



# **INSTRUKCJA DLA INTEGRATORA**

## **E-PODPIS**

---

## Spis treści

<b>1</b>	<b>Historia zmian .....</b>	<b>3</b>
<b>2</b>	<b>Cel i zakres dokumentu .....</b>	<b>4</b>
2.1	Słownik pojęć i skrótów .....	4
<b>3</b>	<b>Dostęp do usług sieciowych e-podpis .....</b>	<b>6</b>
3.1	WS-Security .....	7
3.2	Odpowiedź informująca o błędzie .....	9
<b>4</b>	<b>Definicja usługi sieciowej e-podpis TpSigning5 .....</b>	<b>12</b>
4.1	Diagram sekwencji usługi TpSigning5 .....	13
4.2	Operacja addDocumentToSigning .....	13
4.3	Operacja getSignedDocument .....	18
4.4	Operacja verifySignedDocument .....	22
<b>5</b>	<b>Struktura XML podpisów wykonanych z użyciem systemu e-podpis .....</b>	<b>32</b>
5.1	Podpis Zaufany .....	32
5.1.1	Opis pól elementu ClaimedRole specyficznego dla Podpisu Zaufanego .....	34
5.2	Podpis certyfikatem kwalifikowanym .....	35
5.3	Podpis certyfikatem podpisu osobistego .....	36
<b>6</b>	<b>Załączniki .....</b>	<b>39</b>

# 1 Historia zmian

Wersja	Data	Opis
<b>0.1</b>	08.05.2019	Opracowanie i utworzenie szablonu dokumentu.
<b>0.2</b>	10.05.2019	Uzupełnienie dokumentu.
<b>0.3</b>	13.05.2019	Utworzenie i dodanie do załączników przykładowych żądań, odpowiedzi serwera oraz podpisanego dokumentu.
<b>0.4</b>	14.05.2019	Weryfikacja i poprawki redaktorskie.
<b>0.5</b>	29.05.2019	Obsłużenie uwag Ministerstwa Cyfryzacji. Poprawki w dokumencie: ujednolicenie wykorzystywanego w przykładach środowiska.
<b>0.6</b>	10.06.2019	Uwzględnienie uwagi utrzymania dotyczącej informacji o nadawaniu uprawnień do usługi.
<b>0.7</b>	18.06.2019	Uwzględnienie uwag MC.
<b>0.8</b>	24.05.2021	Dodanie informacji o ograniczeniach w 4.2 Operacja addDocumentToSigning
<b>0.9</b>	21.05.2021	Dodanie informacji o podpisie osobistym, aktualizacja przykładowych komunikatów WS, dodanie załączników pismoOgolnePOSigned.xml oraz verifyPOSignedDocumentReturn.xml

## 2 Cel i zakres dokumentu

Niniejszy dokument opisuje usługi sieciowe systemu e-podpis (Podpis Zaufany) na poziomie technicznym. Dokument przeznaczony jest dla twórców systemów integrujących się z systemem e-podpis (Podpis Zaufany) na poziomie tych interfejsów.

Dokument zawiera przykładowe żądania i odpowiedzi serwera oraz podpisane Podpisem Zaufanym lub certyfikatem kwalifikowanym dokumenty, w których długie wartości elementów zakodowane w Base64 zostały skrócone dla przejrzystości.

Pełne przykładowe żądania i odpowiedzi serwera oraz podpisane Podpisem Zaufanym lub certyfikatem kwalifikowanym dokumenty zawierające nagłówki i podpisy znajdują się w załączonych do instrukcji plikach. Przykładowe komunikaty z załączników pochodzą ze środowiska integracyjnego (INT: <https://int.pz.gov.pl/ep-frontend/>, <https://int.pz.gov.pl/ep-services/tpSigning5>).

### 2.1 Słownik pojęć i skrótów

Pojęcia i skróty użyte w dokumencie zostały mają następujące znaczenie.

Pojęcie/skrót	Znaczenie
<b>System e-podpis</b>	System umożliwiający składanie Podpisu Zaufanego na podstawie danych uwalnianych Środkiem Identyfikacji Elektronicznej, składanie podpisu przy użyciu certyfikatu kwalifikowanego lub certyfikatu podpisu osobistego z e-dowodu.
<b>System PZ</b>	System Profil Zaufany
<b>System zewnętrzny</b>	System używający usług sieciowych systemu e-podpis
<b>Administrator systemu PZ</b>	Użytkownik systemu PZ posiadający uprawnienie do zarządzania słownikiem systemów zewnętrznych.
<b>Usługa sieciowa</b>	Metoda komunikacji elektronicznej pomiędzy systemami informatycznymi. W Systemie e-podpis (Podpis Zaufany) usługi sieciowe zaimplementowane są z wykorzystaniem SOAP/HTTP
<b>SOAP</b>	Simple Object Access Protocol – protokół wymiany informacji ustrukturalizowanej w usłudze sieciowej. ( <a href="http://www.w3.org/TR/soap">http://www.w3.org/TR/soap</a> )
<b>WSDL</b>	Web Services Description Language ( <a href="http://www.w3.org/TR/wsdl">http://www.w3.org/TR/wsdl</a> )
<b>Operacja usługi sieciowej</b>	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](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss))

### 3 Dostęp do usług sieciowych e-podpis

Przed przystąpieniem do integracji z usługą TpSigning5 należy spełnić kryteria formalne określone w dokumencie „Procedura integracji nowych systemów z Profilem Zaufanym.doc” umieszczonym na stronie BIP MC w artykule „Integracja systemów z Profilem Zaufanym”<sup>1</sup>

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

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

W celu zwiększenia bezpieczeństwa, system e-podpis przy konstruowaniu odpowiedzi nie ujawnia, który z powyższych warunków nie został spełniony przez system zewnętrzny. W każdym przypadku zwracana jest odpowiedź podobna do poniższej:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <soap:Fault>
      <faultcode>soap:Client</faultcode>
      <faultstring>Brak uprawnień do wywołania operacji.</faultstring>
      <detail>
        <ns3:WSSigningException xmlns:ns3="http://exception.ws.comarch.gov"
xmlns:ns2="http://signing.ws.comarch.gov">
          <code>401</code>
          <errMessage>Brak uprawnień do wywołania operacji.</errMessage>
        </ns3:WSSigningException>
      </detail>
    </soap:Fault>
  </soap:Body>
```

<sup>1</sup> <https://mc.bip.gov.pl/departament-utrzymania-i-rozwoju-systemow/integracja-systemow-z-profilem-zaufanym.html>

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

### 3.1 WS-Security

Każde żądanie wysyłane przez system zewnętrzny do systemu e-podpis 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 e-podpis 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:

```
<soapenv:Envelope xmlns:sig="http://signing.ws.comarch.gov"
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-CAA396546022CA79D3155747438304131">
          MIIEMTCCAxmG(...)
        </wsse:BinarySecurityToken>
      <ds:Signature Id="SIG-CAA396546022CA79D3155747438304135" 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="sig 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-CAA396546022CA79D3155747438304134">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                <ec:InclusiveNamespaces PrefixList="sig"
                  xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
              </ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256" />
            <ds:DigestValue>KAMD5nq2UG7MxiIJDQahMWFtT2HZkJB8hTWFAw2Ws=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
```

```

<ds:SignatureValue>ZqA/0XC0/Qh0Wif(...)</ds:SignatureValue>
<ds:KeyInfo Id="KI-CAA396546022CA79D3155747438304132">
  <wsse:SecurityTokenReference wsu:Id="STR-CAA396546022CA79D3155747438304133">
    <wsse:Reference URI="#X509-CAA396546022CA79D3155747438304131"
      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-CAA396546022CA79D3155747438304134"
  xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
  <sig:getSignedDocument>
    <id>https://int.pz.gov.pl/ep-frontend/#/doc/preview/rQqiwNKBU6M2n5EZ3vHfhjzI6Px91zCNgCMGpviG</id>
  </sig:getSignedDocument>
</soapenv:Body>
</soapenv:Envelope>

```

Odpowiedź serwera:

```

<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">
      <wsu:Timestamp wsu:Id="TS-40aead62-c0a7-4e97-8f60-8837967ff9cd">
        <wsu:Created>2019-05-10T11:13:04.967Z</wsu:Created>
        <wsu:Expires>2019-05-10T11:18:04.967Z</wsu:Expires>
      </wsu:Timestamp>
      <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-a11a941a-8090-4780-9ecd-9a3900f7c4e9">MIIEQjCCAYqgAwIB(...)
      </wsse:BinarySecurityToken>
      <ds:Signature Id="SIG-496a5c14-f470-4a64-8c99-69706fe67668" 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#">
            </ec:InclusiveNamespaces PrefixList="soap" 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="#TS-40aead62-c0a7-4e97-8f60-8837967ff9cd">
  <ds:Transforms>
    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
      <ec:InclusiveNamespaces PrefixList="wsse soap"
        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:DigestValue>qWYzuL0QdVrDFS6d0S0NsI/reY1NuDsC3Pv7W13HGjM=</ds:DigestValue>
</ds:Reference>
<ds:Reference URI="#_f1555f7f-b42d-4cec-a938-d674ee6a61db">
  <ds:Transforms>
    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
  </ds:Transforms>
  <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
  <ds:DigestValue>kkuCO6P3dh8RDTSTAZ6lkhZDSBaNoyjmeQoMW6IYdF0=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>Rm92i4SM(...)</ds:SignatureValue>
<ds:KeyInfo Id="KI-d991baf4-b1d6-41ed-940b-c2ea2e6e4bd1">
  <wsse:SecurityTokenReference wsu:Id="STR-30aba94a-4f31-4fdf-9270-1b6576661b9d">
    <wsse:Reference URI="#X509-a11a941a-8090-4780-9ecd-9a3900f7c4e9"
      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="_f1555f7f-b42d-4cec-a938-d674ee6a61db"
  xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
  <getSignedDocumentReturn xmlns:ns2="http://signing.ws.comarch.gov" xmlns:ns3="http://exception.ws.comarch.gov">
    PD94bWwgdmVyc2(...)
  </getSignedDocumentReturn>
</soap:Body>
</soap:Envelope>

```

## 3.2 Odpowiedź informująca o błędzie

W przypadku, gdy system e-podpis 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:Body>
    <soap:Fault>
      <faultcode>soap:Client</faultcode>
      <faultstring>Nieprawidłowa struktura parametru id: URL nie rozpoczyna się od oczekiwanego ciągu znaków
'http://192.168.126.128:13080/ep-frontend/#/doc/preview/'.</faultstring>
      <detail>
        <ns3:WSSigningException xmlns:ns3="http://exception.ws.comarch.gov"
xmlns:ns2="http://signing.ws.comarch.gov">
          <code>600</code>
          <errMessage>Nieprawidłowa struktura parametru id: URL nie rozpoczyna się od oczekiwanego ciągu znaków
'https://int.pz.gov.pl/ep-frontend/ep-frontend/#/doc/preview/'.</errMessage>
        </ns3:WSSigningException>
      </detail>
    </soap:Fault>
  </soap:Body>
</soap:Envelope>

```

Odpowiedź zawiera elementy wymienione w poniższej tabeli:

Element	Odbiorca	Przeznaczenie
<b>faultcode</b>	System zewnętrzny	<p>Element przyjmuje następujące wartości, zgodne ze specyfikacją SOAP:</p> <ul style="list-style-type: none"> <li>Client – oznacza że żądanie jest nieuprawnione, skonstruowane w sposób nieprawidłowy lub zawiera nieprawidłowe dane. Po otrzymaniu takiej odpowiedzi system zewnętrzny nie powinien ponawiać żądania w niezmienionej postaci, gdyż jego obsługa nigdy się nie powiedzie</li> <li>Server – oznacza że wystąpił błąd na serwerze uniemożliwiający obsługę żądania. Po otrzymaniu takiej odpowiedzi system zewnętrzny może (ale nie musi) ponowić żądanie w niezmienionej postaci natychmiast, lub po pewnym czasie, gdyż jest prawdopodobne, że jego obsługa w końcu się powiedzie</li> </ul>

Element	Odbiorca	Przeznaczenie
<b>faultstring</b>	Administrator systemu zewnętrznego	<p>Opis powodu nieobsłużenia żądania w postaci tekstu zrozumiałego dla człowieka; Jest przeznaczony dla administratora systemu zewnętrznego do diagnozowania błędów w komunikacji między systemami.</p> <p>Element nie powinien być używany do automatycznego podejmowania decyzji przez system zewnętrzny, gdyż komunikaty w nim zawarte mogą ulegać zmianie w wyniku aktualizacji oprogramowania systemu e-podpis</p>
<b>code</b>	System zewnętrzny	<p>Element przyjmuje wartości właściwe dla konkretnej operacji usługi sieciowej, wymienione w opisie tej usługi.</p> <p>Może być użyty do automatycznego podejmowania decyzji przez system zewnętrzny</p>

## 4 Definicja usługi sieciowej e-podpis

### **TpSigning5**

Schemat XML usługi sieciowej systemu e-podpis zawarty jest w załączonych do instrukcji plikach.

Usługa służy do przesyłania dokumentu do podpisu, pobrania dokumentu oraz weryfikacji podpisu pod dokumentem między systemem e-podpis, a systemami zewnętrznymi. Usługa zachowuje kompatybilność z poprzednimi wersjami usługi `TpSigning` systemu PZ z wyłączeniem dedykowanych dla systemu e-podpis wyszczególnionych opcjonalnych elementów żądań.

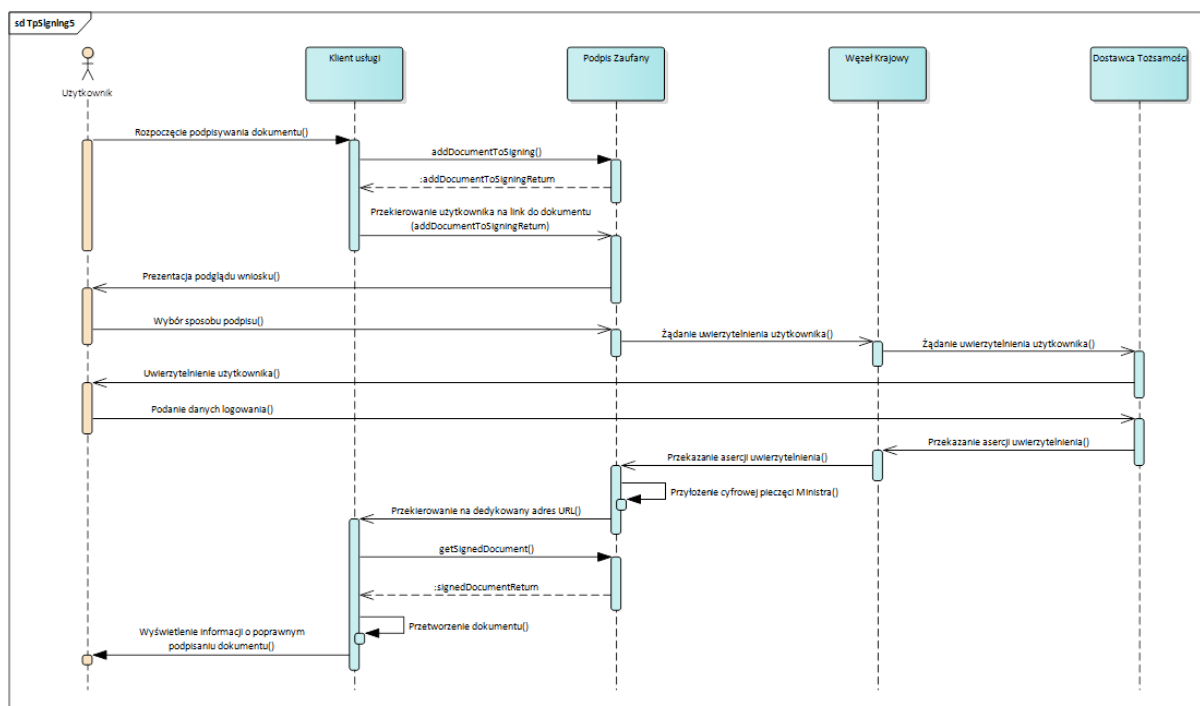
Usługa jest dostępna na środowisku integracyjnym pod adresem: <https://int.pz.gov.pl/ep-services/tpSigning5>

Definicja usługi znajduje się w pliku `tpSigning5.wsdl` załączonym do instrukcji.

Proces podpisu dokumentu z wykorzystaniem usługi `TpSigning5` przebiega w 3 krokach:

1. Klient usługi `TpSigning5` wgrywa przy pomocy operacji `addDocumentToSigning` plik XML przeznaczony do podpisu.
2. Klient usługi `TpSigning5` przekierowuje przeglądarkę użytkownika na URL otrzymany w odpowiedzi operacji `addDocumentToSigning`. Na wyświetlonej stronie użytkownik dokonuje podpisu dokumentu.
3. Klient usługi `TpSigning5` pobiera przy pomocy operacji `getSignedDocument` podpisany plik XML.

## 4.1 Diagram sekwencji usługi TpSigning5



## 4.2 Operacja addDocumentToSigning

Operacja służy do wgrania dokumentu przeznaczonego do podpisania danymi pochodzącymi z certyfikatu znajdującym się na e-Dowodzie. Żądanie składa się z następujących pól:

Pole	Typ	Wymagane	Uwagi
<b>doc</b>	string	tak	Dokument do podpisu w formacie XML, zakodowany w Base64; Maksymalna dopuszczalna wielkość dokumentu to 5 MB
<b>successURL</b>	string	tak	URL na który zostanie przekierowany użytkownik w przypadku gdy dokument zostanie poprawnie podpisany, nie dłuższy niż 1024 znaki, będący poprawnym adresem URL
<b>failureURL</b>	string	tak	URL na który zostanie przekierowany użytkownik w przypadku niepowodzenia podpisu dokumentu, nie dłuższy niż 1024 znaki, będący poprawnym adresem URL

<b>additionalInfo</b>	string	nie	Informacje dodatkowe w postaci tekstu prezentowanego użytkownikowi na stronie do podpisywania, nie dłuższego niż 1024 znaki
<b>cancelURL</b>	string	nie	URL na który zostanie przekierowany użytkownik w przypadku anulowania podpisu dokumentu, nie dłuższy niż 1024 znaki, będący poprawnym adresem URL. Element niekompatybilny z systemem PZ
<b>selectedSignatureMethod</b>	string	nie	Informacja nt. sposobu uwierzytelnienia użytkownika w systemie DU System e-podpis obsługuje trzy sposoby identyfikacji, za pośrednictwem: certyfikatu kwalifikowanego, Systemu Identyfikacji Elektronicznej oraz systemu Profil Zaufany. Dopuszczalne wartości definiowane są w pliku konfiguracyjnym ep-application.conf.xml Parametry: pzProviderID, sieProviderID, qualifiedCertificateProviderID Przykładowe wartości to : pz.gov.pl, sie.gov.pl, qualifiedCertificate Efektem przesłania parametru jest podpowiedzenie użytkownikowi kafelka z wyborem sposobu podpisu w graficznym interfejsie użytkownika systemu e-podpis.

Jeśli wgranie dokumentu udało się, zwracany jest URL na który należy przekierować użytkownika w celu dokonania podpisu.

**Do zwróconego adresu URL nie można dodawać własnych parametrów, a stronę z dokumentem do podpisu można uruchomić tylko raz. Ponowne uruchomienie linku do podpisu spowoduje błąd: Ta strona została już wyświetlona.**

W przeciwnym razie zwracany jest komunikat typu fault, a w nim jeden z poniższych kodów błędów:

Kod	Znaczenie	Przyczyna
401	brak uprawnień	<ul style="list-style-type: none"> <li>system zewnętrzny nie jest uprawniony do wywołania operacji</li> </ul>
600	nieprawidłowy parametr wywołania	<ul style="list-style-type: none"> <li>Dokument w polu <code>doc</code> zakodowany w Base64 nie jest prawidłowym dokumentem xml</li> <li>pole <code>successURL</code> nie jest prawidłowym URL-em, jest puste lub przekracza dopuszczalną długość</li> <li>pole <code>failureURL</code> nie jest prawidłowym URL-em, jest puste lub przekracza dopuszczalną długość</li> <li>pole <code>cancelURL</code> nie jest prawidłowym URL-em, jest puste lub przekracza dopuszczalną długość</li> <li>pole <code>additionalInfo</code> przekracza dopuszczalną długość</li> <li>dokument w polu <code>doc</code> nie jest prawidłowo zakodowany w Base64</li> <li>pole <code>doc</code> jest puste</li> </ul>
602	przesyłany dokument jest zbyt duży	<ul style="list-style-type: none"> <li>dokument w polu <code>doc</code> przekracza dopuszczalny rozmiar</li> </ul>
500	błąd wewnętrzny	<ul style="list-style-type: none"> <li>wystąpił nieoczekiwany błąd w aplikacji ePodpis</li> </ul>

Przykładowe żądanie operacji wygląda następująco:

```
<soapenv:Envelope xmlns:sig="http://signing.ws.comarch.gov"
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-EED14E91F3E18A8E7216242689479716">(…)</wsse:BinarySecurityToken><ds:Signature Id="SIG-EED14E91F3E18A8E72162426894797210"
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="sig 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-EED14E91F3E18A8E7216242689479729"><ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces PrefixList="sig" xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"></ds:Transform></ds:Transforms><ds:DigestMethod
```

```

Algorithm="http://www.w3.org/2001/04/xmldsig#sha256"/><ds:DigestValue>ZLKCS7cfAloKB4SC5pCI5tDtFDCFUEiIG/NhbWs5oi
Q=</ds:DigestValue></ds:Reference></ds:SignedInfo><ds:SignatureValue>u+XnuigrWAAfpICRYjFWuHyRhapi+6UDE(...)=<
/ds:SignatureValue><ds:KeyInfo Id="KI-EED14E91F3E18A8E7216242689479717"><wsse:SecurityTokenReference
wsu:Id="STR-EED14E91F3E18A8E7216242689479718"><wsse:Reference URI="#X509-
EED14E91F3E18A8E7216242689479716" 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-EED14E91F3E18A8E7216242689479729" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
  <sig:addDocumentToSigning>
    <doc>PGE+YTwvYT4=</doc>
    <successURL>https://int.login.gov.pl/saml-emulator/tpSigning5/success</successURL>
    <failureURL>https://int.login.gov.pl/saml-emulator/tpSigning5/failure</failureURL>
    <additionalInfo>Test na potrzeby aktualizacji instrukcji dla IntegratorÅłw</additionalInfo>
  </sig:addDocumentToSigning>
</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-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">
      <wsu:Timestamp wsu:Id="TS-b44e884a-aaae-46b9-994b-aec6753e1d3c">
        <wsu:Created>2021-06-21T09:49:08.390Z</wsu:Created>
        <wsu:Expires>2021-06-21T09:54:08.390Z</wsu:Expires>
      </wsu:Timestamp>
      <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-a47ac771-bc6b-4a9e-aa4d-
2e9a2ea450ae">MIIDXTCCAKWgAwIBAgIIQEJzzaHTx(...)=</wsse:BinarySecurityToken>
      <ds:Signature Id="SIG-97fd7f3c-432e-482e-8f18-54e0309782fd" 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/2001/04/xmldsig-more#rsa-sha256"/>
          <ds:Reference URI="#TS-b44e884a-aaae-46b9-994b-aec6753e1d3c">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                <ec:InclusiveNamespaces PrefixList="wsse soap" 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:DigestValue>1H3QfrQX5UwayLTesP7AZUVAqCewM4TGA41V0OoaLW0=</ds:DigestValue>
  </ds:Reference>
  <ds:Reference URI="#_24cf78c6-8232-4736-b1bf-3631334340d5">
    <ds:Transforms>
      <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
    <ds:DigestValue>MYQqe3TbBt9KeAJIbnvT23EAQPhTEcP3vobuf4UN2Bk=</ds:DigestValue>
  </ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>T4WnxKsB6fIdrPBN3q36nzB+/f/(...)=</ds:SignatureValue>
<ds:KeyInfo Id="KI-c8a4dafc-609c-45cf-bfa4-857ba65d7a5e">
  <wsse:SecurityTokenReference wsu:Id="STR-35295d80-8918-4c45-8a86-bffdba00ee6e">
    <wsse:Reference URI="#X509-a47ac771-bc6b-4a9e-aa4d-2e9a2ea450ae" 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="_24cf78c6-8232-4736-b1bf-3631334340d5" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
  <addDocumentToSigningReturn xmlns:ns2="http://signing.ws.comarch.gov"
xmlns:ns3="http://exception.ws.comarch.gov">https://int.pz.gov.pl/ep-
frontend/#/doc/preview/D0q0rJDDN1DrdYOVLsYn5v0sFXxcdbjV0MDAhVWd</addDocumentToSigningReturn>
</soap:Body>
</soap:Envelope></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:Body>
    <soap:Fault>
      <faultcode>soap:Client</faultcode>
      <faultstring>Wartość pola doc zawiera nieprawidłowe kodowanie Base64.</faultstring>
      <detail>
        <ns3:WSSigningException xmlns:ns3="http://exception.ws.comarch.gov">
          <code>600</code>
          <errMessage>Wartość pola doc zawiera nieprawidłowe kodowanie Base64.</errMessage>
        </ns3:WSSigningException>
      </detail>
    </soap:Fault>
  </soap:Body>
</soap:Envelope>

```

```

</detail>
</soap:Fault>
</soap:Body>
</soap:Envelope>

```

### 4.3 Operacja `getSignedDocument`

Operacja służy do pobrania podpisanego dokumentu. Żądanie składa się z następujących pól:

Pole	Typ	Wymagane	Uwagi
<b>id</b>	string	tak	Adres URL otrzymany w odpowiedzi na żądanie w operacji <code>addDocumentToSigning</code>

Jeśli pobranie dokumentu jest możliwe, zwracany jest podpisany dokument zakodowany w Base64. W przeciwnym razie zwracany jest komunikat typu fault, a w nim jeden z poniższych kodów błędów:

Kod	Znaczenie	Przyczyna
<b>401</b>	brak uprawnień	<ul style="list-style-type: none"> <li>system zewnętrzny nie jest uprawniony do wywołania operacji</li> </ul>
<b>600</b>	nieprawidłowy parametr wywołania	<ul style="list-style-type: none"> <li>pole <code>id</code> jest puste</li> <li>pole <code>id</code> ma nieprawidłową strukturę</li> </ul>
<b>601</b>	nie odnaleziono żądania podpisu	<ul style="list-style-type: none"> <li>nie odnaleziono danego żądania podpisu</li> </ul>
<b>603</b>	nie ma pliku w magazynie	<ul style="list-style-type: none"> <li>dokument o podanym identyfikatorze nie jest zarejestrowany lub został usunięty z systemu</li> </ul>
<b>604</b>	żądanie podpisu nie jest jeszcze podpisane	<ul style="list-style-type: none"> <li>żądanie podpisu dla danego dokumentu nie jest jeszcze podpisane</li> </ul>
<b>616</b>	niezgodna usługa	<ul style="list-style-type: none"> <li>żądanie podpisu zostało utworzone przez inną usługę</li> </ul>
<b>500</b>	błąd wewnętrzny	<ul style="list-style-type: none"> <li>wystąpił nieoczekiwany błąd w systemie e-podpis</li> </ul>

Przykładowe żądanie operacji wygląda następująco:

```
<soapenv:Envelope xmlns:sig="http://signing.ws.comarch.gov"
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="X509-321D6D5888050F47C7155748251449256">
          MIIEMTCCAxmGAWIBAgICAPwwDQYJKoZ(...)
        </wsse:BinarySecurityToken>
        <ds:Signature Id="SIG-321D6D5888050F47C7155748251449260" 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="sig 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-321D6D5888050F47C7155748251449259">
              <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                  <ec:InclusiveNamespaces PrefixList="sig"
                    xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
                </ds:Transform>
              </ds:Transforms>
              <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256" />
              <ds:DigestValue>Y29J38z2XVIoIK2A20sHr+MIKfjJ4xVpD7Oa+We5gqw=</ds:DigestValue>
            </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue>pZmlRCfRj/BamUgn(...)
        </ds:SignatureValue>
        <ds:KeyInfo Id="KI-321D6D5888050F47C7155748251449257">
          <wsse:SecurityTokenReference wsu:Id="STR-321D6D5888050F47C7155748251449258">
            <wsse:Reference URI="#X509-321D6D5888050F47C7155748251449256"
              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>
    </wsse:Security>
  </soapenv:Header>
  <soapenv:Body>
```

```

</soapenv:Header>
<soapenv:Body wsu:Id="id-321D6D5888050F47C7155748251449259"
  xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
  <sig:getSignedDocument>
    <id>https://int.pz.gov.pl/ep-frontend/#/doc/preview/G9qnA0X0I2rneoKDrl7TeV52HnAZpxB6vHC2ijJJ</id>
  </sig:getSignedDocument>
</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-ENV:Header xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <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"
      soap:mustUnderstand="1">
      <wsu:Timestamp wsu:Id="TS-403570f1-f82f-489b-960d-d2d77a173d66">
        <wsu:Created>2019-05-10T12:01:53.396Z</wsu:Created>
        <wsu:Expires>2019-05-10T12:06:53.396Z</wsu:Expires>
      </wsu:Timestamp>
      <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-b6372e3e-8d69-4625-b7dd-5692e10538d2">
        MIIIEQjCCAyqgAwIBAgICAPMwDQY(...)
      </wsse:BinarySecurityToken>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="SIG-ffa931ce-2403-4c79-ba03-1917d7a77d03">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="soap"/>
          </ds:CanonicalizationMethod>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
          <ds:Reference URI="#TS-403570f1-f82f-489b-960d-d2d77a173d66">
            <ds:Transforms>
              <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="wsse soap"/>
              </ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256"/>
            <ds:DigestValue>0fQ1jpnz9KC7rTajIIatZCtU1AxToI3GI2XUSN6xNPQ=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
      </ds:Signature>
    </wsse:Security>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <...>
  </SOAP-ENV:Body>
</soap:Envelope>

```

```

</ds:Reference>
<ds:Reference URI="#_37f89bcc-c926-43b0-9cfb-869d5a82feb5">
  <ds:Transforms>
    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
  </ds:Transforms>
  <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
  <ds:DigestValue>3lNwcXl4O1CutTupMGgx+4CautI/Sz4h9S1pCKq7s8g=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
  mQzLlLWHiFapMCIKzw+/7(...)
</ds:SignatureValue>
<ds:KeyInfo Id="KI-f8bde8ea-9f53-448a-ad96-a60fa7c64ee0">
  <wsse:SecurityTokenReference
    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"
    wsu:Id="STR-f366d518-2e7e-45e8-90ea-db9788d77983">
    <wsse:Reference URI="#X509-b6372e3e-8d69-4625-b7dd-5692e10538d2"
      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 xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
  wsu:Id="_37f89bcc-c926-43b0-9cfb-869d5a82feb5">
  <getSignedDocumentReturn>
    PD94bWwgdmVyc2lva(...)
  </getSignedDocumentReturn>
</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:Body>
    <soap:Fault>
      <faultcode>soap:Client</faultcode>
      <faultstring>Nieprawidłowa struktura parametru id: URL nie rozpoczyna się od oczekiwanego ciągu znaków
        'https://int.pz.gov.pl/ep-frontend/#/doc/preview/'.
    </soap:Fault>
  </soap:Body>
</soap:Envelope>

```

```

</faultstring>
<detail>
  <ns3:WSSigningException xmlns:ns3="http://exception.ws.comarch.gov">
    <code>600</code>
    <errMessage>Nieprawidłowa struktura parametru id: URL nie rozpoczyna się od oczekiwanego ciągu
      znaków 'https://int.pz.gov.pl/ep-frontend/#/doc/preview/'.
    </errMessage>
  </ns3:WSSigningException>
</detail>
</soap:Fault>
</soap:Body>
</soap:Envelope>

```

## 4.4 Operacja `verifySignedDocument`

Operacja służy do weryfikowania podpisu lub podpisów pod dokumentem XML. W odpowiedzi zwracana jest struktura XML zawierająca szczegółowe informacje na temat podpisu. Żądanie składa się z następujących pól:

Pole	Typ	Wymagane	Uwagi
<b>document</b>	string	tak	Podpisany dokument w formacie XML, zakodowany w Base64; Maksymalna dopuszczalna wielkość dokumentu to 5 MB

Jeśli weryfikacja podpisu lub podpisów się powiedzie, zwracana jest struktura XML składająca się z następujących elementów:

Element	Typ	Uwagi
<b>ValidDocumentSignature</b>	boolean	Informacja czy dokument jest poprawnie podpisany; Atrybut <i>znaczenie</i> opisuje zawartość tego pola i przyjmuje wartości „Prawidłowy” oraz „Nieprawidłowy”
<b>SignatureType</b>	string	Zawsze ciąg znaków „XAdES”
<b>GenerationTime</b>	date	Data i godzina wygenerowania tego dokumentu XML z informacjami na temat podpisu

Element	Typ	Uwagi
<b>StatusInfo</b>	element XML	Szczegółowe informacje na temat podpisu; Element ten jest tworzony dla każdego podpisu pod dokumentem. W przypadku braku podpisu tworzony jest jeden taki element zawierający informację o braku podpisu

Element `StatusInfo` składa się z następujących elementów:

Element	Typ	Uwagi
<b>ValidSignature</b>	boolean	Informacja czy podpis jest prawidłowy; Atrybut <code>znaczenie</code> opisuje zawartość tego pola i przyjmuje wartości „Prawidłowy” oraz „Nieprawidłowy”
<b>VerifyStatus</b>	int	Status weryfikacji podpisu; Atrybut <code>znaczenie</code> opisuje zawartość tego pola. Zwracane są następujące wartości: <ul style="list-style-type: none"> <li>• 0 – Zgodny z dokumentem</li> <li>• 1 – Niezgodny z dokumentem</li> <li>• 2 – Brak załączników</li> <li>• 3 – Niepoprawna struktura podpisu</li> <li>• 5 – Brak podpisu</li> </ul>
<b>VerifySignerCert</b>	int	Certyfikat użyty w podpisie; Atrybut <code>znaczenie</code> opisuje zawartość tego pola. Zwracane są następujące wartości: <ul style="list-style-type: none"> <li>• -1 – [Brak] – brak informacji lub podpisu</li> <li>• 0 – Ważny – certyfikat ważny</li> <li>• 1 – Nieważny – certyfikat nieważny</li> <li>• 2 – Unieważniony – certyfikat podpisujący unieważniony</li> <li>• 3 – Nieznany wystawca – nie znaleziono certyfikatu wystawcy w bazie</li> <li>• 4 – Brak OCSP lub CRL – brak odpowiedzi OCSP lub CRL</li> <li>• 5 – Błędny – ogólny błąd certyfikatu</li> </ul>

Element	Typ	Uwagi
<b>VerifySignerCertUsage</b>	int	<p>Sposób użycia certyfikatu wykorzystanego w podpisie; Atrybut <i>znaczenie</i> opisuje zawartość tego pola. Zwracane są następujące wartości:</p> <ul style="list-style-type: none"> <li>• 1 – kwalifikowany</li> <li>• 2 – niewykorzystany</li> <li>• 3 – logowanie</li> <li>• 4 – Zaufana odpowiedź OCSP</li> <li>• 5 – Generacja odpowiedzi OCSP na podstawie CRL</li> <li>• 6 – Przekierowanie na OCSP danego CA</li> <li>• 7 – UPO</li> <li>• 8 – EPO</li> <li>• 9 – TSA</li> </ul> <p>Element może wskazywać na więcej niż jedno zastosowanie certyfikatu. Podane w liście wartości traktowane są jako pozycje bitu wartości w reprezentacji binarnej. Bit na dziesiątej pozycji pełni rolę pomocniczą i oznacza, że przynajmniej jedna pozycja z listy jest prawdziwa. Przykładowo wartość elementu 924 – binarnie 1100011100 oznacza, że prawdziwe są pozycje logowanie, Zaufana odpowiedź OCSP, Generacja odpowiedzi OCSP na podstawie CRL, TSA</p>
<b>CommitmentType</b>	string	Wartość pola „Commitment type” z podpisu
<b>GracePeriod</b>	int	Wartość pola „Grace period” z podpisu
<b>ParentSignatureId</b>	string	Identyfikator podpisu nadrzędnego w przypadku kontrasygnaty
<b>SignatureCertIssuer</b>	string	Dane wystawcy certyfikatu
<b>SignatureCertSerial</b>	string	Numer seryjny certyfikatu użytego w podpisie
<b>SignatureCertSubject</b>	string	Dane posiadacza certyfikatu
<b>SignatureId</b>	string	Identyfikator podpisu
<b>SigningTime</b>	date	Data i godzina podpisania dokumentu
<b>UriID</b>	string	Wskaźniki do podpisanych elementów



Element	Typ	Uwagi
<b>SignatureTimeStamp</b>	element XML	Informacje o oznaczeniu podpisu czasem; W przypadku braku oznaczenia czasem atrybut <code>znaczenie</code> przyjmuje wartość „Brak oznaczenia czasem”. W przeciwnym razie element ten tworzony jest dla każdego oznaczenia czasem. Struktura elementu opisana jest w tabeli poniżej
<b>ArchiveTimeStamp</b>	element XML	Informacje o postaci archiwalnej podpisu; W przypadku braku oznaczenia czasem atrybut <code>znaczenie</code> przyjmuje wartość „Brak postaci archiwalnej”. W przeciwnym razie tworzony jest element o strukturze opisanej w tabeli poniżej
<b>EP</b>	element XML	Informacja o podpisie zaufanym; Atrybut <code>czy_obecny</code> informuje czy dokument jest podpisany podpisem zaufanym. Atrybut może przyjmować następujące wartości: <ul style="list-style-type: none"> <li>• <code>true</code> – dokument jest podpisany podpisem zaufanym; Element EP zawiera podpis zaufany</li> <li>• <code>false</code> – dokument nie jest podpisany podpisem zaufanym</li> </ul>
<b>ZP</b>	element XML	Informacja o podpisie profilem zaufanym; Atrybut <code>czy_obecny</code> informuje czy dokument jest podpisany profilem zaufanym. Atrybut może przyjmować następujące wartości: <ul style="list-style-type: none"> <li>• <code>true</code> – dokument jest podpisany profilem zaufanym; Element ZP zawiera podpis profilem zaufanym</li> <li>• <code>false</code> – dokument nie jest podpisany profilem zaufanym</li> </ul>

Elementy `SignatureTimeStamp` i `ArchiveTimeStamp` mają następującą strukturę:

Element	Typ	Uwagi
<b>TimeStampTime</b>	date	Czas oznaczenia podpisu
<b>VerifyStatus</b>	int	Status weryfikacji oznaczenia podpisu; Atrybut <code>znaczenie</code> opisuje zawartość tego pola. Zwracane są następujące wartości: <ul style="list-style-type: none"> <li>-1 – [brak]</li> <li>0 – Brak znacznika</li> <li>1 – Znacznik prawidłowy</li> <li>2 – Znacznik nieprawidłowy</li> <li>3 – Nieważny certyfikat OCSP</li> <li>4 – Niezaufany certyfikat OCSP</li> <li>5 – Nieważny certyfikat TSA</li> <li>6 – Niezaufany certyfikat TSA</li> </ul>

Jeśli weryfikacja podpisu lub podpisów się nie powiedzie, zwracany jest komunikat typu `fault`, z jednym z poniższych kodów błędów:

Kod	Znaczenie	Przyczyna
<b>401</b>	brak uprawnień	<ul style="list-style-type: none"> <li>system zewnętrzny nie jest uprawniony do wywołania operacji</li> </ul>
<b>600</b>	nieprawidłowy parametr wywołania	<ul style="list-style-type: none"> <li>pole <code>document</code> jest puste</li> <li>dokument nie jest w formacie XML</li> <li>wystąpił błąd w trakcie parsowania dokumentu, dla którego ma być przeprowadzona weryfikacja podpisu</li> <li>Wartość pola <code>document</code> zawiera nieprawidłowe kodowanie Base64.</li> </ul>
<b>602</b>	przesyłany dokument jest zbyt duży	<ul style="list-style-type: none"> <li>dokument w polu <code>document</code> przekracza dopuszczalny rozmiar</li> </ul>
<b>500</b>	błąd wewnętrzny	<ul style="list-style-type: none"> <li>wystąpił nieoczekiwany błąd w systemie e-podpis</li> </ul>

Przykładowe żądanie operacji :

```
<soapenv:Envelope xmlns:sig="http://signing.ws.comarch.gov"
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="X509-321D6D5888050F47C7155748320119571">
          MIIEMTCCAxmGAWIBAgICAPwwDQY(...)
        </wsse:BinarySecurityToken>
      <ds:Signature Id="SIG-321D6D5888050F47C7155748320119575" 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="sig 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-321D6D5888050F47C7155748320119574">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                <ec:InclusiveNamespaces PrefixList="sig"
                  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:DigestValue>Dj/K6xGVLOECNqQy9MmuLwqc90uGlue5X3CWE5I0EVY=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>LD9RkWHS9SbetJLun(...)
      </ds:SignatureValue>
      <ds:KeyInfo Id="KI-321D6D5888050F47C7155748320119572">
        <wsse:SecurityTokenReference wsu:Id="STR-321D6D5888050F47C7155748320119573">
          <wsse:Reference URI="#X509-321D6D5888050F47C7155748320119571"
            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:Envelope>
```

```

</soapenv:Header>
<soapenv:Body wsu:Id="id-321D6D5888050F47C7155748320119574"
  xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
  <sig:verifySignedDocument>
    <document>
      PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0i(...)
    </document>
  </sig:verifySignedDocument>
</soapenv:Body>
</soapenv:Envelope>

```

Przykładowa odpowiedź dla poprawnego żądania:

```

<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <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"
      soap:mustUnderstand="1">
      <wsu:Timestamp wsu:Id="TS-ca18755a-703e-4219-85d4-d93cc1b22e79">
        <wsu:Created>2019-05-13T08:17:30.548Z</wsu:Created>
        <wsu:Expires>2019-05-13T08:22:30.548Z</wsu:Expires>
      </wsu:Timestamp>
      <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="X509-645c9d40-71e0-41da-a78b-ae3e197e413f">
        MIIe3DCCA8SgAwIBAgIDIBe7MA0GCSqGSIb3DQEBCwUAMF(...)
      </wsse:BinarySecurityToken>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="SIG-2549a9dd-ee66-43a3-ada3-32e0c8779879">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="soap"/>
          </ds:CanonicalizationMethod>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
          <ds:Reference URI="#TS-ca18755a-703e-4219-85d4-d93cc1b22e79">
            <ds:Transforms>
              <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="wsse soap"/>
              </ds:Transform>
            </ds:Transforms>
          </ds:Reference>
        </ds:SignedInfo>
      </ds:Signature>
    </wsse:Security>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <ns1:VerifySignedDocument>
      <document>
        PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0i(...)
      </document>
    </ns1:VerifySignedDocument>
  </SOAP-ENV:Body>
</soap:Envelope>

```

```

</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<ds:DigestValue>6ReyvP4hItqWc90NwwlWjvg1gYR6SBzfx/hMFXKHQVY=</ds:DigestValue>
</ds:Reference>
<ds:Reference URI="#_dfb4ea07-f3b9-484b-8e9c-c1e6dbd2d3c1">
  <ds:Transforms>
    <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:Transform>
  </ds:Transforms>
  <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
  <ds:DigestValue>Nd3uj9aXi5rBQM/httuG2sjoid0fbqmkvvqPVEb9uOc=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
  FakTUJqr/iV9IXCzfEsX0FVryY(...)
</ds:SignatureValue>
<ds:KeyInfo Id="KI-5e78e317-8695-4e41-b3e0-8018cdb12ca5">
  <wsse:SecurityTokenReference
    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"
    wsu:Id="STR-4eb1ae6a-ffd2-4c29-af41-fe4bbf2b8c90">
    <wsse:Reference URI="#X509-645c9d40-71e0-41da-a78b-ae3e197e413f"
      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 xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
  wsu:Id="_dfb4ea07-f3b9-484b-8e9c-c1e6dbd2d3c1">
  <verifySignedDocumentReturn><?xml version="1.0" encoding="UTF-8" standalone="yes"?>
    <VerifyResult>
      <ValidDocumentSignature
        znaczenie="Prawidłowy">true
      </ValidDocumentSignature>
      <SignatureType>XAdES</SignatureType>
      <GenerationTime>2019-05-13T10:17:30.377+02:00</GenerationTime>
      <StatusInfo>
        <ValidSignature

```

```

        znaczenie="Prawidłowy">true
    </ValidSignature>
    <VerifyStatus znaczenie="Zgodny z dokumentem">0</VerifyStatus>
    <VerifySignerCert
        znaczenie="Ważny">0
    </VerifySignerCert>
    <VerifySignerCertUsage znaczenie="kwalifikowany"
        kwalifikowany="true">513
    </VerifySignerCertUsage>
    <CommitmentType></CommitmentType>
    <GracePeriod>1</GracePeriod>
    <ParentSignatureId></ParentSignatureId>
    <SignatureCertIssuer
        C="PL" CN="CPI CA for epuap TEST2" OU="CPI CA for epuap TEST2" O="CPI">C=PL,O=CPI,OU=CPI CA
        for epuap
        TEST2,CN=CPI CA for epuap TEST2
    </SignatureCertIssuer>
    <SignatureCertSerial>356389232</SignatureCertSerial>
    <SignatureCertSubject
        ST="mazowieckie" C="PL" E="sebastian.nowakowski@coi.gov.pl" OU="SUA" CN="epodpis_sign_int"
        L="Warszawa"
        O="COI">
C=PL,ST=mazowieckie,L=Warszawa,O=COI,OU=SUA,CN=epodpis_sign_int,E=sebastian.nowakowski@coi.gov.pl
    </SignatureCertSubject>
    <SignatureId>Signature-268256e6-1fc0-4845-ab48-2e8fbf030ac8</SignatureId>
    <SigningTime>2019-05-13T10:17:29.978+02:00</SigningTime>
    <UriID
        lp="1"></UriID>
    <UriID lp="2">#SignedProps-268256e6-1fc0-4845-ab48-2e8fbf030ac8</UriID>
    <SignatureTimeStamp
        znaczenie="Brak oznaczenia czasem"/>
    <ArchiveTimeStamp znaczenie="Brak postaci archiwalnej"/>
    <ZP czy_obecny="false"/>
    <EP czy_obecny="true">
    <xades:ClaimedRole
        xmlns:xades="http://uri.etsi.org/01903/v1.3.2#">
    <pz:EPSignature
        xmlns:pz="http://crd.gov.pl/xml/schematy/podpis_zaufany/">
    <pz:NaturalPerson>
        <pz:CurrentFamilyName>Jaszewski</pz:CurrentFamilyName>
        <pz:FirstName>Mariusz</pz:FirstName>

```

```

        <pz:DateOfBirth>1955-01-28</pz:DateOfBirth>
        <pz:PersonalIdentifier>55012896459</pz:PersonalIdentifier>
    </pz:NaturalPerson>
    <pz:SignatureData>
        <pz:IdentityIssuer>int.login.gov.pl</pz:IdentityIssuer>
        <pz:IdentityIssueTimestamp>2019-05-13T10:17:29.985+02:00</pz:IdentityIssueTimestamp>
    </pz:SignatureData>
    </pz:EPSignature>
</xades:ClaimedRole>
</EP>
</StatusInfo>
</VerifyResult>
</verifySignedDocumentReturn>
</soap:Body>
</soap:Envelope>

```

Przykładowa odpowiedź dla nieprawidłowego żądania:

```

<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <soap:Fault>
      <faultcode>soap:Client</faultcode>
      <faultstring>Błąd w trakcie parsowania dokumentu, dla którego ma być przeprowadzona weryfikacja podpisu.
    </faultstring>
      <detail>
        <ns3:WSSigningException xmlns:ns3="http://exception.ws.comarch.gov">
          <code>600</code>
          <errMessage>Błąd w trakcie parsowania dokumentu, dla którego ma być przeprowadzona weryfikacja
            podpisu.
          </errMessage>
        </ns3:WSSigningException>
      </detail>
    </soap:Fault>
  </soap:Body>
</soap:Envelope>

```

## 5 Struktura XML podpisów wykonanych z użyciem systemu e-podpis

### 5.1 Podpis Zaufany

Schemat XML Podpisu Zaufanego wykonywanego za pośrednictwem systemu e-podpis zawarty jest w załączonych do instrukcji plikach.

Podpis Zaufany zachowuje kompatybilność z podpisem Profilem Zaufanym z wyłączeniem elementu „ClaimedRole” - zawierającym informacje o czasie lokalnym, systemie uwalniającym dane osobowe oraz osobie składającej podpis. Element przystosowano do specyficznych danych wykorzystywanych do składania Podpisu Zaufanego pochodzących z Systemu Identyfikacji Elektronicznej.

Przykładowy prosty dokument XML zawierający prawidłowy Podpis Zaufany:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<a>a
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signature-4884ee9a-b36a-4ee4-8c0b-2976b0eeb265">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
      <ds:Reference URI="">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
            <ds:XPath>not(ancestor-or-self::ds:Signature)</ds:XPath>
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
        <ds:DigestValue>mrkd4MdiaDrsmvTIO/OFk9PwqXvte8W9oZHKwfwZBcw=</ds:DigestValue>
      </ds:Reference>
      <ds:Reference Type="http://uri.etsi.org/01903#SignedProperties"
        URI="#SignedProps-4884ee9a-b36a-4ee4-8c0b-2976b0eeb265">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
        <ds:DigestValue>M5zOg95YzvyLDA6PIFm8wIoRMLVGbbK9Cbv0CD+0ixE=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue Id="SignatureValue-4884ee9a-b36a-4ee4-8c0b-2976b0eeb265">
```



```

e/bWRQVbIxcRJTCpAs12ehb(...)
</ds:SignatureValue>
<ds:KeyInfo>
  <ds:X509Data>
    <ds:X509Certificate>
      MIIDhTCCAm2gAwIBAg(...)
    </ds:X509Certificate>
  </ds:X509Data>
</ds:KeyInfo>
<ds:Object Id="QualifyingInfos-4884ee9a-b36a-4ee4-8c0b-2976b0eeb265">
  <xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.3.2#"
    Id="QualifyingProps-4884ee9a-b36a-4ee4-8c0b-2976b0eeb265"
    Target="#Signature-4884ee9a-b36a-4ee4-8c0b-2976b0eeb265">
    <xades:SignedProperties Id="SignedProps-4884ee9a-b36a-4ee4-8c0b-2976b0eeb265">
      <xades:SignedSignatureProperties>
        <xades:SigningTime>2019-05-10T12:32:39.887+02:00</xades:SigningTime>
        <xades:SigningCertificate>
          <xades:Cert>
            <xades:CertDigest>
              <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
              <ds:DigestValue>hsz2z8IYfByFc7/H4bw4DD1IIm8BaCZnXhZdbzrqQSs=</ds:DigestValue>
            </xades:CertDigest>
            <xades:IssuerSerial>
              <ds:X509IssuerName>CN=CPI CA for epuap TEST2,OU=CPI CA for epuap TEST2,O=CPI,C=PL
              </ds:X509IssuerName>
              <ds:X509SerialNumber>1042639510</ds:X509SerialNumber>
            </xades:IssuerSerial>
          </xades:Cert>
        </xades:SigningCertificate>
        <xades:SignaturePolicyIdentifier>
          <xades:SignaturePolicyImplied/>
        </xades:SignaturePolicyIdentifier>
        <xades:SignerRole>
          <xades:ClaimedRoles>
            <xades:ClaimedRole>
              <pz:EPSignature xmlns:pz="http://crd.gov.pl/xml/schematy/podpis_zaufany/">
                <pz:NaturalPerson>
                  <pz:CurrentFamilyName>Jaszewski</pz:CurrentFamilyName>
                  <pz:FirstName>Mariusz</pz:FirstName>
                  <pz:DateOfBirth>1955-01-28</pz:DateOfBirth>
                  <pz:PersonalIdentifier>55012896459</pz:PersonalIdentifier>
                </pz:NaturalPerson>

```

```

        <pz:SignatureData>
            <pz:IdentityIssuer>int.login.gov.pl</pz:IdentityIssuer>
            <pz:IdentityIssueTimestamp>2019-05-10T12:32:39.896+02:00
            </pz:IdentityIssueTimestamp>
        </pz:SignatureData>
    </pz:EPSignature>
</xades:ClaimedRole>
</xades:ClaimedRoles>
</xades:SignerRole>
</xades:SignedSignatureProperties>
</xades:SignedProperties>
</xades:QualifyingProperties>
</ds:Object>
</ds:Signature>
</a>

```

### 5.1.1 Opis pól elementu `ClaimedRole` specyficznego dla Podpisu Zaufanego

Pole	Opis
<b>EPSignature</b>	Sekcja zawierająca informacje o osobie fizycznej, która złożyła Podpis Zaufany pod dokumentem oraz sekcję z informacjami o złożonym Podpisie Zaufanym. Atrybut pola wskazuje adres schematu zgodnie z którym wykonany został Podpis Zaufany
<b>NaturalPerson</b>	Sekcja informacji o osobie fizycznej, która złożyła Podpis Zaufany pod dokumentem
<b>CurrentFamilyName</b>	Nazwisko osoby, która złożyła Podpis Zaufany pod dokumentem
<b>FirstName</b>	Imię osoby, która złożyła Podpis Zaufany pod dokumentem
<b>DateOfBirth</b>	Data urodzenia osoby, która złożyła Podpis Zaufany pod dokumentem
<b>PersonalIdentifier</b>	Numer identyfikacyjny osoby, która złożyła Podpis Zaufany pod dokumentem. W przypadku Polskiego Dostawcy Tożsamości PESEL.
<b>SignatureData</b>	Sekcja informacji o złożonym Podpisie Zaufanym
<b>IdentityIssuer</b>	Wystawca danych osobowych użytych w Podpisie Zaufanym
<b>IdentityIssueTimestamp</b>	Data i czas wykonania Podpisu Zaufanego

## 5.2 Podpis certyfikatem kwalifikowanym

Schemat XML podpisu certyfikatem kwalifikowanym wykonywanym za pośrednictwem systemu e-podpis zawarty jest w załączonych do instrukcji plikach.

Podpis certyfikatem kwalifikowanym z użyciem systemu e-podpis zachowuje kompatybilność z podpisem certyfikatem kwalifikowanym z użyciem systemu Profil Zaufany.

Przykładowy prosty dokument XML zawierający prawidłowy podpis certyfikatem kwalifikowanym:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<a>a
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signature-c14e47f0-37ae-467e-b929-2f947d532381">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
      <ds:Reference URI="">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
            <ds:XPath>not(ancestor-or-self::ds:Signature)</ds:XPath>
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
        <ds:DigestValue>mrkd4MdiaDrsmvTIO/OFk9PwqXvte8W9oZHKwfwZBcw=</ds:DigestValue>
      </ds:Reference>
      <ds:Reference Type="http://uri.etsi.org/01903#SignedProperties"
        URI="#SignedProps-c14e47f0-37ae-467e-b929-2f947d532381">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
        <ds:DigestValue>5plwHG1oFDCXObr708oY9RCBUeXzpP0aCp2jU5VdCuQ=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue Id="SignatureValue-c14e47f0-37ae-467e-b929-2f947d532381">
      vzY7JNuMG4VWsvt/1OMOlG(...)
    </ds:SignatureValue>
    <ds:KeyInfo>
      <ds:X509Data>
        <ds:X509Certificate>MIIGHTCCBAWgAwIBAgI(...)
        </ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
```

```

<ds:Object Id="QualifyingInfos-c14e47f0-37ae-467e-b929-2f947d532381">
  <xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.3.2#"
    Id="QualifyingProps-c14e47f0-37ae-467e-b929-2f947d532381"
    Target="#Signature-c14e47f0-37ae-467e-b929-2f947d532381">
    <xades:SignedProperties Id="SignedProps-c14e47f0-37ae-467e-b929-2f947d532381">
      <xades:SignedSignatureProperties>
        <xades:SigningTime>2019-05-29T11:22:49.174+02:00</xades:SigningTime>
        <xades:SigningCertificate>
          <xades:Cert>
            <xades:CertDigest>
              <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
              <ds:DigestValue>W7YVEEGtRLi72QlszcoJdMt9M+qLEkbnYIXGvplZIzs= </ds:DigestValue>
            </xades:CertDigest>
            <xades:IssuerSerial>
              <ds:X509IssuerName>2.5.4.97=#0c10564154504c2d35323631303239363134,CN=CenCert QTSP
                CA,O=Enigma Systemy Ochrony Informacji Sp. z o.o.,C=PL
              </ds:X509IssuerName>
              <ds:X509SerialNumber>352268059709829817</ds:X509SerialNumber>
            </xades:IssuerSerial>
          </xades:Cert>
        </xades:SigningCertificate>
        <xades:SignaturePolicyIdentifier>
          <xades:SignaturePolicyImplied/>
        </xades:SignaturePolicyIdentifier>
      </xades:SignedSignatureProperties>
    </xades:SignedProperties>
  </xades:QualifyingProperties>
</ds:Object>
</ds:Signature>
</a>

```

## 5.3 Podpis certyfikatem podpisu osobistego

Schemat XML podpisu certyfikatem osobistym wykonywanym za pośrednictwem systemu e-podpis zawarty jest w załączonych do instrukcji plikach.

Przykładowy prosty dokument XML zawierający prawidłowy podpis certyfikatem osobistym:

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<a>a
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="id-00d675b8592b966ed17a14e21c378d98">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

```

```

<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256"/>
<ds:Reference Id="ID-d314e1201b1503dbe64f59bd5018a969" URI="">
  <ds:Transforms>
    <ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
      <ds:XPath>not(ancestor-or-self::ds:Signature)</ds:XPath>
    </ds:Transform>
  </ds:Transforms>
  <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
  <ds:DigestValue>mrkd4MdiaDrsmvTIO/Ofk9PwqXvte8W9oZHKwfwZBcw=</ds:DigestValue>
</ds:Reference>
<ds:Reference Type="http://uri.etsi.org/01903#SignedProperties"
  URI="#xades-id-00d675b8592b966ed17a14e21c378d98">
  <ds:Transforms>
    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
  </ds:Transforms>
  <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
  <ds:DigestValue>ow+aod0ppAWs9bhj+arznUmfvBQSpnz+t1ogH7W21x0=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue Id="value-id-00d675b8592b966ed17a14e21c378d98">
  Iq5YusVhOazaLTB+YyBZqNq7vq(...)
</ds:SignatureValue>
<ds:KeyInfo>
  <ds:X509Data>
    <ds:X509Certificate>
      MIIDGjCCAp+gAwIBAgIQeVlgnWx6wgy2rc(...)
    </ds:X509Certificate>
  </ds:X509Data>
</ds:KeyInfo>
<ds:Object>
  <xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.3.2#"
    Target="#id-00d675b8592b966ed17a14e21c378d98">
    <xades:SignedProperties Id="xades-id-00d675b8592b966ed17a14e21c378d98">
      <xades:SignedSignatureProperties>
        <xades:SigningTime>2021-06-21T10:44:59Z</xades:SigningTime>
        <xades:SigningCertificate>
          <xades:Cert>
            <xades:CertDigest>
              <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
              <ds:DigestValue>PLO7+Jcma4/Yort4OvREJb3RABBrwkN1hTSQq05zMRU=</ds:DigestValue>
            </xades:CertDigest>
            <xades:IssuerSerial>

```

```
<ds:X509IssuerName>C=PL,O=MSWiA,OU=CPD,2.5.4.5=#13083230313930313330,CN=PL.ID
  Authorization CA
</ds:X509IssuerName>
<ds:X509SerialNumber>161300661494100671964481831383562473301</ds:X509SerialNumber>
</xades:IssuerSerial>
</xades:Cert>
</xades:SigningCertificate>
</xades:SignedSignatureProperties>
<xades:SignedDataObjectProperties>
  <xades:DataObjectFormat ObjectReference="#ID-d314e1201b1503dbe64f59bd5018a969">
    <xades:MimeType>text/xml</xades:MimeType>
  </xades:DataObjectFormat>
  <xades:CommitmentTypeIndication>
    <xades:CommitmentTypeId>
      <xades:Identifier>http://uri.etsi.org/01903/v1.2.2#ProofOfApproval</xades:Identifier>
    </xades:CommitmentTypeId>
    <xades:AllSignedDataObjects/>
  </xades:CommitmentTypeIndication>
</xades:SignedDataObjectProperties>
</xades:SignedProperties>
</xades:QualifyingProperties>
</ds:Object>
</ds:Signature>
</a>
```

## 6 Załączniki

1. tpSigning5.wsdl – schemat XML usługi sieciowej TpSignig5
2. wssec-policies.wsdl – schemat XML polityki WS Security
3. podpis\_ep.xsd – schemat XML Podpisu Zaufanego
4. xmldsig-core-schema.xsd – schemat XML podpisu certyfikatem kwalifikowanym
5. addDocumentToSigning.xml – żądanie przychodzące TpSigning5.addDocumentToSigning
6. addDocumentToSigningReturn.xml – odpowiedź TpSignig5.addDocumentToSigningReturn
7. getSignedDocument.xml – żądanie przychodzące TpSigning5.getSignedDocument
8. getSignedDocumentReturn.xml – odpowiedź TpSignig5.getSignedDocumentReturn
9. verifySignedDocument.xml – żądanie przychodzące TpSigning5.verifySignedDocument
10. verifySignedDocumentReturn.xml – odpowiedź TpSignig5.verifySignedDocumentReturn dla dokumentu z Podpisem Zaufanym
11. verifyCKSignedDocumentReturn.xml – odpowiedź TpSignig5.verifySignedDocumentReturn dla dokumentu podpisanego certyfikatem kwalifikowanym
12. pismoOgolneSigned.xml – przykładowy podpisany Podpisem Zaufanym dokument XML (Pismo ogólne do podmiotu publicznego - stary wzór – pochodzące z ePUAP)
13. pismoOgolneCKSigned.xml – przykładowy podpisany Certyfikatem Kwalifikowanym dokument XML (Pismo ogólne do podmiotu publicznego - stary wzór – pochodzące z ePUAP)
14. pismoOgolnePOSigned.xml – przykładowy podpisany Certyfikatem Osobistym dokument XML (Pismo ogólne do podmiotu publicznego - stary wzór – pochodzące z ePUAP)
15. verifyPOSignedDocumentReturn.xml – odpowiedź TpSignig5.verifySignedDocumentReturn dla dokumentu podpisanego certyfikatem osobistym