi. W przeciwnym razie zwracany jest komunikat typu fault, a w nim jeden z poniższych kodów błędów:

Kod	Znaczenie	Przyczyna
401	brak uprawnień	• system kliencki nie jest uprawniony do wywołania usługi
600	nieprawidłowy parametr wywołania	• walidacja nowych danych konta wykazała błędy
603	konto o podanym identyfikatorze nie istnieje	• nie ma konta użytkownika o podanym identyfikatorze
604	konto użytkownika zdezaktywowane	• konto użytkownika o podanym `userId` zostało zdezaktywowane
680	nieprawidłowy parametr requestTimestamp	• zbyt duża różnica między parametrem requestTimestamp a czasem systemowym serwera
500	błąd wewnętrzny	• wystąpił nieoczekiwany błąd w systemie DT
700	jednoczesna modyfikacja	• w innym wywołaniu nastąpiła zmiana danych konta i bieżąca operacja została odwołana

Przykładowe wywołanie metody wygląda następująco:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:idp="http://www.cpi.gov.pl/dt/IdpIdentityManagementServiceSchema">
  <soapenv:Header/>
  <soapenv:Body>
    <idp:reqModifyIdentity callId="1799884873392299849" requestTimestamp="2014-06-30T12:12:57.238+02:00">
      <idp:userId>user02</idp:userId>
      <idp:email>tomasz.nowak@adres.pl</idp:email>
      <idp:phoneNumber>+48600654321</idp:phoneNumber>
    </idp:reqModifyIdentity>
  </soapenv:Body>
</soapenv:Envelope>
```

Jeśli powyższe żądanie jest prawidłowe to odpowiedź serwera wygląda następująco:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Header/>
  <soap:Body>
    <ns4:respModifyIdentity callId="1799884873392299849" responseTimestamp="2014-06-30T12:12:57.519+02:00"
xmlns:ns2="http://www.cpi.gov.pl/dt/CommonSchema"
xmlns:ns4="http://www.cpi.gov.pl/dt/IdpIdentityManagementServiceSchema"/>
  </soap:Body>
</soap:Envelope>
```

Odpowiedź serwera na powyższe żądanie w przypadku nieprawidłowego parametru wywołania jest następująca:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Header/>
  <soap:Body>
    <soap:Fault>
      <faultcode>soap:Server</faultcode>
      <faultstring>Użytkownik o identyfikatorze 'user02' nie jest zarejestrowany w systemie.</faultstring>
      <detail>
        <ns4:errorFault callId="1799884873392299849" responseTimestamp="2014-06-30T12:12:57.349+02:00"
xmlns:ns2="http://www.cpi.gov.pl/dt/CommonSchema"
xmlns:ns4="http://www.cpi.gov.pl/dt/IdpIdentityManagementServiceSchema"/>
          <ns2:code>603</ns2:code>
          <ns2:description> Użytkownik o identyfikatorze 'user02' nie jest zarejestrowany w systemie.</ns2:description>
        </ns4:errorFault>
      </detail>
    </soap:Fault>
  </soap:Body>
</soap:Envelope>
```

3.1.3. Operacja `isUserIdAvailable`

Operacja służy do sprawdzenia, czy identyfikator użytkownika jest zajęty.

Struktura danych żądania sprawdzenia zajętości identyfikatora jest następująca:

Pole	Typ	Wymagane	Uwagi
userId	string(255)	tak	

Jeśli identyfikator jest wolny, zwracana jest odpowiedź „true”. Jeśli identyfikator jest zajęty, zwracana jest odpowiedź „false”. Jeśli w trakcie obsługi żądania wystąpi błąd, zwracany jest komunikat typu fault, a w nim jeden z poniższych kodów błędów:

Kod	Znaczenie	Przyczyna
401	brak uprawnień	• system kliencki nie jest uprawniony do wywołania usługi
600	nieprawidłowy parametr wywołania	• walidacja podanego identyfikatora użytkownika wykazała błędy
680	nieprawidłowy parametr requestTimestamp	• zbyt duża różnica między parametrem requestTimestamp a czasem systemowym serwera
500	błąd wewnętrzny	• wystąpił nieoczekiwany błąd w systemie DT

Przykładowe wywołanie metody wygląda następująco:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:idp="http://www.cpi.gov.pl/dt/IdpIdentityManagementServiceSchema">
  <soapenv:Header/>
  <soapenv:Body>
    <idp:reqIsUserIdAvailable callId="1067150200325354720" requestTimestamp="2014-06-30T12:02:48.731+02:00">
      <idp:userId>user02</idp:userId>
    </idp:reqIsUserIdAvailable>
  </soapenv:Body>
</soapenv:Envelope>
```

Jeśli powyższe żądanie jest prawidłowe, to odpowiedź serwera wygląda następująco:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Header/>
  <soap:Body>
    <ns4:respIsUserIdAvailable callId="1067150200325354720" responseTimestamp="2014-06-30T12:02:48.948+02:00"
xmlns:ns2="http://www.cpi.gov.pl/dt/CommonSchema"
xmlns:ns4="http://www.cpi.gov.pl/dt/IdpIdentityManagementServiceSchema">
      <available>false</available>
    </ns4:respIsUserIdAvailable>
  </soap:Body>
</soap:Envelope>
```

3.2. Usługa `IdpIdentityInfo`

Usługa służy do uzyskiwania informacji o kontach zarejestrowanych w systemie DT. Możliwe jest uzyskiwanie danych konta oraz tłumaczenie identyfikatora asercji SAML na identyfikator użytkownika, dla którego ta asercja została wystawiona.

Usługa dostępna jest pod adresem https://pz.gov.pl/dt-services/idpIdentityInfoService .

Definicja usługi znajduje się w pliku idpIdentityInfoService.wsdl. Typy danych używane przez usługę zawarte są w plikach identityInfo.xsd i common.xsd.

3.2.1. Operacja `getUserInfo`

Operacja służy do uzyskania danych konta użytkownika. Żądanie składa się z następujących pól:

Pole	Typ	Wymagane	Uwagi
userId	string(255)	tak	Pole może zawierać cyfry, małe i duże litery łacińskie oraz znaki '-' i '_'. Pozostałe znaki nie są dopuszczalne.

W odpowiedzi serwer zwraca następujące informacje:

Pole	Typ	Uwagi
userId	string(255)	Powtórzona wartość z żądania
email	string(255)	Adres email użytkownika
phoneNumber	string(40)	Numer telefonu użytkownika z funkcją odbierania SMS

Jeśli podczas obsługi żądania wystąpił błąd, zwracany jest komunikat typu fault, a w nim jeden z poniższych kodów błędów:

Kod	Znaczenie	Przyczyna
401	brak uprawnień	• system kliencki nie jest uprawniony do wywołania usługi
600	nieprawidłowy parametr wywołania	• w żądaniu podano pusty identyfikator użytkownika
601	brak tożsamości o podanym identyfikatorze	• użytkownik o podanym `userId` nie jest zarejestrowany w systemie DT
602	konto użytkownika zdezaktywowane	• konto użytkownika o podanym `userId` zostało zdezaktywowane

Kod	Znaczenie	Przyczyna
680	nieprawidłowy parametr requestTimestamp	• zbyt duża różnica między parametrem requestTimestamp a czasem systemowym serwera
500	błąd wewnętrzny	• wystąpił nieoczekiwany błąd w systemie DT

Przykładowe wywołanie metody wygląda następująco:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:idp="http://www.cpi.gov.pl/dt/IdpIdentityInfoServiceSchema">
  <soapenv:Header/>
  <soapenv:Body>
    <idp:reqGetUserInfo callId="7863316176426946194" requestTimestamp="2014-06-30T12:15:13.974+02:00">
      <idp:userId>user01</idp:userId>
    </idp:reqGetUserInfo>
  </soapenv:Body>
</soapenv:Envelope>
```

Jeśli powyższe żądanie jest prawidłowe to odpowiedź serwera wygląda następująco:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Header/>
  <soap:Body>
    <respGetUserInfo callId="7863316176426946194" responseTimestamp="2014-06-30T12:15:14.726+02:00"
xmlns="http://www.cpi.gov.pl/dt/IdpIdentityInfoServiceSchema" xmlns:ns3="http://www.cpi.gov.pl/dt/CommonSchema">
      <userId>user01</userId>
      <email>tomasz.nowak@mail.com</email>
      <phoneNumber>+48600123456</phoneNumber>
    </respGetUserInfo>
  </soap:Body>
</soap:Envelope>
```

Odpowiedź serwera na powyższe żądanie w przypadku niezarejestrowanego identyfikatora użytkownika jest następująca:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Header/>
  <soap:Body>
    <soap:Fault>
      <faultcode>soap:Server</faultcode>
      <faultstring>Brak tożsamości o identyfikatorze użytkownika 'user0-'.</faultstring>
      <detail>
        <errorFault callId="7863316176426946194" responseTimestamp="2014-06-30T12:15:14.437+02:00"
xmlns="http://www.cpi.gov.pl/dt/IdpIdentityInfoServiceSchema" xmlns:ns3="http://www.cpi.gov.pl/dt/CommonSchema">
          <ns3:code>601</ns3:code>
          <ns3:description>Brak tożsamości o identyfikatorze użytkownika 'user0-'.</ns3:description>
        </errorFault>
      </detail>
    </soap:Fault>
  </soap:Body>
```

```
</soap:Envelope>
```

3.2.2. Operacja `resolveUserId`

Operacja służy do przetłumaczenia identyfikatora asercji SAML na identyfikator użytkownika, dla którego ta asercja została wystawiona.

Żądanie składa się z następujących pól:

Pole	Typ	Wymagane	Uwagi
assertionId	string(255)	tak	Identyfikator asercji znajduje się w atrybucie „ID” elementu „Assertion” w asercji uzyskanej np. w odpowiedzi na żądanie artifactResolve wysłane do systemu DT.

W odpowiedzi serwer zwraca identyfikator użytkownika dla którego została wystawiona asercja o podanym identyfikatorze. Jeśli podczas obsługi żądania wystąpił błąd, zwracany jest komunikat typu fault, a w nim jeden z poniższych kodów błędów:

Kod	Znaczenie	Przyczyna
401	brak uprawnień	• system kliencki nie jest uprawniony do wywołania usługi
600	nieprawidłowy parametr wywołania	• w żądaniu podano pusty identyfikator asercji
602	konto użytkownika zdezaktywowane	• konto użytkownika dla którego wystawiono asercję zostało zdezaktywowane
603	nieprawidłowy identyfikator asercji	• asercja o podanym identyfikatorze nie jest zarejestrowana w systemie DT
604	nieprawidłowy identyfikator asercji	• asercja o podanym identyfikatorze jest nieważna
680	nieprawidłowy parametr requestTimestamp	• zbyt duża różnica między parametrem requestTimestamp a czasem systemowym serwera
500	błąd wewnętrzny	• wystąpił nieoczekiwany błąd w systemie DT

Przykładowe wywołanie metody wygląda następująco:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:idp="http://www.cpi.gov.pl/dt/IdpIdentityInfoServiceSchema">
```

```
  <soapenv:Header/>
  <soapenv:Body>
    <idp:reqResolveUserId callId="4486392602934445466" requestTimestamp="2014-06-30T12:32:52.120+02:00">
      <idp:assertionId>ID_e8c718c1-97fb-47a7-9c71-63ba31debf25</idp:assertionId>
    </idp:reqResolveUserId>
  </soapenv:Body>
</soapenv:Envelope>
```

Jeśli powyższe żądanie jest prawidłowe to odpowiedź serwera wygląda następująco:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Header/>
  <soap:Body>
    <respResolveUserId callId="4486392602934445466" responseTimestamp="2014-06-30T12:32:52.592+02:00"
xmlns="http://www.cpi.gov.pl/dt/IdpIdentityInfoServiceSchema" xmlns:ns3="http://www.cpi.gov.pl/dt/CommonSchema">
      <userId>user01</userId>
    </respResolveUserId>
  </soap:Body>
</soap:Envelope>
```

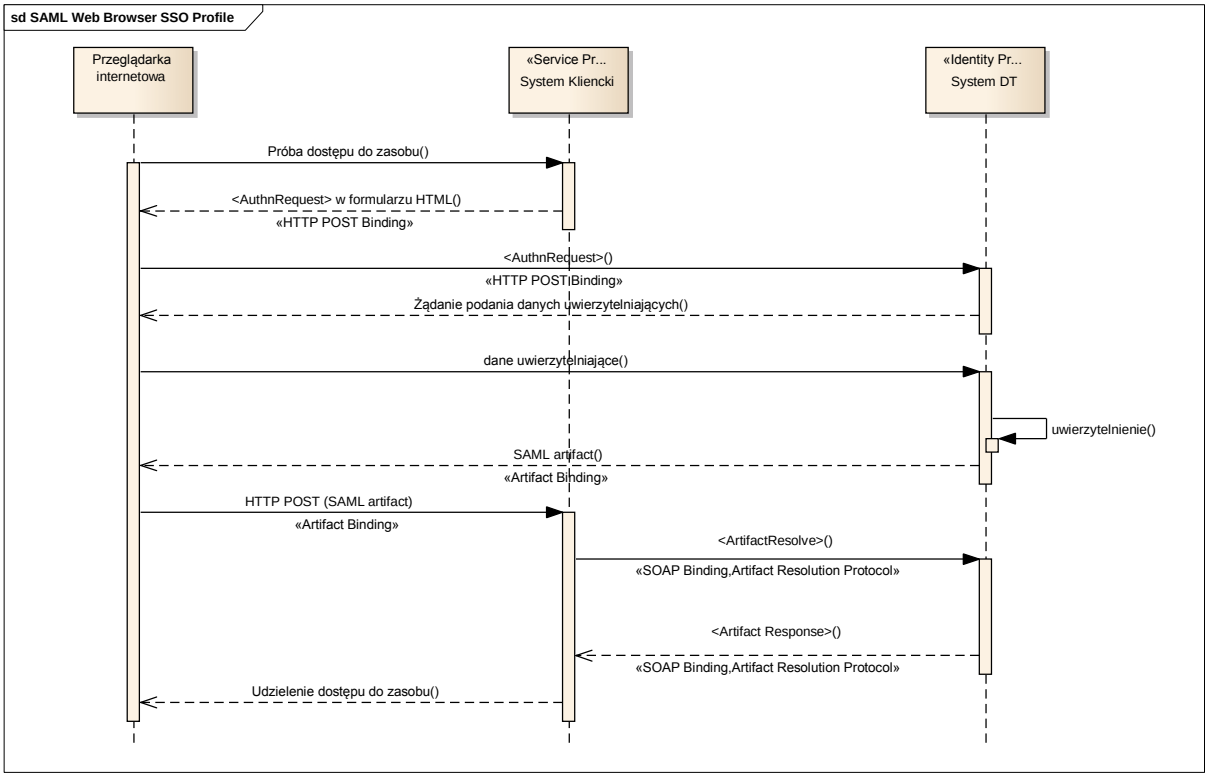
Odpowiedź serwera na powyższe żądanie w przypadku nieważnej asercji jest następująca:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Header/>
  <soap:Body>
    <soap:Fault>
      <faultcode>soap:Server</faultcode>
      <faultstring>Asercja o identyfikatorze 'ID_e8c718c1-97fb-47a7-9c71-63ba31debf25' jest nieważna.</faultstring>
      <detail>
        <errorFault callId="4486392602934445466" responseTimestamp="2014-06-30T12:32:52.573+02:00"
xmlns="http://www.cpi.gov.pl/dt/IdpIdentityInfoServiceSchema" xmlns:ns3="http://www.cpi.gov.pl/dt/CommonSchema">
          <ns3:code>603</ns3:code>
          <ns3:description>Asercja o identyfikatorze 'ID_e8c718c1-97fb-47a7-9c71-63ba31debf25' jest
nieważna.</ns3:description>
        </errorFault>
      </detail>
    </soap:Fault>
  </soap:Body>
</soap:Envelope>
```

4. Uwierzytelnienie przy pomocy SAML w systemie DT

System DT może służyć jako dostawca tożsamości w mechanizmie SSO. Funkcjonalność ta jest zapewniona w standardzie SAML 2.0. Więcej informacji o tym standardzie można znaleźć pod adresem https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security.

Proces uwierzytelniania z wykorzystaniem Dostawcy Tożsamości zgodny z SAML 2.0 przedstawiono na rysunku Rysunek 1.



Rysunek 1 Uwierzytelnianie w Systemie DT

W procesie uwierzytelniania biorą udział trzy systemy:

- przeglądarka internetowa uruchomiona na komputerze użytkownika
- system udostępniający usługi użytkownikowi (wykorzystując strony HTML) – Service Provider (System Kliencki)
- system udostępniający usługi uwierzytelnienia – Identity Provider (System DT).

Proces uwierzytelniania składa się z następujących kroków:

1.0. Przeglądarka internetowa użytkownika próbuje uzyskać dostęp do Systemu Klienckiego. Użytkownik nie był wcześniej uwierzytelniony w Systemie Klienckim.
1.1. System Kliencki po sprawdzeniu, że użytkownik nie jest uwierzytelniony, tworzy żądanie uwierzytelnienia SAML (<AuthnRequest>) i przekazuje odpowiednio przygotowany formularz HTML umożliwiający automatyczne wywołanie systemu Dostawca Tożsamości.

1.2. Przeglądarka internetowa przekazuje żądanie uwierzytelnienia do systemu Dostawca Tożsamości.
1.3. System DT po sprawdzeniu, że użytkownik nie jest uwierzytelniony w Systemie DT, przekazuje do przeglądarki stronę przeznaczoną do pobrania danych uwierzytelniających użytkownika.
1.4. Przeglądarka internetowa przekazuje wprowadzone przez użytkownika dane uwierzytelniające.
1.5. System DT przeprowadza uwierzytelnianie. Tworzona jest asercja SAML potwierdzająca tożsamość użytkownika.
1.6. System DT przekazuje artefakt SAML identyfikujący utworzoną asercję w sposób umożliwiający automatyczne wywołanie Systemu Klienckiego.
1.7. Przeglądarka internetowa przekazuje artefakt SAML do Systemu Klienckiego.
1.8. System Kliencki wywołuje usługę sieciową Systemu DT do pobierania wyników uwierzytelnienia, przekazując artefakt SAML otrzymany za pośrednictwem przeglądarki internetowej.
1.9. System DT zwraca asercję SAML zawierającą informację o uwierzytelnionym użytkowniku.
1.10. System Kliencki na podstawie asercji SAML przeprowadza autoryzację użytkownika i udziela dostępu do żądanego w kroku 1.0 zasobu.

Usługa Single-Sign-On Systemu DT (odbierająca żądania AuthnRequest) dostępna jest pod adresem https://pz.gov.pl/dt/SingleSignOnService.

Przykładowe żądanie AuthnRequest przekazywane w krokach 1.2 i 1.3 wygląda następująco:

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:AuthnRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
AssertionConsumerServiceURL="http://client.system.pl/index" Destination="http://www.cpi.gov.pl/dt/SingleSignOnService"
ID="ID_ac99bd70-2428-449a-92d0-47abdd84def9" IssueInstant="2014-06-30T08:03:21.789Z"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Version="2.0">
  <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://klient01.pl</saml2:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <ds:Reference URI="">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="ds saml2 saml2p
xenc"/>
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <ds:DigestValue>z5uDGv2yRzddVYx/lDh3LqweBVM=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>F6inIhf4dbX8RZgTWXoA3ZzmPLxccS6nu/guac(…)<ds:SignatureValue>
    <ds:KeyInfo>
      <ds:X509Data>
        <ds:X509Certificate>MIIE3TCCA8WgAwIBAgIIKKqJnqOvcj4w(…)</ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </ds:Signature>
  <saml2p:NameIDPolicy AllowCreate="false" Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"/>
</saml2p:AuthnRequest>
```

Przykładowy artefakt SAML przekazywany w krokach 1.6 i 1.7 zakodowany w Base64 wygląda następująco:

```
AAQAAcnceygFBb+m6oU0QfFClgJEIo9xVz7eKhr4hDP11aX2WDl2yxUS+7A=
```

Usługa ArtifactResolution Systemu DT dostępna jest pod adresem https://pz.gov.pl/dt-services/idpArtifactResolutionService.

Przykładowe żądanie ArtifactResolve przesyłane w kroku 1.8 wygląda następująco:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"/>
  <soap:Body>
    <saml2p:ArtifactResolve xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" ID="ID_736c1d00-c436-425a-ad01-7c854849479b" IssueInstant="2014-
06-30T08:28:10.982Z" Version="2.0">
      <saml2:Issuer>https://klient01.pl</saml2:Issuer>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
          <ds:Reference URI="">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
                <dsig-xpath:XPath xmlns:dsig-xpath="http://www.w3.org/2002/06/xmldsig-filter2"
Filter="intersect">here()/ancestor::saml2p:ArtifactResolve[1]</dsig-xpath:XPath>
              </ds:Transform>
              <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
                <dsig-xpath:XPath xmlns:dsig-xpath="http://www.w3.org/2002/06/xmldsig-filter2"
Filter="subtract">here()/ancestor::ds:Signature[1]</dsig-xpath:XPath>
              </ds:Transform>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="ds saml2
saml2p xenc"/>
              </ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>X10rg4RHo3IXu5QGNpPKUpyTybM=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>Pbuy1Dzjz72hQUwhAhqJLupB69AMQoKOa(…)</ds:SignatureValue>
        <ds:KeyInfo>
          <ds:X509Data>
            <ds:X509Certificate>MIIE3TCCA8WgAwIBAgIIKKqJnqOvcj4wDQYJKoZIhvcNA(…)<ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </ds:Signature>
      <saml2p:Artifact>AAQAAcnceygFBb+m6oU0QfFClgJEIo9xVz7eKhr4hDP11aX2WDl2yxUS+7A=</saml2p:Artifact>
    </saml2p:ArtifactResolve>
  </soap:Body>
</soap:Envelope>
```

Odpowiedź systemu DT na przykładowe żądanie ArtifactResolve przesyłana w kroku 1.9 wygląda następująco:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"/>
  <soap:Body>
    <saml2p:ArtifactResponse xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" ID="ID_3c7b202e-9a7c-4ce6-9782-a0e917b63a1a"
InResponseTo="ID_cb03cfdc-7225-4c58-ac6f-44856684b641" IssueInstant="2014-06-30T08:44:57.244Z" Version="2.0">
      <saml2:Issuer>https://pz.gov.pl/dt</saml2:Issuer>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
          <ds:Reference URI="">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
                <dsig-xpath:XPath xmlns:dsig-xpath="http://www.w3.org/2002/06/xmldsig-filter2"
Filter="intersect">here()/ancestor::saml2p:ArtifactResponse[1]</dsig-xpath:XPath>
              </ds:Transform>
              <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
                <dsig-xpath:XPath xmlns:dsig-xpath="http://www.w3.org/2002/06/xmldsig-filter2"
Filter="subtract">here()/ancestor::ds:Signature[1]</dsig-xpath:XPath>
              </ds:Transform>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="ds saml2
saml2p xenc"/>
              </ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>dAArH6aoBZY7kQ3CiWqBnCcHOwQ=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>PY8QjBi3Rtz48Mha05xOHtZvtvz0EgJdnT2ZqOmSvjI5Xbzx9aR(...)<ds:SignatureValue>
        <ds:KeyInfo>
          <ds:X509Data>
            <ds:X509Certificate>MIIE3TCCA8WgAwIBAgIIKKqJnqOvcj4wDQYJKoZIhvcNAQEFBQ(...)<ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </ds:Signature>
      <saml2p:Status>
        <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
      </saml2p:Status>
      <saml2p:Response ID="ID_0ad409da-903e-4f1a-b018-c021c60956c0" InResponseTo="ID_bdb7ebc7-7b5c-4b8e-a2d4-
e1cb153f349c" IssueInstant="2014-06-30T08:44:57.032Z" Version="2.0">
        <saml2:Issuer>https://pz.gov.pl/dt</saml2:Issuer>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <ds:Reference URI="">
              <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
                  <dsig-xpath:XPath xmlns:dsig-xpath="http://www.w3.org/2002/06/xmldsig-filter2"
Filter="intersect">here()/ancestor::saml2p:Response[1]</dsig-xpath:XPath>
                </ds:Transform>
```

```
                    <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
                      <dsig-xpath:XPath xmlns:dsig-xpath="http://www.w3.org/2002/06/xmldsig-filter2"
Filter="subtract">here()/ancestor::ds:Signature[1]</dsig-xpath:XPath>
                    </ds:Transform>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                      <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="ds saml2
saml2p xenc"/>
                    </ds:Transform>
                  </ds:Transforms>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                  <ds:DigestValue>mfVd+smkmZXuXHqe+3VMeRaaCT4=</ds:DigestValue>
                </ds:Reference>
              </ds:SignedInfo>
              <ds:SignatureValue>TQRZVLRCGBhLUvcqlZ0IQeWaeRAZ9YPEq5NbuhTj(…)<ds:SignatureValue>
              <ds:KeyInfo>
                <ds:X509Data>
                  <ds:X509Certificate>MIIE3TCCA8WgAwIBAgIIKKqJnqOvcj4wDQYJKoZI(…)<ds:X509Certificate>
                </ds:X509Data>
              </ds:KeyInfo>
            </ds:Signature>
            <saml2p:Status>
              <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
            </saml2p:Status>
            <saml2:Assertion ID="ID_9e61a687-67bc-4d9e-956d-50cbb3757937" IssueInstant="2014-06-30T08:44:57.032Z"
Version="2.0">
              <saml2:Issuer>https://pz.gov.pl/dt</saml2:Issuer>
              <saml2:Subject>
                <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">user01</saml2:NameID>
                <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                  <saml2:SubjectConfirmationData InResponseTo="ID_bdb7ebc7-7b5c-4b8e-a2d4-e1cb153f349c"
NotOnOrAfter="2014-06-30T08:45:27.032Z" Recipient="http://system.kliencki.pl/index"/>
                </saml2:SubjectConfirmation>
              </saml2:Subject>
              <saml2:Conditions NotBefore="2014-06-30T08:44:57.032Z" NotOnOrAfter="2014-06-30T08:45:27.032Z">
                <saml2:AudienceRestriction>
                  <saml2:Audience>system_kliencki_01</saml2:Audience>
                </saml2:AudienceRestriction>
              </saml2:Conditions>
              <saml2:AuthnStatement AuthnInstant="2014-06-30T08:44:57.032Z" SessionIndex="ID_9e61a687-67bc-4d9e-956d-
50cbb3757937">
                <saml2:AuthnContext>

<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClas
sRef>
                </saml2:AuthnContext>
              </saml2:AuthnStatement>
            </saml2:Assertion>
          </saml2p:Response>
        </saml2p:ArtifactResponse>
      </soap:Body>
    </soap:Envelope>
```

5. SAML w komunikacji z Zewnętrznymi Dostawcami Tożsamości

System DT może używać do uwierzytelnienia użytkownika Zewnętrznych Dostawców Tożsamości (ZDT). Dla takiej komunikacji używany jest standard SAML 2.0. Wymagana jest wcześniejsza rejestracja ZDT w systemie DT. Użytkownik w trakcie uwierzytelnienia podejmuje decyzję, czy chce się uwierzytelnić lokalnie, w systemie DT, czy w wybranym przez siebie ZDT.

Mechanizm uwierzytelnienia w ZDT jest również używany do autoryzacji podpisu profilem zaufanym. Uwierzytelnienie i autoryzacja podpisu profilem zaufanym w ZDT opisana jest w poniższych rozdziałach.

5.1. Uwierzytelnienie w ZDT

Komunikacja SAML 2.0 między systemem DT a ZDT przebiega analogicznie jak w rozdz. 4., przy czym System DT pełni tutaj rolę SP (Service Provider), a ZDT pełni rolę IdP (Identity Provider).

Proces uwierzytelniania składa się z następujących kroków:

1. System DT wyświetla nieuwierzytelnionemu użytkownikowi dostępne opcje uwierzytelnienia.
2. Użytkownik podejmuje decyzję, że chce się uwierzytelnić w Zewnętrznym Dostawcy Tożsamości. Przeglądarka internetowa użytkownika wysyła do Systemu DT żądanie z informacją, który ZDT wybrał użytkownik.
3. System DT tworzy żądanie uwierzytelnienia SAML (<AuthnRequest>) i przekazuje odpowiednio przygotowany formularz HTML umożliwiający automatyczne wywołanie wybranego przez użytkownika systemu ZDT.
4. Przeglądarka internetowa przekazuje żądanie uwierzytelnienia do ZDT.
5. ZDT przekazuje do przeglądarki stronę przeznaczoną do pobrania danych uwierzytelniających użytkownika.
6. Przeglądarka internetowa przekazuje wprowadzone przez użytkownika dane uwierzytelniające.
7. ZDT przeprowadza uwierzytelnianie. Tworzona jest asercja SAML potwierdzająca tożsamość użytkownika.
8. ZDT przekazuje artefakt SAML identyfikujący utworzoną asercję w sposób umożliwiający automatyczne wywołanie ZDT.
9. Przeglądarka internetowa przekazuje artefakt SAML do Systemu DT.
10. System DT wywołuje usługę sieciową ZDT do pobierania wyników uwierzytelnienia, przekazując artefakt SAML otrzymany za pośrednictwem przeglądarki internetowej.
11. ZDT zwraca asercję SAML zawierającą informację o uwierzytelnionym użytkowniku.
12. System DT na podstawie asercji SAML przeprowadza autoryzację użytkownika.

Powyższe kroki mogą zostać zagnieżdżone w procesie opisanym w rozdz. 4., zastępując kroki 3–4 w tamtym procesie. Taki połączony proces zapewni użytkownikowi uwierzytelnienie w Systemie Klienckim, poprzez przejście przez System DT do Zewnętrznego Dostawcy Tożsamości. Proces taki przedstawia poniższy rysunek.

Rysunek 2. Przekazywanie uwierzytelnienia między Systemem Klienckim, DT i ZDT (SAML Proxying)

Przykładowe żądanie AuthnRequest przekazywane w kroku 3. wygląda następująco:

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:AuthnRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
AssertionConsumerServiceURL="https://pz.gov.pl/dt/index" Destination="https://zewnetrzny.dt.pl/SingleSignOnService"
ID="ID_ac99bd70-2428-449a-92d0-47abdd84def9" IssueInstant="2014-06-30T08:03:21.789Z"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" ForceAuthn="true" Version="2.0">
  <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://pz.gov.pl/dt</saml2:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <ds:Reference URI="">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="ds saml2 saml2p
xenc"/>
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <ds:DigestValue>z5uDGv2yRzddVYx/lDh3LqweBVM=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>F6inIhf4dbX8RZgTWXoA3ZzmPLxccS6nu/guac(…)<ds:SignatureValue>
    <ds:KeyInfo>
      <ds:X509Data>
        <ds:X509Certificate>MIIE3TCCA8WgAwIBAgIIKKqJnqOvcj4w(…)</ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </ds:Signature>
  <saml2p:NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"/>
</saml2p:AuthnRequest>
```

Przykładowy artefakt SAML przekazywany w kroku 8. zakodowany w Base64 wygląda następująco:

```
AAQAAcnceygFBb+m6oU0QfFClgJEIo9xVz7eKhr4hDP11aX2WDl2yxUS+7A=
```

WSDL usługi Zewnętrznego Dostawcy Tożsamości, o której mowa w kroku 10, wygląda następująco:

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions name="ArtifactResolutionService" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/" xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl"
xmlns:tns="http://pz.gov.pl/zdt/ArtifactResolutionService" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" targetNamespace="http://pz.gov.pl/zdt/ArtifactResolutionService">
        <wsdl:types>
                <xsd:schema>
                        <xsd:import namespace="urn:oasis:names:tc:SAML:2.0:protocol"
schemaLocation="saml/v2/saml-schema-protocol-2.0.xsd"/>
                </xsd:schema>
        </wsdl:types>

        <wsdl:message name="artifactResolveMessage">
                <wsdl:part element="samlp:ArtifactResolve" name="artifactResolve"/>
        </wsdl:message>
        <wsdl:message name="artifactResponseMessage">
                <wsdl:part element="samlp:ArtifactResponse" name="artifactResponse"/>
        </wsdl:message>

        <wsdl:portType name="ArtifactResolutionServiceInterface">
                <wsdl:operation name="resolveArtifact">
                        <wsdl:input message="tns:artifactResolveMessage" name="artifactResolveMessage"/>
                        <wsdl:output message="tns:artifactResponseMessage" name="artifactResponseMessage"/>
                </wsdl:operation>
        </wsdl:portType>

        <wsdl:binding type="tns:ArtifactResolutionServiceInterface" name="ArtifactResolutionServiceSoapBinding">
                <wsaw:UsingAddressing wsdl:required="false"/>
                <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
                <wsdl:operation name="resolveArtifact">
                        <soap:operation soapAction="" style="document"/>
                        <wsdl:input name="artifactResolveMessage">
                                <soap:body use="literal"/>
                        </wsdl:input>
                        <wsdl:output name="artifactResponseMessage">
                                <soap:body use="literal"/>
                        </wsdl:output>
                </wsdl:operation>
        </wsdl:binding>

        <wsdl:service name="ArtifactResolutionService">
                <wsdl:port binding="tns:ArtifactResolutionServiceSoapBinding" name="ArtifactResolutionServicePort">
                        <soap:address location="FILL_ME"/>
                </wsdl:port>
        </wsdl:service>
</wsdl:definitions>
```

Przykładowe żądanie ArtifactResolve przesyłane w kroku 10. wygląda następująco:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"/>
  <soap:Body>
    <saml2p:ArtifactResolve xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
```

```
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" ID="ID_736c1d00-c436-425a-ad01-7c854849479b" IssueInstant="2014-06-30T08:28:10.982Z" Version="2.0">
        <saml2:Issuer>https://pz.gov.pl/dt</saml2:Issuer>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <ds:Reference URI="">
              <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
                  <dsig-xpath:XPath xmlns:dsig-xpath="http://www.w3.org/2002/06/xmldsig-filter2" Filter="intersect">here()/ancestor::saml2p:ArtifactResolve[1]</dsig-xpath:XPath>
                </ds:Transform>
                <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
                  <dsig-xpath:XPath xmlns:dsig-xpath="http://www.w3.org/2002/06/xmldsig-filter2" Filter="subtract">here()/ancestor::ds:Signature[1]</dsig-xpath:XPath>
                </ds:Transform>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                  <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="ds saml2 saml2p xenc"/>
                </ds:Transform>
              </ds:Transforms>
              <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
              <ds:DigestValue>X10rg4RHo3IXu5QGNpPKUpyTybM=</ds:DigestValue>
            </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue>Pbuy1Dzjz72hQUwhAhqJLupB69AMQoKOa(…)</ds:SignatureValue>
          <ds:KeyInfo>
            <ds:X509Data>
              <ds:X509Certificate>MIIE3TCCA8WgAwIBAgIIKKqJnqOvcj4wDQYJKoZIhvcNA(…)<ds:X509Certificate>
            </ds:X509Data>
          </ds:KeyInfo>
        </ds:Signature>
        <saml2p:Artifact>AAQAAcnceygFBb+m6oU0QfFClgJEIo9xVz7eKhr4hDP11aX2WDl2yxUS+7A=</saml2p:Artifact>
      </saml2p:ArtifactResolve>
    </soap:Body>
</soap:Envelope>
```

Odpowiedź ZDT na przykładowe żądanie ArtifactResolve przesyłana w kroku 11. wygląda następująco:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"/>
  <soap:Body>
    <saml2p:ArtifactResponse xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" ID="ID_3c7b202e-9a7c-4ce6-9782-a0e917b63a1a" InResponseTo="ID_cb03cfdc-7225-4c58-ac6f-44856684b641" IssueInstant="2014-06-30T08:44:57.244Z" Version="2.0">
      <saml2:Issuer>https://zdt01.pl</saml2:Issuer>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
          <ds:Reference URI="">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
```

```
                <dsig-xpath:XPath xmlns:dsig-xpath="http://www.w3.org/2002/06/xmldsig-filter2"
Filter="intersect">here()/ancestor::saml2p:ArtifactResponse[1]</dsig-xpath:XPath>
              </ds:Transform>
              <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
                <dsig-xpath:XPath xmlns:dsig-xpath="http://www.w3.org/2002/06/xmldsig-filter2"
Filter="subtract">here()/ancestor::ds:Signature[1]</dsig-xpath:XPath>
              </ds:Transform>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="ds saml2
saml2p xenc"/>
              </ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>dAArH6aoBZY7kQ3CiWqBnCcHOwQ=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>PY8QjBi3Rtz48Mha05xOHtZvtvz0EgJdnT2ZqOmSvjI5Xbzx9aR(...)<ds:SignatureValue>
        <ds:KeyInfo>
          <ds:X509Data>
            <ds:X509Certificate>MIIE3TCCA8WgAwIBAgIIKKqJnqOvcj4wDQYJKoZIhvcNAQEFBQ(...)<ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </ds:Signature>
      <saml2p:Status>
        <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
      </saml2p:Status>
      <saml2p:Response ID="ID_0ad409da-903e-4f1a-b018-c021c60956c0" InResponseTo="ID_bdb7ebc7-7b5c-4b8e-a2d4-
e1cb153f349c" IssueInstant="2014-06-30T08:44:57.032Z" Version="2.0">
        <saml2:Issuer>https://zdt01.pl</saml2:Issuer>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <ds:Reference URI="">
              <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
                  <dsig-xpath:XPath xmlns:dsig-xpath="http://www.w3.org/2002/06/xmldsig-filter2"
Filter="intersect">here()/ancestor::saml2p:Response[1]</dsig-xpath:XPath>
                </ds:Transform>
                <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
                  <dsig-xpath:XPath xmlns:dsig-xpath="http://www.w3.org/2002/06/xmldsig-filter2"
Filter="subtract">here()/ancestor::ds:Signature[1]</dsig-xpath:XPath>
                </ds:Transform>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                  <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="ds saml2
saml2p xenc"/>
                </ds:Transform>
              </ds:Transforms>
              <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
              <ds:DigestValue>mfVd+smkmZXuXHqe+3VMeRaaCT4=</ds:DigestValue>
            </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue>TQRZVLRCGBhLUvcqlZ0IQeWaeRAZ9YPEq5NbuhTj(...)<ds:SignatureValue>
          <ds:KeyInfo>
            <ds:X509Data>
              <ds:X509Certificate>MIIE3TCCA8WgAwIBAgIIKKqJnqOvcj4wDQYJKoZI(...)<ds:X509Certificate>
            </ds:X509Data>
```

```
            </ds:KeyInfo>
          </ds:Signature>
          <saml2p:Status>
            <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
          </saml2p:Status>
          <saml2:Assertion ID="ID_9e61a687-67bc-4d9e-956d-50cbb3757937" IssueInstant="2014-06-30T08:44:57.032Z"
Version="2.0">
            <saml2:Issuer>https://zdt01.pl</saml2:Issuer>
            <saml2:Subject>
              <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">user01</saml2:NameID>
              <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml2:SubjectConfirmationData InResponseTo="ID_bdb7ebc7-7b5c-4b8e-a2d4-e1cb153f349c"
NotOnOrAfter="2014-06-30T08:45:27.032Z" Recipient="https://pz.gov.pl/dt/index"/>
              </saml2:SubjectConfirmation>
            </saml2:Subject>
            <saml2:Conditions NotBefore="2014-06-30T08:44:57.032Z" NotOnOrAfter="2014-06-30T08:45:27.032Z">
              <saml2:AudienceRestriction>
                <saml2:Audience>dostawca_tożsamości</saml2:Audience>
              </saml2:AudienceRestriction>
            </saml2:Conditions>
            <saml2:AuthnStatement AuthnInstant="2014-06-30T08:44:57.032Z" SessionIndex="ID_9e61a687-67bc-4d9e-956d-
50cbb3757937">
              <saml2:AuthnContext>

<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClas
sRef>
              </saml2:AuthnContext>
            </saml2:AuthnStatement>
          </saml2:Assertion>
        </saml2p:Response>
      </saml2p:ArtifactResponse>
    </soap:Body>
</soap:Envelope>
```

5.2. Autoryzacja podpisu profilem zaufanym w ZDT

Zewnętrzny Dostawca Tożsamości może zostać użyty do autoryzacji podpisu profilem zaufanym, w zależności od preferencji posiadacza profilu zaufanego. Operacja taka realizowana jest z wykorzystaniem standardu SAML 2.0, według procesu przedstawionego w rozdz. 5.1. Uwierzytelnienie w ZDT, z następującymi zmianami:

1. System DT wysyła żądanie AuthnRequest różniący się od opisanego w rozdz. 5.1. w sposób następujący:

    a. dodany element <RequestedAuthnContext> z elementem <AuthnContextDeclRef> o wartości " urn:pl:profil_zaufany:const:SAML:2.0:ac:autoryzacja_podpisu",

    b. dodany element <Scoping> z atrybutem ProxyCount o wartości „0",

    c. dodany atrybut ForceAuthn o wartości „true",

    d. dodany atrybut ProviderName o wartości „Profil Zaufany: autoryzacja podpisu dokumentu XYZ", gdzie XYZ to nazwa dokumentu, którego podpis jest autoryzowany.

2. Zewnętrzny Dostawca Tożsamości wysyła odpowiedź Response różniącą się od opisanej w rozdz. 5.1. w sposób następujący:

    a. w asercji element <AuthnStatement> zawiera element <AuthnContextDeclRef> o wartości "urn:pl:profil_zaufany:const:SAML:2.0:ac:autoryzacja_podpisu".

Przykładowe żądanie AuthnRequest przekazywane w procesie autoryzacji podpisu wygląda następująco (różnice w porównaniu z żądaniem z rozdz. 5.1. zostały pogrubione):

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:AuthnRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
AssertionConsumerServiceURL="https://pz.gov.pl/dt/index" Destination="https://zewnetrzny.dt.pl/SingleSignOnService"
ID="ID_ac99bd70-2428-449a-92d0-47abdd84def9" IssueInstant="2014-06-30T08:03:21.789Z"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" ForceAuthn="true" ProviderName="Profil
Zaufany: autoryzacja podpisu dokumentu Wniosek o udostępnienie informacji publicznej" Version="2.0">
  <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://pz.gov.pl/dt</saml2:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <ds:Reference URI="">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="ds saml2 saml2p
xenc"/>
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <ds:DigestValue>z5uDGv2yRzddVYx/lDh3LqweBVM=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>F6inIhf4dbX8RZgTWXoA3ZzmPLxccS6nu/guac(...)<ds:SignatureValue>
    <ds:KeyInfo>
      <ds:X509Data>
        <ds:X509Certificate>MIIE3TCCA8WgAwIBAgIIKKqJnqOvcj4w(...)</ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </ds:Signature>
  <saml2p:NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"/>
  <saml2p:RequestedAuthnContext>

<saml2:AuthnContextDeclRef>urn:pl:profil_zaufany:const:SAML:2.0:ac:autoryzacja_podpisu</saml2:AuthnCo
ntextDeclRef>
  </saml2p:RequestedAuthnContext>
  <saml2p:Scoping ProxyCount="0"/>
</saml2p:AuthnRequest>
```

Przekazany artefakt i żądanie ArtifactResolve wygląda tak samo, jak w rozdz. 5.1.

Odpowiedź ZDT na żądanie ArtifactResolve wygląda następująco (różnice w porównaniu z żądaniem z rozdz. 5.1. zostały pogrubione):

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"/>
  <soap:Body>
```

```
    <saml2p:ArtifactResponse xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" ID="ID_3c7b202e-9a7c-4ce6-9782-a0e917b63a1a"
InResponseTo="ID_cb03cfdc-7225-4c58-ac6f-44856684b641" IssueInstant="2014-06-30T08:44:57.244Z" Version="2.0">
      <saml2:Issuer>https://zdt01.pl</saml2:Issuer>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
          <ds:Reference URI="">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
                <dsig-xpath:XPath xmlns:dsig-xpath="http://www.w3.org/2002/06/xmldsig-filter2"
Filter="intersect">here()/ancestor::saml2p:ArtifactResponse[1]</dsig-xpath:XPath>
              </ds:Transform>
              <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
                <dsig-xpath:XPath xmlns:dsig-xpath="http://www.w3.org/2002/06/xmldsig-filter2"
Filter="subtract">here()/ancestor::ds:Signature[1]</dsig-xpath:XPath>
              </ds:Transform>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="ds saml2
saml2p xenc"/>
              </ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>dAArH6aoBZY7kQ3CiWqBnCcHOwQ=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>PY8QjBi3Rtz48Mha05xOHtZvtvz0EgJdnT2ZqOmSvjI5Xbzx9aR(...)<ds:SignatureValue>
        <ds:KeyInfo>
          <ds:X509Data>
            <ds:X509Certificate>MIIE3TCCA8WgAwIBAgIIKKqJnqOvcj4wDQYJKoZIhvcNAQEFBQ(...)<ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </ds:Signature>
      <saml2p:Status>
        <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
      </saml2p:Status>
      <saml2p:Response ID="ID_0ad409da-903e-4f1a-b018-c021c60956c0" InResponseTo="ID_bdb7ebc7-7b5c-4b8e-a2d4-
e1cb153f349c" IssueInstant="2014-06-30T08:44:57.032Z" Version="2.0">
        <saml2:Issuer>https://zdt01.pl</saml2:Issuer>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <ds:Reference URI="">
              <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
                  <dsig-xpath:XPath xmlns:dsig-xpath="http://www.w3.org/2002/06/xmldsig-filter2"
Filter="intersect">here()/ancestor::saml2p:Response[1]</dsig-xpath:XPath>
                </ds:Transform>
                <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
                  <dsig-xpath:XPath xmlns:dsig-xpath="http://www.w3.org/2002/06/xmldsig-filter2"
Filter="subtract">here()/ancestor::ds:Signature[1]</dsig-xpath:XPath>
                </ds:Transform>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                  <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="ds saml2
saml2p xenc"/>
```

```
                </ds:Transform>
              </ds:Transforms>
              <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
              <ds:DigestValue>mfVd+smkmZXuXHqe+3VMeRaaCT4=</ds:DigestValue>
            </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue>TQRZVLRCGBhLUvcqlZ0IQeWaeRAZ9YPEq5NbuhTj(…)<ds:SignatureValue>
          <ds:KeyInfo>
            <ds:X509Data>
              <ds:X509Certificate>MIIE3TCCA8WgAwIBAgIIKKqJnqOvcj4wDQYJKoZI(…)<ds:X509Certificate>
            </ds:X509Data>
          </ds:KeyInfo>
        </ds:Signature>
        <saml2p:Status>
          <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
        </saml2p:Status>
        <saml2:Assertion ID="ID_9e61a687-67bc-4d9e-956d-50cbb3757937" IssueInstant="2014-06-30T08:44:57.032Z"
Version="2.0">
          <saml2:Issuer>https://zdt01.pl</saml2:Issuer>
          <saml2:Subject>
            <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">user01</saml2:NameID>
            <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
              <saml2:SubjectConfirmationData InResponseTo="ID_bdb7ebc7-7b5c-4b8e-a2d4-e1cb153f349c"
NotOnOrAfter="2014-06-30T08:45:27.032Z" Recipient="https://pz.gov.pl/dt/index"/>
            </saml2:SubjectConfirmation>
          </saml2:Subject>
          <saml2:Conditions NotBefore="2014-06-30T08:44:57.032Z" NotOnOrAfter="2014-06-30T08:45:27.032Z">
            <saml2:AudienceRestriction>
              <saml2:Audience>dostawca_tożsamości</saml2:Audience>
            </saml2:AudienceRestriction>
          </saml2:Conditions>
          <saml2:AuthnStatement AuthnInstant="2014-06-30T08:44:57.032Z" SessionIndex="ID_9e61a687-67bc-4d9e-956d-
50cbb3757937">
            <saml2:AuthnContext>

<saml2:AuthnContextDeclRef>urn:pl:profil_zaufany:const:SAML:2.0:ac:autoryzacja_podpisu</saml2:AuthnCo
ntextDeclRef>
            </saml2:AuthnContext>
          </saml2:AuthnStatement>
        </saml2:Assertion>
      </saml2p:Response>
    </saml2p:ArtifactResponse>
  </soap:Body>
</soap:Envelope>
```

5.3. Reguły przetwarzania

W komunikacji między Systemem DT a Zewnętrznym Dostawcą Tożsamości obowiązują następujące reguły:

1. Zewnętrzny Dostawca Tożsamości obsługuje przekazywanie żądania AuthnRequest za pomocą HTTP POST Binding.

2. Zewnętrzny Dostawca Tożsamości udostępnia usługę Artifact Resolution Service służącą do rozwiązywania artefaktów. Rozdział 5.1. zawiera definicję (WSDL) tej usługi.

3. System DT podpisuje zarówno żądania AuthnRequest jak i ArtifactResolve. Zewnętrzny Dostawca Tożsamości weryfikuje podpis tych żądań i nie obsługuje ich, jeśli żądanie jest niepodpisane, podpis jest nieprawidłowy lub niezaufany.

4. Zewnętrzny Dostawca Tożsamości podpisuje w odpowiedzi na żądanie ArtifactResolve zarówno element <saml2p:Response> jak i element <saml2p:ArtifactResponse>. System DT weryfikuje podpis tych elementów i nie uznaje odpowiedzi, jeśli jest ona niepodpisana, podpis jest nieprawidłowy lub niezaufany.

5. Zewnętrzny Dostawca Tożsamości przekazuje odpowiedź na żądanie AuthnRequest za pomocą bindingu HTTP Artifact Binding.

6. System DT akceptuje artefakt wyłącznie w kontrolce formularza XHTML przekazywanego w żądaniu HTTP POST.

7. Jeśli System DT umieści w żądaniu AuthnRequest element <AuthnContextDeclRef> o wartości "urn:pl:profil_zaufany:const:SAML:2.0:ac:autoryzacja_podpisu", to Zewnętrzny Dostawca Tożsamości:

    a. uwierzytelnia użytkownika na zasadach określonych w Rozporządzeniu w sprawie zasad i warunków potwierdzania, przedłużania ważności, unieważniania oraz wykorzystania profilu zaufanego elektronicznej platformy usług administracji publicznej,

    b. prezentuje użytkownikowi podczas uwierzytelnienia tekst zawarty w elemencie ProviderName tego żądania,

8. Jeśli System DT umieści w żądaniu AuthnRequest element <Scoping> z atrybutem ProxyCount o wartości „0", to Zewnętrzny Dostawca Tożsamości samodzielnie realizuje uwierzytelnienie użytkownika i nie wykorzystuje do tego celu innych dostawców tożsamości.

9. Jeśli System DT umieści w żądaniu AuthnRequest atrybut ForceAuthn o wartości „true", to Zewnętrzny Dostawca Tożsamości przeprowadza proces uwierzytelnienia bez uwzględnienia wcześniejszych uwierzytelnień lub sesji użytkownika.