centralny ośrodek informatyki

gov.pl Serwis polskiego rządu

e-podpis

v.1.0

INSTRUKCJA DLA INTEGRATORA

E-PODPIS

Spis treści

1 Historia zmian

Wersja	Data	Opis
0.1	08.05.2019	Opracowanie i utworzenie szablonu dokumentu.
0.2	10.05.2019	Uzupełnienie dokumentu.
0.3	13.05.2019	Utworzenie i dodanie do załączników przykładowych żądań, odpowiedzi serwera oraz podpisanego dokumentu.
0.4	14.05.2019	Weryfikacja i poprawki redaktorskie.
0.5	29.05.2019	Obsłużenie uwag Ministerstwa Cyfryzacji. Poprawki w dokumencie: ujednolicenie wykorzystywanego w przykładach środowiska.
0.6	10.06.2019	Uwzględnienie uwagi utrzymania dotyczącej informacji o nadawaniu uprawnień do usługi.
0.7	18.06.2019	Uwzględnienie uwag MC.
1.0	07.08.2019	Aktualizacja numeracji

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
System e-podpis	System umożliwiający składanie Podpisu Zaufanego na podstawie danych uwalnianych Środkiem Identyfikacji Elektronicznej lub składanie podpisu przy użyciu certyfikatu kwalifikowanego
System PZ	System Profil Zaufany
System zewnętrzny	System używający usług sieciowych systemu e-podpis
Administrator systemu PZ	Użytkownik systemu PZ posiadający uprawnienie do zarządzania słownikiem systemów zewnętrznych.
Usługa sieciowa	Metoda komunikacji elektronicznej pomiędzy systemami informatycznymi. W Systemie e-podpis (Podpis Zaufany) 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)

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" [1]

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>
```

[1] 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/xmlenc#sha256"/>
                  <ds:DigestValue>KAMD5nq2UG7MxiJIJDQahMWFIgT2HZkJB8hTWFAw2Ws=</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-40aeed62-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#"/>
               </ds:CanonicalizationMethod>
               <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
```

```
            <ds:Reference URI="#TS-40aeed62-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
faultcode	System zewnętrzny	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 zewnętrzny 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 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

Element	Odbiorca	Przeznaczenie
faultstring	Administrator systemu zewnętrznego	Opis powodu nieobsłużenia żądania w postaci tekstu zrozumiałego dla człowieka; Jest przeznaczony dla administratora systemu zewnętrznego do diagnozowania błędów w komunikacji między systemami. 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
code	System zewnętrzny	Element przyjmuje wartości właściwe dla konkretnej operacji usługi sieciowej, wymienione w opisie tej usługi. Może być użyty do automatycznego podejmowania decyzji przez system zewnętrzny

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 usługą `TpSigning` systemu PZ z wyłączeniem dedykowanych dla systemu e-podpis wyszczególnionych opcjonalnych elementów żądań.

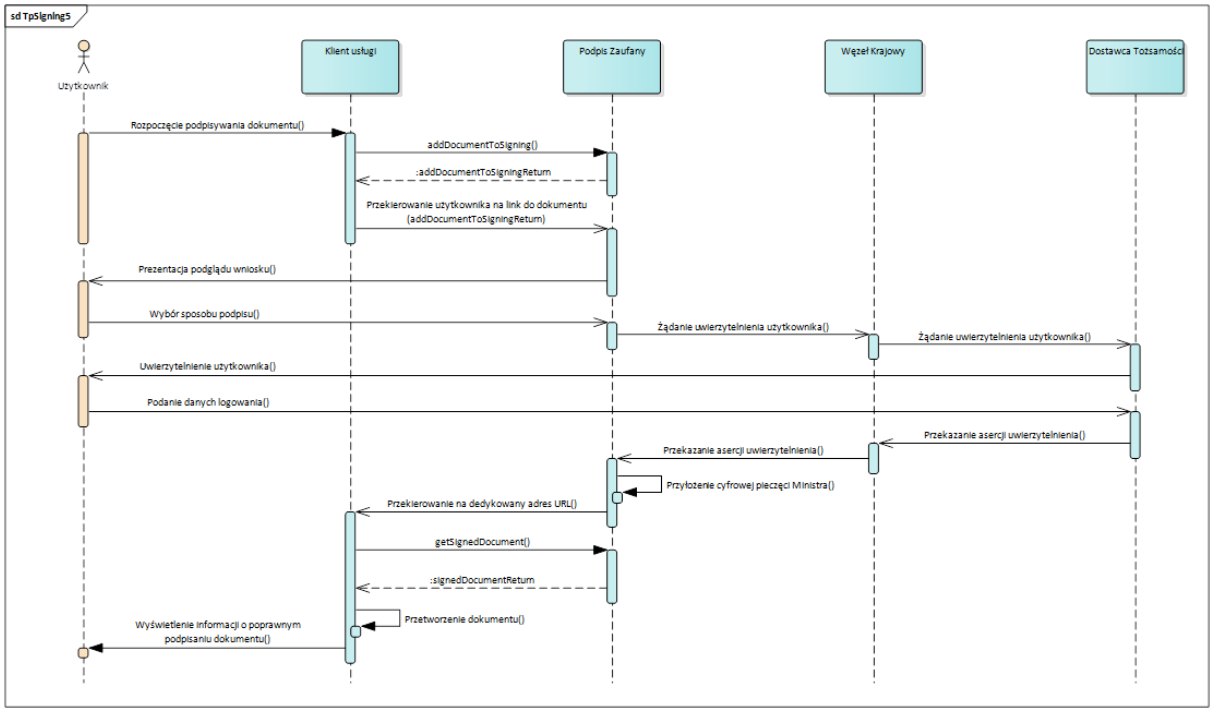
Usługa jest dostępna na środowisku integracyjnym pod adresem: https://int.pz.gov.pl/ep-services/tpSigning5

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

additionalInfo	string	nie	Informacje dodatkowe w postaci tekstu prezentowanego użytkownikowi na stronie do podpisywania, nie dłuższego niż 1024 znaki
cancelURL	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
selectedSignatureMethod	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 podpis. W przeciwnym razie zwracany jest komunikat typu fault, a w nim jeden z poniższych kodów błędów:

Kod	Znaczenie	Przyczyna
401	brak uprawnień	• system zewnętrzny nie jest uprawniony do wywołania operacji

600	nieprawidłowy parametr wywołania	• Dokument w polu `doc` zakodowany w Base64 nie jest prawidłowym dokumentem xml • pole `successURL` nie jest prawidłowym URL-em, jest puste lub przekracza dopuszczalną długość • pole `failureURL` nie jest prawidłowym URL-em, jest puste lub przekracza dopuszczalną długość • pole `cancelURL` nie jest prawidłowym URL-em, jest puste lub przekracza dopuszczalną długość • pole `additionalInfo` przekracza dopuszczalną długość • dokument w polu `doc` nie jest prawidłowo zakodowany w Base64 • pole `doc` jest puste
602	przesyłany dokument jest zbyt duży	• dokument w polu `doc` przekracza dopuszczalny rozmiar
500	błąd wewnętrzny	• wystąpił nieoczekiwany błąd w aplikacji ePodpis

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="X509-321D6D5888050F47C7155748178497341">
            MIIEMTCCAxmg(...)
         </wsse:BinarySecurityToken>
         <ds:Signature Id="SIG-321D6D5888050F47C7155748178497345" 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-321D6D5888050F47C7155748178497344">
```

```
                <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>rbf5K6qRnHUpZBBCw5J035H/3U+CBgCLZiKQJz1lyTE=</ds:DigestValue>
              </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>XLo1+481GOZJj1b7oKcJLD(...)
            </ds:SignatureValue>
            <ds:KeyInfo Id="KI-321D6D5888050F47C7155748178497342">
              <wsse:SecurityTokenReference wsu:Id="STR-321D6D5888050F47C7155748178497343">
                <wsse:Reference URI="#X509-321D6D5888050F47C7155748178497341"
                        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-321D6D5888050F47C7155748178497344"
            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</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 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-b9115921-5451-4b56-a76f-fc1d28632667">
                <wsu:Created>2019-05-10T11:49:43.906Z</wsu:Created>
```

```
            <wsu:Expires>2019-05-10T11:54:43.906Z</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="X509-43ff7150-746f-4c69-8a1e-078fb5f6528e">
          MIIEQjCCAyqgAwIBAgICAPMwDQY(...)
        </wsse:BinarySecurityToken>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="SIG-97833b35-0799-46d4-8363-
73c35955266c">
          <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-b9115921-5451-4b56-a76f-fc1d28632667">
              <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/xmlenc#sha256"/>
              <ds:DigestValue>y3zUEsNXsdbvErYfMfB/TIrrgJ/X2TP4lQFZMbmOLgw=</ds:DigestValue>
            </ds:Reference>
            <ds:Reference URI="#_1bef65e2-7162-4cbe-b5da-bc87fefa6ba3">
              <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>EQbnueRkRUnQnNvdQPJTR6zsIGnzIsNJ8jk/lXL0SQQ=</ds:DigestValue>
            </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue>
            lASOFp/JcwsEoa8g/CvGozA(...)
          </ds:SignatureValue>
          <ds:KeyInfo Id="KI-e8f9c26d-9a8a-4699-9cbc-65e96385a996">
            <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-71f24440-0596-4c57-b062-cb24de1879ab">
              <wsse:Reference URI="#X509-43ff7150-746f-4c69-8a1e-078fb5f6528e"
```

```
                    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="_1bef65e2-7162-4cbe-b5da-bc87fefa6ba3">
    <addDocumentToSigningReturn>https://int.pz.gov.pl/ep-
frontend/#/doc/preview/pCn9KEvGNmedEDUasjDDdVwp2s6lDUpG6zOzrLrV
    </addDocumentToSigningReturn>
</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>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>
```

4.3 Operacja getSignedDocument

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

Pole	Typ	Wymagane	Uwagi
id	string	tak	Adres URL otrzymany w odpowiedzi na żądanie w operacji `addDocumentToSigning`

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
401	brak uprawnień	• system zewnętrzny nie jest uprawniony do wywołania operacji
600	nieprawidłowy parametr wywołania	• pole `id` jest puste • pole `id` ma nieprawidłową strukturę
601	nie odnaleziono żądania podpisu	• nie odnaleziono danego żądania podpisu
603	nie ma pliku w magazynie	• dokument o podanym identyfikatorze nie jest zarejestrowany lub został usunięty z systemu
604	żądanie podpisu nie jest jeszcze podpisane	• żądanie podpisu dla danego dokumentu nie jest jeszcze podpisane
616	niezgodna usługa	• żądanie podpisu zostało utworzone przez inną usługę
500	błąd wewnętrzny	• wystąpił nieoczekiwany błąd w systemie e-podpis

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/xmlenc#sha256"/>
              <ds:DigestValue>Y29J38z2XVIoIK2A20sHr+MlKfjJ4xVpD7Oa+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>
    </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">
            MIIEQjCCAyqgAwIBAgICAPMwDQY(...)
         </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/xmlenc#sha256"/>
                  <ds:DigestValue>0fQ1jpnz9KC7rTajIIatZCtU1AxTol3GI2XUSN6xNPQ=</ds:DigestValue>
               </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>
      PD94bWwgdmVyc2lvb(...)
   </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/'.
         </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
document	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
ValidDocumentSignature	boolean	Informacja czy dokument jest poprawnie podpisany; Atrybut `znaczenie` opisuje zawartość tego pola i przyjmuje wartości „Prawidłowy” oraz „Nieprawidłowy”
SignatureType	string	Zawsze ciąg znaków „XAdES”
GenerationTime	date	Data i godzina wygenerowania tego dokumentu XML z informacjami na temat podpisu
StatusInfo	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
ValidSignature	boolean	Informacja czy podpis jest prawidłowy; Atrybut `znaczenie` opisuje zawartość tego pola i przyjmuje wartości „Prawidłowy” oraz „Nieprawidłowy”

Element	Typ	Uwagi
VerifyStatus	int	Status weryfikacji podpisu; Atrybut `znaczenie` opisuje zawartość tego pola. Zwracane są następujące wartości: • 0 – Zgodny z dokumentem • 1 – Niezgodny z dokumentem • 2 – Brak załączników • 3 – Niepoprawna struktura podpisu • 5 – Brak podpisu
VerifySignerCert	int	Certyfikat użyty w podpisie; Atrybut `znaczenie` opisuje zawartość tego pola. Zwracane są następujące wartości: • -1 – [Brak] – brak informacji lub podpisu • 0 – Ważny – certyfikat ważny • 1 – Nieważny – certyfikat nieważny • 2 – Unieważniony – certyfikat podpisujący unieważniony • 3 – Nieznany wystawca – nie znaleziono certyfikatu wystawcy w bazie • 4 – Brak OCSP lub CRL – brak odpowiedzi OCSP lub CRL • 5 – Błędny – ogólny błąd certyfikatu

Element	Typ	Uwagi
VerifySignerCertUsage	int	Sposób użycia certyfikatu wykorzystanego w podpisie; Atrybut `znaczenie` opisuje zawartość tego pola. Zwracane są następujące wartości: • 1 – kwalifikowany • 2 – niewykorzystany • 3 – logowanie • 4 – Zaufana odpowiedź OCSP • 5 – Generacja odpowiedzi OCSP na podstawie CRL • 6 – Przekierowanie na OCSP danego CA • 7 – UPO • 8 – EPO • 9 – TSA 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
CommitmentType	string	Wartość pola „Commitment type” z podpisu
GracePeriod	int	Wartość pola „Grace period” z podpisu
ParentSignatureId	string	Identyfikator podpisu nadrzędnego w przypadku kontrasygnaty
SignatureCertIssuer	string	Dane wystawcy certyfikatu
SignatureCertSerial	string	Numer seryjny certyfikatu użytego w podpisie
SignatureCertSubject	string	Dane posiadacza certyfikatu
SignatureId	string	Identyfikator podpisu
SigningTime	date	Data i godzina podpisania dokumentu
UriID	string	Wskaźniki do podpisanych elementów

Element	Typ	Uwagi
SignatureTimeStamp	element XML	Informacje o oznaczeniu podpisu czasem; W przypadku braku oznaczenia czasem atrybut `znaczenie` przyjmuje wartość „Brak oznaczenia czasem”. W przeciwnym razie element ten tworzony jest dla każdego oznaczenia czasem. Struktura elementu opisana jest w tabeli poniżej
ArchiveTimeStamp	element XML	Informacje o postaci archiwalnej podpisu; W przypadku braku oznaczenia czasem atrybut `znaczenie` przyjmuje wartość „Brak postaci archiwalnej”. W przeciwnym razie tworzony jest element o strukturze opisanej w tabeli poniżej
EP	element XML	Informacja o podpisie zaufanym; Atrybut `czy_obecny` informuje czy dokument jest podpisany podpisem zaufanym. Atrybut może przyjmować następujące wartości: • true – dokument jest podpisany podpisem zaufanym; Element EP zawiera podpis zaufany • false – dokument nie jest podpisany podpisem zaufanym
ZP	element XML	Informacja o podpisie profilem zaufanym; Atrybut `czy_obecny` informuje czy dokument jest podpisany profilem zaufanym. Atrybut może przyjmować następujące wartości: • true – dokument jest podpisany profilem zaufanym; Element ZP zawiera podpis profilem zaufanym • false – dokument nie jest podpisany profilem zaufanym

Elementy SignatureTimeStamp i ArchiveTimeStamp mają następującą strukturę:

Element	Typ	Uwagi
TimeStampTime	date	Czas oznaczenia podpisu
VerifyStatus	int	Status weryfikacji oznaczenia podpisu; Atrybut `znaczenie` opisuje zawartość tego pola. Zwracane są następujące wartości: • -1 – [brak] • 0 – Brak znacznika • 1 – Znacznik prawidłowy • 2 – Znacznik nieprawidłowy • 3 – Nieważny certyfikat OCSP • 4 – Niezaufany certyfikat OCSP • 5 – Nieważny certyfikat TSA • 6 – Niezaufany certyfikat TSA

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

Kod	Znaczenie	Przyczyna
401	brak uprawnień	• system zewnętrzny nie jest uprawniony do wywołania operacji
600	nieprawidłowy parametr wywołania	• pole `document` jest puste • dokument nie jest w formacie XML • wystąpił błąd w trakcie parsowania dokumentu, dla którego ma być przeprowadzona weryfikacja podpisu • Wartość pola `document` zawiera nieprawidłowe kodowanie Base64.
602	przesyłany dokument jest zbyt duży	• dokument w polu `document` przekracza dopuszczalny rozmiar
500	błąd wewnętrzny	• wystąpił nieoczekiwany błąd w systemie e-podpis

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/K6xGVLOECNqQy9MmuLwqc90uGlue5X3CWE5l0EVY=</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: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:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>6ReyvP4hItqWc90NwvlWjvg1gYR6SBzfx/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/iV9lXCzfEsX0FVryY(...)
          </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>mrkd4MdiaDrsmvTlO/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>M5zOg95YzvyLDA6PlFm8wIoRMLVGbbK9Cbv0CD+0ixE=</ds:DigestValue>
         </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue Id="SignatureValue-4884ee9a-b36a-4ee4-8c0b-2976b0eeb265">
```

```
      e/bWRQVbIxcrJTcTpAs12ehb(...)
   </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
EPSignature	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
NaturalPerson	Sekcja informacji o osobie fizycznej, która złożyła Podpis Zaufany pod dokumentem
CurrentFamilyName	Nazwisko osoby, która złożyła Podpis Zaufany pod dokumentem
FirstName	Imię osoby, która złożyła Podpis Zaufany pod dokumentem
DateOfBirth	Data urodzenia osoby, która złożyła Podpis Zaufany pod dokumentem
PersonalIdentifier	Numer identyfikacyjny osoby, która złożyła Podpis Zaufany pod dokumentem. W przypadku Polskiego Dostawcy Tożsamości PESEL.
SignatureData	Sekcja informacji o złożonym Podpisie Zaufanym
IdentityIssuer	Wystawca danych osobowych użytych w Podpisie Zaufanym
IdentityIssueTimestamp	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>mrkd4MdiaDrsmvTlO/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">
         vzY7JNuMG4VWisvt/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>
```

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)