centralny ośrodek informatyki

gov.pl Serwis polskiego rządu

e-podpis

v.1.0

INSTRUKCJA PRZEJŚCIA NA TPSIGNING5

W SYSTEMIE E-PODPIS

Z USŁUGI TPSIGNING SYSTEMU PZ

DLA INTEGRATORA E-PODPIS

Spis treści

1. Historia zmian

Wersja	Data	Opis
0.1	14.05.2019	Opracowanie i utworzenie szablonu dokumentu.
0.2	14.05.2019	Uzupełnienie dokumentu.
0.3	14.05.2019	Weryfikacja i poprawki redaktorskie.
0.4	29.05.2019	Obsłużenie uwag Ministerstwa Cyfryzacji.
0.5	18.06.2019	Uwzględnienie uwag MC.
1.0	07.08.2019	Aktualizacja numeracji

2. Cel i zakres dokumentu

Niniejszy dokument opisuje na poziomie technicznym przejście z usługi sieciowej TpSigning systemu PZ na usługę TpSigning5 systemu e-podpis (Podpis Zaufany). Dokument przeznaczony jest dla twórców systemów zintegrowanych z systemem PZ i chcących zintegrować się z systemem e-podpis (Podpis Zaufany) na poziomie tych interfejsów.

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

Przykładowe żądania i odpowiedzi serwera oraz podpisany Podpisem Zaufanym dokument zawierające nagłówki i podpisy znajdują się w plikach załączonych do instrukcji dla Integratora e-podpis. 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 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

3. Dostęp do usług sieciowych e-podpis

Zasady dostępu do usług sieciowych e-podpis opisane zostały w dokumencie instrukcji dla Integratora systemu e-podpis i są zgodne z zasadami dostępu do usług sieciowych systemu PZ opisanymi w dokumencie dla Integratora PZ (https://pz.gov.pl/Instrukcja_Integratora_PZ.pdf Rozdział 2. Dostęp do usług sieciowych PZ).

W przypadku chęci przełączenia systemu zewnętrznego zintegrowanego z usługą TpSigning systemu PZ w zakresie dostępu do usługi TpSignig5 systemu e-podpis wystarczy spełnić poniższy warunek:

- System zewnętrzny musi mieć przyznane przez administratora systemu PZ uprawnienie do wywoływania operacji usługi sieciowej w systemie e-podpis.

4. Definicja usługi sieciowej e-podpis TpSigning5

Szczegółowy opis usługi sieciowej e-podpis TpSigning5 znajduje się w instrukcji dla Integratora e-podpis. Usługa TpSigning5 w systemie e-podpis jest kompatybilna z usługą TpSigning w systemie PZ opisaną w instrukcji dla Integratora PZ (https://pz.gov.pl/Instrukcja_Integratora_PZ.pdf Rozdział 3.1 Usługa TpSigning) w zakresie operacji addDocumentToSigning, getSignedDocument oraz verifiSignedDocument.

Usługa TpSigning5 nie posiada operacji hasTrustedProfilePerson. Wszystkie różnice w kompatybilnych operacjach między TpSigning w systemie PZ, a Tpsigning5 w systemie e-podpis opisane zostały poniżej.

W celu przełączenia systemu zewnętrznego zintegrowanego z usługą TpSigning systemu PZ wystarczy zmienić adres do usługi WS. Usługa TpSigning5 systemu e-podpis jest dostępna na środowisku testowym pod adresem https://test.pz.gov.pl/ep-services/tpSigning5

4.1. Różnice w operacji addDocumentToSigning

Szczegółowy opis operacji addDocumentToSigning znajduje się w instrukcji dla Integratora e-podpis. Poniżej w tabeli znajdują się opcjonalne pola obsługiwane przez TpSigning5 w systemie e-podpis – nie obsługiwane przez TpSigning w systemie PZ.

Pole	Typ	Wymagane	Uwagi
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.
cancelURL	string	nie	URL na który zostanie przekierowany użytkownik w przypadku anulowania podpisu dokumentu, nie dłuższy niż 1024 znaki, będący poprawnym adresem URL

Przykładowe żądanie operacji uwzględniające wyżej opisane różnice:

```
<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://test.login.gov.pl/saml-emulator/tpSigning5/success</successURL>
      <failureURL>https://test.login.gov.pl/saml-emulator/tpSigning5/failure</failureURL>
      <cancelURL>https://test.login.gov.pl/saml-emulator/tpSigning5/cancel</cancelURL>
      <selectedSignatureMethod>pz.gov.pl</selectedSignatureMethod>
      <additionalInfo>Test</additionalInfo>
   </sig:addDocumentToSigning>
</soapenv:Body>
</soapenv:Envelope>
```

Poprawna odpowiedź serwera na żądanie oraz obsługa błędów opisana została w instrukcji dla Integratora e-podpis. Obsługa w systemie e-podpis jest kompatybilna z obsługą w systemie PZ opisaną w instrukcji dla Integratora PZ (https://pz.gov.pl/Instrukcja_Integratora_PZ.pdf Rozdział 3.1.1 Operacja `addDocumentToSigning`).

4.2. Różnice w operacji `verifySignedDocument`

Szczegółowy opis operacji `verifiSignedDocument` znajduje się w instrukcji dla Integratora e-podpis. Poniżej w tabeli znajduje się pole elementu `StatusInfo` zwracane w odpowiedzi przez TpSigning5 w systemie e-podpis – nie zwracane przez TpSigning w systemie PZ.

Pole	Typ	Opis
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

Przykładowa odpowiedź dla poprawnego żądania uwzględniająca wyżej opisane różnice:

```
<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>
```


Żądanie oraz obsługa błędów opisana została w instrukcji dla Integratora e-podpis. Obsługa w systemie e-podpis jest kompatybilna z obsługą w systemie PZ opisaną w instrukcji dla Integratora PZ (https://pz.gov.pl/Instrukcja_Integratora_PZ.pdf Rozdział 3.1.3 Operacja `verifySignedDocument`).

5. Różnice w podpisie

Szczegółowy opis struktury Podpisu Zaufanego, definicja XSD oraz różnica Podpisu Zaufanego w kontekście podpisu Profilem Zaufanym została opisana w instrukcji dla Integratora e-podpis.