centralny ośrodek informatyki

INSTRUKCJA DLA INTEGRATORA

Z SYSTEMEM WĘZEŁ PODPISU

Spis treści

Spis treści

1 Historia zmian

Wersja	Data	Opis
0.1	22.09.2023	Opracowanie i utworzenie szablonu dokumentu.
0.2	26.09.2023	Uzupełnienie dokumentu
0.3	05.10.2023	Utworzenie i dodanie do załączników przykładowych żądań, odpowiedzi serwera oraz podpisanego dokumentu.
0.4	04.12.2023	Dodanie plików XML dla certyfikatu kwalifikowanego oraz certyfikatu podpisu osobistego
0.5	21.02.2024	Uzupełnienie kodów błędów
0.6	04.06.2025	Aktualizacja dokumentu
1.0	22.08.2025	Aktualizacja dokumentu
1.1	28.11.2025	Uzupełnienie dokumentu o informacje związane z usługą signing REST.
1.2	23.02.2026	Uzupełnienie dokumentu w zakresie odwołania do aktualnej dokumentacji Swagger UI.

2 Cel i zakres dokumentu

Niniejszy dokument opisuje usługi sieciowe systemu **Węzeł Podpisu** na poziomie technicznym. Dokument przeznaczony jest dla twórców systemów integrujących się z systemem **Węzeł Podpisu** na poziomie tych interfejsów.

Dokument zawiera przykładowe żądania i odpowiedzi serwera wraz z dokumentami podpisanymi podpisem zaufanym, podpisem osobistym oraz kwalifikowanym, w których długie wartości elementów zakodowane w Base64 zostały skrócone dla zachowania przejrzystości dokumentu.

Dodatkowe materiały dla SOAP znajdują się w plikach załączonych do instrukcji. Przykładowe komunikaty z załączników pochodzą ze środowiska integracyjnego (INT: https://int.podpis.gov.pl:1443/ws/public/sgws/services/signingService).

Informacje dotyczące REST znajdują się w rozdziale Definicja usługi sieciowej REST signing REST.

2.1 Słownik pojęć i skrótów

Pojęcie/skrót	Znaczenie
System Węzeł Podpisu	System umożliwiający złożenie podpisu zaufanego, podpisu kwalifikowanego przy użyciu certyfikatu kwalifikowanego lub podpisu osobistego z wykorzystaniem certyfikatu z e-dowodu.
Profil Zaufany	Środek identyfikacji elektronicznej zawierający zestaw danych identyfikujących i opisujących osobę fizyczną, która posiada pełną albo ograniczoną zdolność do czynności prawnych, który został wydany w sposób, o którym mowa w art. 20c albo art. 20cb ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U.2005 nr 64, poz.565; t.j. Dz. U. 2021 poz. 670).
Podpis zaufany	Podpis elektroniczny, którego autentyczność i integralność są zapewniane przy użyciu pieczęci elektronicznej ministra właściwego do spraw informatyzacji, zawierający: 1. dane identyfikujące osobę, ustalone na podstawie środka identyfikacji elektronicznej wydanego w systemie, o którym mowa w art. 20aa pkt 1 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, obejmujące: • imię (imiona), • nazwisko, • numer PESEL, 2. identyfikator środka identyfikacji elektronicznej, przy użyciu którego został złożony, 3. czas jego złożenia.

Pojęcie/skrót	Znaczenie
Podpis osobisty	Jest to zaawansowany podpis elektroniczny. Prawdziwość danych posiadacza podpisu potwierdza certyfikat podpisu osobistego, zawierający imię (imiona), nazwisko, obywatelstwo oraz numer PESEL. Podpis osobisty ma taki sam skutek prawny jak podpis własnoręczny. Podpis osobisty może być wykorzystywany również w kontaktach z podmiotami innymi niż publiczne, ale tylko, jeżeli obie strony wyrażą na to zgodę. Podpis osobisty może służyć m.in. do złożenia podpisu dokumentów elektronicznych wysyłanych do urzędu.
Podpis kwalifikowany	Jest to zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego (Dz.U.UE.910/2014). Podpis kwalifikowany to powszechnie używana nazwa bezpiecznego podpisu elektronicznego weryfikowanego za pomocą ważnego kwalifikowanego certyfikatu. Z uwagi na bezpieczeństwo obrotu prawnego dokumenty przedkładane usługodawcy przez usługobiorcę za pośrednictwem środków komunikacji elektronicznej muszą być zabezpieczone przed niekontrolowaną modyfikacją, a więc muszą być elektronicznie podpisane. Podpis kwalifikowany jest autoryzowanym sposobem potwierdzenia tożsamości. Centra Certyfikacji wydają certyfikaty kwalifikowane służące do złożenia podpisu kwalifikowanego. Dokument w ten sposób podpisany jest prawnie wiążącym.
e-dowód	Dowód osobisty (dokument tożsamości) posiadający warstwę elektroniczną, umożliwiającą jego posiadaczowi uwierzytelnienie w usługach online za pomocą profilu osobistego oraz potwierdzenie obecności w określonym czasie i miejscu.
System zewnętrzny	System używający usług sieciowych systemu **Węzeł Podpisu.**
Administrator systemu PZ	Użytkownik systemu Profil Zaufany posiadający m.in. uprawnienie do zarządzania słownikiem systemów zewnętrznych.
Usługa sieciowa	Metoda komunikacji elektronicznej realizowana pomiędzy systemami informatycznymi. W Systemie Węzeł Podpisu usługi sieciowe zaimplementowane są z wykorzystaniem SOAP/HTTPS.
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).
REST	Representational State Transfer, to styl architektoniczny do tworzenia usług sieciowych, który umożliwia komunikację między różnymi systemami komputerowymi poprzez Internet. Jest to zestaw zasad i wytycznych dla tworzenia skalowalnych i wydajnych usług, które wykorzystują protokół HTTP i operacje na zasobach (np. pobieranie, dodawanie, aktualizacja, usuwanie danych).

Pojęcie/skrót	Znaczenie
JSON	JavaScript Object Notation, lekki format wymiany danych komputerowych. JSON jest formatem tekstowym, bazującym na podzbiorze języka JavaScript.
Operacja usługi sieciowej	Akcja SOAP w znaczeniu stosowanym w WSDL.
WS-Security	Web Services Security – rozszerzenie SOAP stosowane w celu zabezpieczenia usług sieciowych. (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss)
XAdES	Format podpisu elektronicznego, który służy do podpisywania dokumentów w formacie XML. Specyfikacja techniczna wskazana w Decyzji wykonawczej Komisji (UE) 2015/1506 z dnia 8 września 2015 r. ustanawiającej specyfikacje dotyczące formatów zaawansowanych podpisów elektronicznych oraz zaawansowanych pieczęci elektronicznych, które mają być uznane przez podmioty sektora publicznego to ETSI TS 103171 v.2.1.1. W usłudze są dostępne dwa rodzaje podpisu XAdES: otoczony i otaczający. Różnią się one strukturą podpisanego pliku.
XAdES otoczony (enveloped)	Podpis znajduje się w strukturze dokumentu – jest „otoczony" treścią dokumentu. Jeśli taki dokument podpisuje więcej osób, ich podpisy zostaną umieszczone w strukturze dokumentu obok siebie i mogą zostać odczytane jednocześnie.
XAdES otaczający (enveloping)	Treść dokumentu znajduje się w strukturze podpisu – jest „otoczona" podpisem. Jeśli taki dokument podpisuje więcej osób, struktura każdego kolejnego podpisu będzie „otaczała" treść dokumentu z wcześniejszym podpisem. Oznacza to, że podczas odczytywania pliku nie zostaną wyświetlone wszystkie podpisy jednocześnie.
PAdES	Format podpisu elektronicznego, który służy do podpisywania dokumentów w formacie PDF. Specyfikacja techniczna wskazana w Decyzji wykonawczej Komisji (UE) 2015/1506 z dnia 8 września 2015 r. ustanawiającej specyfikacje dotyczące formatów zaawansowanych podpisów elektronicznych oraz zaawansowanych pieczęci elektronicznych, które mają być uznane przez podmioty sektora publicznego to ETSI TS103172 v.2.2.2.

3 Dostęp do usług sieciowych systemu Węzeł Podpisu

Przed przystąpieniem do integracji z usługami sieciowymi systemu Węzeł Podpisu należy spełnić kryteria formalne określone w dokumencie „Procedura integracji systemów oraz wymiany certyfikatu do integracji systemów z podpisem zaufanym" umieszczonym na stronie BIP MC.

Wszystkie usługi sieciowe systemu **Węzeł Podpisu** zabezpieczone są za pomocą mechanizmu mTLS (*Mutual TLS authentication*), który stanowi rozszerzenie protokołu TLS . Uzyskanie dostępu do usługi przez system zewnętrzny związane jest ze spełnieniem wszystkich poniższych warunków:

- Nawiązując połączenie mTLS do systemu Węzeł Podpisu klient musi dołączyć certyfikat kliencki, który wymagany jest w procesie wzajemnego uwierzytelniania.
- Żądanie wysyłane do systemu **Węzeł Podpisu** 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 Profil Zaufany.
- Certyfikat kliencki użyty przez system zewnętrzny do podpisania żądania musi być dodany przez administratora systemu PZ do listy certyfikatów systemu zewnętrznego w systemie Profil Zaufany.
- System zewnętrzny musi być oznaczony przez administratora systemu PZ, jako aktywny w systemie Profil Zaufany.
- System zewnętrzny musi mieć przyznane przez administratora systemu PZ uprawnienie do wywoływania operacji usługi sieciowej w systemie **Węzeł Podpisu**.

W celu zwiększenia bezpieczeństwa, system **Węzeł Podpisu** 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 xmlns:ns1="http://ws.apache.org/wss4j">ns1:SecurityError</faultcode>
      <faultstring>A security error was encountered when verifying the message</faultstring>
    </soap:Fault>
  </soap:Body>
</soap:Envelope>
```

3.1 Bezpieczeństwo

3.1.1 WS-Security

Każde żądanie wysyłane przez system zewnętrzny do systemu **Węzeł Podpisu** 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 **Węzeł Podpisu** 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:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wp="http://wp.pz2.coi.gov.pl">
	<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="X509-87F27529A1676C3943169640084849136">MIIEMzCCAxugAwIBAgIEUZv(...)</wsse:BinarySecurityToken>
			<ds:Signature Id="SIG-87F27529A1676C3943169640084849140" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
				<ds:SignedInfo>
					<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
						<ec:InclusiveNamespaces PrefixList="soapenv wp" 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-87F27529A1676C3943169640084849139">
						<ds:Transforms>
							<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
								<ec:InclusiveNamespaces PrefixList="wp" 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>I+BKqXqD2(...)</ds:DigestValue>
					</ds:Reference>
				</ds:SignedInfo>
				<ds:SignatureValue>lhIKaVgPV8Wwno(...)</ds:SignatureValue>
				<ds:KeyInfo Id="KI-87F27529A1676C3943169640084849137">
					<wsse:SecurityTokenReference wsu:Id="STR-87F27529A1676C3943169640084849138">
						<wsse:Reference URI="#X509-87F27529A1676C3943169640084849136" 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-87F27529A1676C3943169640084849139" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
```

```
                <wp:getRequest>
                        <signRequestUrl>https://int.podpis.gov.pl/ui/wp/ik3cknlddkp7i10hz4qjn6xvsklkta4r3xxfybyn/preview</signRequestUrl>
                        <documentIdentifiers>
                                <!--1 or more repetitions:-->
                                <documentIdentifier>1</documentIdentifier>
                        </documentIdentifiers>
                </wp:getRequest>
        </soapenv:Body>
</soapenv:Envelope>
```

Odpowiedź serwera:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
        <soap: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" soap:mustUnderstand="1">
                        <wsu:Timestamp wsu:Id="TS-1f85825d-6a53-4902-b462-1a84df64e543">
                                <wsu:Created>2023-10-04T06:27:28.486Z</wsu:Created>
                                <wsu:Expires>2023-10-04T06:32:28.486Z</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="X509-12dc0ae3-
74d9-412c-9c58-17d3029e6515">MIIDTTCCA(...)</wsse:BinarySecurityToken>
                        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="SIG-4aa7eff2-0f68-49b2-be1e-3fc4bac4bc9c">
                                <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 UR I="#TS-1f85825d-6a53-4902-b462-1a84df64e543">
                                                <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>GzoZzE6hfSl(...)</ds:DigestValue>
                                        </ds:Reference>
                                        <ds:Reference URI="#_3fb70277-2331-4c32-8418-cfb14f124a92">
                                                <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>OAGEIaa(...)</ds:DigestValue>
                                        </ds:Reference>
                                </ds:SignedInfo>
                                <ds:SignatureValue>BwHyTzO4o+Fu+ioqAV(...)</ds:SignatureValue>
                                <ds:KeyInfo Id="KI-5a1b6e80-8e8d-428b-a47a-3c9e1085d960">
```

```
                                                <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-d47efb78-5825-4756-bd96-37ad7ee03f65">
                                                    <wsse:Reference URI="#X509-12dc0ae3-74d9-412c-9c58-17d3029e6515" 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:Header>
                                <soap:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="_3fb70277-2331-4c32-8418-cfb14f124a92">
                                    <ns2:getResponse xmlns:ns2="http://wp.pz2.coi.gov.pl" xmlns:ns3="http://wp.pz2.coi.gov.pl/fault">
                                        <signedDocuments>
                                            <signedDocument>
                                                <identifier>1</identifier>
                                                <content>PD94bWwgdmVyc2lvb(...)</content>
                                            </signedDocument>
                                        </signedDocuments>
                                    </ns2:getResponse>
                                </soap:Body>
</soap:Envelope>
```

3.1.2 Odpowiedź informująca o błędzie - SOAP

W przypadku, gdy system **Węzeł Podpisu** 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:Server</faultcode>
      <faultstring>Parametr successUrl 's' nie jest prawidłowym URL-em</faultstring>
      <detail>
        <ns3:invalidRequestFault xmlns:ns3="http://wp.pz2.coi.gov.pl/fault" xmlns:ns2="http://wp.pz2.coi.gov.pl">
          <identifier>cf6903fd-af0c-422c-ac97-593a27dfe76b</identifier>
          <timestamp>2023-10-04T06:46:53.338Z</timestamp>
          <message>Parametr successUrl 's' nie jest prawidłowym URL-em</message>
        </ns3:invalidRequestFault>
      </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
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 .
detail	System zewnętrzny	Szczegółowy opis błędu: • Identifier – kod błędu • Timestamp – Data i godziną błedu • Message - Opis powodu nieobsłużenia żądania w postaci tekstu

3.1.3 REST Security

Aby mieć możliwość skorzystania z usługi należy w nagłówku przekazać:

- X-API-Version – wersja API do użycia
- X-Client-Cert - Base64 zakodowany certyfikat klienta w formacie DER.

Przykład:

"X-API-Version: 1"

-H "X-Client-Cert: 2JzNiTBKMbaJhRTPL5C…"

4 Definicja usługi sieciowej SOAP

signing SOAP

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

Usługa służy do przesyłania dokumentu do podpisu, pobrania podpisanego dokumentu, dodawania dokumentu wraz z załącznikami do istniejącego żądania podpisu pod dokumentem między systemem, a systemami zewnętrznymi.

Usługa pozwala na podpisywanie dokumentów w formacie XAdES oraz PAdES. Usługa jest dostępna na środowisku integracyjnym pod adresem: https://int.podpis.gov.pl:1443/ws/public/sgws/services/signingService

Definicja usługi znajduje się w pliku signing.wsdl załączonym do instrukcji.

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

1. Klient usługi signing wgrywa przy pomocy operacji `create` plik XML przeznaczony do podpisu.
2. Klient usługi `signing` przekierowuje przeglądarkę użytkownika na URL otrzymany w odpowiedzi operacji `create`. Na wyświetlonej stronie użytkownik dokonuje podpisu dokumentu.
3. Klient usługi `signing` pobiera przy pomocy operacji `get` podpisany plik XML.
4. Klient usługi `signing` wgrywa przy pomocy operacji `add` dodatkowy dokument przeznaczony do podpisu (jako uzupełnienie) w ramach żądania `create`.

4.1 Operacja create

Operacja służy do wgrania dokumentu przeznaczonego do podpisu. Żądanie składa się z następujących pól:

Pole	Typ	Wymagane	Uwagi
signatureFormat	String	Tak	Dopuszczalne wartości formatu podpisu dokumentu: • XAdES otoczony • ZAdES otaczający • PAdES W ramach jednego żądania obsługiwany jest jeden format podpisu pod dokumentem.
signatureMethods	Element XML	Nie	Element może występować wielokrotnie. Dopuszczalne wartości metody podpisu. Efektem jest wyświetlenie użytkownikowi dostępnych metod podpisu w graficznym interfejsie użytkownika systemu.
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
cancelURL	String	Nie	URL na który zostanie przekierowany użytkownik w przypadku anulowania podpisu dokumentu, nie dłuższy niż 1024 znaki, będący poprawnym adresem URL.
documents	Element XML	Nie	Element może występować wielokrotnie. Zawiera informacje dotyczące podpisywanego dokumentu.

Element `signatureMethods` posiada następującą strukturę:

Pole	Typ	Wymagane	Uwagi
signatureMethod	String	Nie	Dopuszczalne metody podpisu: • PZ_PZ – Podpis zaufany - autoryzacja z profilu zaufanego • PZ_SIE – Podpis zaufany - autoryzacja eDowodem • PQ – podpis kwalifikowany • PS – podpis osobisty • MO – podpis aplikacją mObywatel **Uwaga!** Dla podpisu jednego dokumentu w formacie XAdES dostępne są wszystkie metody podpisu. Dla podpisu wielu dokumentów w formacie XAdES dostępne metody podpisu to: PZ_PZ, PZ_SIE, MO Dla podpisu jednego lub wielu dokumentów w formacie PAdES dostępne metody podpisu to: PZ_PZ, PZ_SIE, MO

Element `document` posiada następującą strukturę:

Pole	Typ	Wymagane	Uwagi
content	String	Tak	Dokument do podpisu zakodowany jest w Base64;
information	String	Tak	Informacje dodatkowe w postaci tekstu prezentowanego użytkownikowi na stronie do podpisywania, nie dłuższego niż 4096 znaków
identifier	Int	Tak	Identyfikator dokumentu
xsltURL	String	Nie	URL transformaty określającej wygląd dokumentu elektronicznego w formacie xml
attachments	Element XML	Nie	Dane załącznika dokumentu; Element może występować wielokrotnie. Każde wystąpienie musi posiadać unikalną wartość pola uri.

Element `attachment` posiada następującą strukturę:

Pole	Typ	Wymagane	Uwagi
content	String	Tak	Binarny załącznik dokumentu zakodowany w Base64;
externalRepositoryId	String	Tak	Dopuszczalne wartości identyfikatorów zewnętrznych repozytoriów. Repozytorium ePUAP - elektroniczna Platforma Usług Administracji Publicznej
fileId	String	Tak	Identyfikator pliku w zewnętrznym repozytorium.
mimeType	String	Tak	Typ MIME załącznika, nie dłuższy niż 255 znaków; W przypadku braku pola w żądaniu zostanie przyjęta domyślna wartość „application/octet-stream”.
uri	String	Tak	Identyfikator URI unikalny w ramach dokumentu, nie dłuższy niż 255 znaków np. nazwa dokumentu.

Jeśli wgranie dokumentu udało się, zwracany jest URL na który należy przekierować użytkownika w celu złożenia podpisu pod dokumentem. Do zwróconego adresu URL nie można dodawać własnych parametrów.

Jeśli wgranie dodatkowego dokumentu się nie powiodło, zwracany jest komunikat błędu typu fault, a w nim jeden z poniższych kodów błędów:

Kod	Znaczenie	Przyczyna
InvalidRequestFault	Nieprawidłowy parametr wywołana	• Dokument w polu content 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 • dokument w polu content nie jest prawidłowo zakodowany w Base64 • pole content jest puste

		• pole documentIdentifier jest puste lub przyjmuje nieprawidłową wartość
InvalidDocumentFormatFault	Nieprawidłowy format dokumentu	Nieprawidłowy format podpisu dla podpisywanego dokumentu. np. PAdES nie przyjmuje załączników.
DocumentMaxCountExceededFault	Niedozwolona liczba dokumentów	Liczba dokumentów do podpisu przekracza maksymalną dozwoloną wartość.
AattachmentMaxCountExceededFault	Niedozwolona liczba załączników	Dokument posiada zbyt dużą liczbę załączników.
FileTooBigFault	Zbyt duży plik	Dokument w polu content przekracza dopuszczalny rozmiar.
InternalErrorFault	Błąd wewnętrzny	Wystąpił nieoczekiwany błąd w systemie
systemNoAccessFault	Brak uprawnień	System zewnętrzny nie jest uprawniony do wywołania operacji
InvalidAttachmentFormatFault	Nieprawidłowy format dokumentu	Nieprawidłowy format dokumentu

Przykładowe żądanie operacji wygląda następująco:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wp="http://wp.pz2.coi.gov.pl">
    <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-
87F27529A1676C3943169640324145063">MIIEMzCCAxugAwIBAgIEUZ(...)</wsse:BinarySecurityToken>
            <ds:Signature Id="SIG-87F27529A1676C3943169640324145166" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <ec:InclusiveNamespaces PrefixList="soapenv wp"
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-4468C93F67B6EA8EA216944365218404">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                <ec:InclusiveNamespaces PrefixList="wp"
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>P1USUUF9NJq(...)</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>
                <ds:SignatureValue>fwTYTZWgmQiDBr(...)</ds:SignatureValue>
                <ds:KeyInfo Id="KI-87F27529A1676C3943169640324145064">
```

```
                                        <wsse:SecurityTokenReference wsu:Id="STR-87F27529A1676C3943169640324145065">
                                                <wsse:Reference URI="#X509-87F27529A1676C3943169640324145063"
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-4468C93F67B6EA8EA216944365218404" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">
                <wp:createRequest>
                        <signatureFormat>XAdES</signatureFormat>
                        <successUrl>http://wspolnysukces.spoldzielnie.org/wp-content/uploads/2018/03/logo_WSPOLNY-
SUKCES_awers.png</successUrl>
                        <failureUrl>https://marcosantadev.com/wp-content/uploads/Fatal_Error_Unit_Test.jpg</failureUrl>
                        <cancelUrl>http://localhost:8080/cancel</cancelUrl>
                        <documents>
                                <document>
                                        <content>77u/PD94bWwgdm(...)</content>
                                        <information>Dokument testowy</information>
                                        <identifier>1</identifier>
                                        <xsltUrl>http://crd.gov.pl/wzor/2021/12/10/11121/styl.xsl</xsltUrl>
                                </document>
                        </documents>
                </wp:createRequest>
        </soapenv:Body>
</soapenv:Envelope>
```

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

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
        <soap:Header>
                <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-65fd8ea0-831e-406a-a8d2-11676b714ac6">
                                <wsu:Created>2023-10-04T07:07:21.625Z</wsu:Created>
                                <wsu:Expires>2023-10-04T07:12:21.625Z</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="X509-91d8ddc9-
e9ba-4de5-98d1-b901170ee7b1">MIIDTTCCAj(...)</wsse:BinarySecurityToken>
                        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="SIG-0cf97143-dfd2-4b41-b8a3-5987b538461b">
                                <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-65fd8
ea0-831e-406a-a8d2-11676b714ac6">
```

```
                                                <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>VLPE/kfvZ/h0UuK(...)</ds:DigestValue>
                                        </ds:Reference>
                                        <ds:Reference URI="#_3bca3185-06e0-48fc-acdb-d354a707b682">
                                                <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>AZAVUmW4ms4iJvnN(...)</ds:DigestValue>
                                        </ds:Reference>
                                </ds:SignedInfo>
                                <ds:SignatureValue>sEsNJ/F8jhaHglBFED(...)</ds:SignatureValue>
                                <ds:KeyInfo Id="KI-55519513-e258-40ae-bfca-b72d4beffdc9">
                                        <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-
aeb43815-d99c-4ba2-963f-da84ee98dad7">
                                                <wsse:Reference URI="#X509-91d8ddc9-e9ba-4de5-98d1-b901170ee7b1"
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:Header>
        <soap:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="_3bca3185-06e0-48fc-acdb-
d354a707b682">
                <ns2:createResponse xmlns:ns2="http://wp.pz2.coi.gov.pl" xmlns:ns3="http://wp.pz2.coi.gov.pl/fault">
                        <signRequestUrl>https://int.podpis.gov.pl/ui/wp/u3bd5rtdfswbq6k3qou8r1srf7bumkuuzujyle3g/preview</signRequestUrl>
                </ns2:createResponse>
        </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:Server</faultcode>
      <faultstring>Parametr successUrl 's' nie jest prawidłowym URL-em</faultstring>
      <detail>
        <ns3:invalidRequestFault xmlns:ns3="http://wp.pz2.coi.gov.pl/fault" xmlns:ns2="http://wp.pz2.coi.gov.pl">
          <identifier>f13ff84c-9348-4acb-9832-358f78b5b94e</identifier>
          <timestamp>2023-10-04T07:42:28.151Z</timestamp>
          <message>Parametr successUrl 's' nie jest prawidłowym URL-em</message>
```

```
        </ns3:invalidRequestFault>
      </detail>
    </soap:Fault>
  </soap:Body>
</soap:Envelope>
```

4.2 Operacja get

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

Pole	Typ	Wymagane	Uwagi
signRequestUrl	String	Tak	Adres URL otrzymany w odpowiedzi na żądanie w operacji create
documentIdentifiers	Element XML	Tak	Identyfikator podpisanego dokumentu

Element `documentIdentifiers` posiada następującą strukturę:

Pole	Typ	Wymagane	Uwagi
documentIdentifier	Int	Tak	Unikalny identyfikator dokumentu

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
InvalidRequestFault	Nieprawidłowy parametr wywołana	• pole signRequestURL nie jest prawidłowym URL-em, jest puste lub przekracza dopuszczalną długość • pole documentIdentifier jest puste lub przyjmuje nieprawidłową wartość
SignRequestNotFoundFault	Nieprawidłowy URL	Nieprawidłowy URL do podpisu dokumentu
InvalidSignRequestStatusFault	Brak możliwości pobrania dokumentu	Status żądania podpisu nie pozwala na pobranie dokumentu
signRequestExpiredFault	Wygaśnięcie dokumentu	Ważność dokumentu wygasła
InternalErrorFault	Błąd wewnętrzny	Wystąpił nieoczekiwany błąd w systemie
systemNoAccessFault	Brak uprawnień	System zewnętrzny nie jest uprawniony do wywołania operacji

Przykładowe żądanie operacji wygląda następująco:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wp="http://wp.pz2.coi.gov.pl">
```

```
<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="X509-87F27529A1676C39431696405766454113">MIIEMzCCAxugAwIBAgIEUZ(...)</wsse:BinarySecurityToken>
<ds:Signature Id="SIG-87F27529A1676C39431696405766455117" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
<ec:InclusiveNamespaces PrefixList="soapenv wp" 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-87F27529A1676C39431696405766455116">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
<ec:InclusiveNamespaces PrefixList="wp" 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>kJPERd2VEoLI(...)</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>f+neofaAi1US7Sxd3XN9MY(...)</ds:SignatureValue>
<ds:KeyInfo Id="KI-87F27529A1676C39431696405766455114">
<wsse:SecurityTokenReference wsu:Id="STR-87F27529A1676C39431696405766455115">
<wsse:Reference URI="#X509-87F27529A1676C39431696405766454113" 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-87F27529A1676C39431696405766455116" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
<wp:getRequest>
<signRequestUrl>https://int.podpis.gov.pl/ui/wp/om4tuyytxwxcosjp31zs4h3tkosvl1o19jz8o7fe/preview</signRequestUrl>
<documentIdentifiers>
<!--1 or more repetitions:-->
<documentIdentifier>1</documentIdentifier>
</documentIdentifiers>
</wp:getRequest>
</soapenv:Body>
</soapenv:Envelope>
```

Jeśli powyższe żądanie jest prawidłowe to odpowiedź serwera wygląda następująco:

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

```
    <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-b5f0e3de-c996-4c42-a78c-642b3fb73723">
        <wsu:Created>2023-10-04T07:49:26.556Z</wsu:Created>
        <wsu:Expires>2023-10-04T07:54:26.556Z</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="X509-2e7aabaf-4d77-47db-afc7-
7dede4834955">MIIDTTCCAjWgAwIBAgIIMDNW(...)</wsse:BinarySecurityToken>
      <ds:Signature Id="SIG-66258b07-c3cf-4667-b545-d109041ed722" 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-b5f0e3de-c996-4c42-a78c-642b3fb73723">
            <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>2UCAxXfimdJkKMzl3gNrydda9tL5hjsfeXeEqXZ91Fc=</ds:DigestValue>
          </ds:Reference>
          <ds:Reference URI="#_04a02294-8d43-48c3-80a0-e7de9933c119">
            <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>S0gafGNPxxaGqm3Z(...)</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>fn4SAN6S5eq+lA6s6JYOi(...)</ds:SignatureValue>
        <ds:KeyInfo Id="KI-5b48151f-887f-4e87-9338-207bcdefc3d9">
          <wsse:SecurityTokenReference wsu:Id="STR-796d34f6-3183-434e-b7a8-f995a9143845">
            <wsse:Reference URI="#X509-2e7aabaf-4d77-47db-afc7-7dede4834955" 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:Header>
  <soap:Body wsu:Id="_04a02294-8d43-48c3-80a0-e7de9933c119" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">
    <ns2:getResponse xmlns:ns2="http://wp.pz2.coi.gov.pl" xmlns:ns3="http://wp.pz2.coi.gov.pl/fault">
      <signedDocuments>
        <signedDocument>
          <identifier>1</identifier>
          <content>PD94bWwgdmVyc2lvbj0i(...)</content>
        </signedDocument>
```

```
    </signedDocuments>
   </ns2:getResponse>
  </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:Server</faultcode>
      <faultstring>Żądanie podpisu o id: om4tuyytxwxcosjp31zs4h3tkosvl1o19jz8o7fe wygasło</faultstring>
      <detail>
        <ns3:signRequestExpiredFault xmlns:ns3="http://wp.pz2.coi.gov.pl/fault" xmlns:ns2="http://wp.pz2.coi.gov.pl">
          <identifier>a294c01a-0549-42c4-b3fb-bc8b3a9f38cf</identifier>
          <timestamp>2023-10-04T08:09:22.403Z</timestamp>
          <message>Żądanie podpisu o id: om4tuyytxwxcosjp31zs4h3tkosvl1o19jz8o7fe wygasło</message>
        </ns3:signRequestExpiredFault>
      </detail>
    </soap:Fault>
  </soap:Body>
</soap:Envelope>
```

4.3 Operacja add

Operacja służy do dodawania dokumentu wraz z załącznikami do istniejącego żądania podpisu. W odpowiedzi zwracana jest struktura XML zawierająca szczegółowe informacje na temat podpisu. Żądanie składa się z następujących pól:

Pole	Typ	Wymagane	Uwagi
signRequestUrl	String	Tak	Adres URL otrzymany w odpowiedzi na żądanie w operacji create
documents	Element XML	Tak	Element może występować wielokrotnie. Zawiera informacje dotyczące podpisywanego dokumentu.

Element `document` posiada następującą strukturę:

Pole	Typ	Wymagane	Uwagi
content	String	Tak	Dokument do podpisu zakodowany jest w Base64;

information	String	Tak	Informacje dodatkowe w postaci tekstu prezentowanego użytkownikowi na stronie do podpisywania, nie dłuższego niż 4096 znaków
identifier	Int	Tak	Identyfikator dokumentu
xsltUrl	String	Nie	URL transformaty określającej wygląd dokumentu elektronicznego w formacie xml
attachments	Element XML	Nie	Dane załącznika dokumentu; element może występować wielokrotnie. Każde wystąpienie musi posiadać unikalną wartość pola uri.

Element `attachment` posiada następującą strukturę:

Pole	Typ	Wymagane	Uwagi
content	String	Tak	Binarny załącznik dokumentu zakodowany w Base64;
externalRepositoryId	String	Tak	Dopuszczalne wartości identyfikatorów zewnętrznych repozytoriów. Repozytorium ePUAP - elektroniczna Platforma Usług Administracji Publicznej
fileId	String	Tak	Identyfikator pliku w zewnętrznym repozytorium.
mimeType	String	Tak	Typ MIME załącznika, nie dłuższy niż 255 znaków; W przypadku braku pola w żądaniu zostanie przyjęta domyślna wartość „application/octet-stream”.
uri	String	Tak	Identyfikator URI unikalny w ramach dokumentu, nie dłuższy niż 255 znaków

Jeśli wgranie dodatkowego dokumentu na adres URL żądania się powiodło to zwracana jest struktura XML zawierająca szczegółowe informacje na temat podpisu.

Jeśli wgranie dodatkowego dokumentu się nie powiodło, zwracany jest komunikat błędu typu fault, a w nim jeden z poniższych kodów błędów:

Kod	Znaczenie	Przyczyna
invalidRequestFault	Nieprawidłowy parametr wywołana	• Dokument w polu content 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 • dokument w polu content nie jest prawidłowo zakodowany w Base64 • pole content jest puste • pole documentIdentifier jest puste lub przyjmuje nieprawidłową wartość
signRequestNotFoundFault	Nieprawidłowy URL	Nieprawidłowy URL do podpisu dokumentu
invalidSignRequestStatusFault	Brak możliwości pobrania dokumentu	Status żądania podpisu nie pozwala na pobranie dokumentu
signRequestExpiredFault	Wygaśnięcie dokumentu	Ważność dokumentu wygasła
invalidDocumentFormatFault	Nieprawidłowy format dokumentu	Nieprawidłowy format podpisu dla podpisywanego dokumentu. np. PAdES nie przyjmuje załączników.
documentMaxCountExceededFault	Niedozwolona liczba dokumentów	Liczba dokumentów do podpisu przekracza maksymalną dozwoloną wartość.
attachmentMaxCountExceededFault	Niedozwolona liczba załączników	Dokument posiada zbyt dużą liczbę załączników.
fileTooBigFault	Zbyt duży plik	Dokument w polu content przekracza dopuszczalny rozmiar.
concurrentModificationFault	Nieprawidłowy identyfikator żądania	Żądanie podpisu zostało w międzyczasie zmodyfikowane
internalErrorFault	Błąd wewnętrzny	Wystąpił nieoczekiwany błąd w systemie
systemNoAccessFault	Brak uprawnień	system zewnętrzny nie jest uprawniony do wywołania operacji
invalidAttachmentFormatFault	Nieprawidłowy format dokumentu	Nieprawidłowy format dokumentu

Przykładowe żądanie operacji :

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wp="http://wp.pz2.coi.gov.pl">
	<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="X509-87F27529A1676C39431696409758769141">MIIEMzCCAxugAwIBAgI(...)</wsse:BinarySecurityToken>
			<ds:Signature Id="SIG-87F27529A1676C39431696409758770145" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
				<ds:SignedInfo>
					<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
						<ec:InclusiveNamespaces PrefixList="soapenv wp" 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-87F27529A1676C39431696409758770144">
						<ds:Transforms>
							<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
								<ec:InclusiveNamespaces PrefixList="wp" 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>YyKyS28Lcz9Ru(...)</ds:DigestValue>
					</ds:Reference>
				</ds:SignedInfo>
				<ds:SignatureValue>PV3CnFY2Vu/kzGDS743(...)</ds:SignatureValue>
				<ds:KeyInfo Id="KI-87F27529A1676C39431696409758770142">
					<wsse:SecurityTokenReference wsu:Id="STR-87F27529A1676C39431696409758770143">
						<wsse:Reference URI="#X509-87F27529A1676C39431696409758769141" 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-87F27529A1676C39431696409758770144" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
		<wp:addRequest>

	<signRequestUrl>https://int.podpis.gov.pl/ui/wp/e9r2pmsvmbs0ekd1b8mls0n7hjaml6qjb5lxvaww/preview</signRequestUrl>
			<documents>
				<!--1 or more repetitions:-->
				<document>
					<content>77u/PD94bWwgdmVyc2lv(...)</content>
					<information>Dokument 2</information>
					<identifier>2</identifier>
					<!--Optional:-->
```

```
                                        <xsltUrl>http://crd.gov.pl/wzor/2021/12/10/11121/styl.xsl</xsltUrl>
                                </document>
                        </documents>
                </wp:addRequest>
        </soapenv:Body>
</soapenv:Envelope>
```

Przykładowa odpowiedź dla poprawnego żądania:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
        <soap: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" soap:mustUnderstand="1">
                        <wsu:Timestamp wsu:Id="TS-79815c08-07b7-4dd1-87d6-5efb2159c4d0">
                                <wsu:Created>2023-10-04T08:55:58.771Z</wsu:Created>
                                <wsu:Expires>2023-10-04T09:00:58.771Z</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="X509-7c3c4b0d-
12c5-4d2f-8d25-4685ea0688a2">MIIDTTCCAjWg(...)</wsse:BinarySecurityToken>
                        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="SIG-8ef7a1a0-bf57-4667-9f31-84dfab906a9c">
                                <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-79815
c08-07b7-4dd1-87d6-5efb2159c4d0">
                                                <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>EwDB0s6724okyes(...)</ds:DigestValue>
                                        </ds:Reference>
                                        <ds:Reference URI="#_ff32a78f-e4b6-4471-b9ca-05683edb6ae5">
                                                <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>I5BUPuhS+jlwxzcGCi(...)</ds:DigestValue>
                                        </ds:Reference>
                                </ds:SignedInfo>
                                <ds:SignatureValue>N8gtAFNKktMU6hhdActnJhAMY(...)</ds:SignatureValue>
                                <ds:KeyInfo Id="KI-6eb79190-8dd5-412c-8ffa-2426a671c1fd">
                                        <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-1412c5fa-754c-4e07-b526-302b4aea5d95">
                                                                    <wsse:Reference URI="#X509-7c3c4b0d-12c5-4d2f-8d25-4685ea0688a2"
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:Header>
                            <soap:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="_ff32a78f-e4b6-4471-b9ca-
05683edb6ae5">
                                    <ns2:addResponse xmlns:ns2="http://wp.pz2.coi.gov.pl" xmlns:ns3="http://wp.pz2.coi.gov.pl/fault"/>
                            </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:Server</faultcode>
      <faultstring>Przekroczono dopuszczalną liczbę dokumentów:2</faultstring>
      <detail>
        <ns3:documentMaxCountExceededFault xmlns:ns3="http://wp.pz2.coi.gov.pl/fault" xmlns:ns2="http://wp.pz2.coi.gov.pl">
          <identifier>fc433a77-47db-43a8-a738-c96b785a9345</identifier>
          <timestamp>2023-10-04T09:13:27.592Z</timestamp>
          <message>Przekroczono dopuszczalną liczbę dokumentów:2</message>
        </ns3:documentMaxCountExceededFault>
      </detail>
    </soap:Fault>
  </soap:Body>
</soap:Envelope>
```

5 Definicja usługi sieciowej REST

signing REST

Usługa służy do złożenia podpisu pod dokumentem/dokumentami w ramach utworzonego żądania podpisu, a podpisywany dokument może posiadać załącznik/ załączniki. Po złożeniu podpisu istnieje możliwość pobrania podpisanego dokumentu/ dokumentów.

Usługa signing REST umożliwia złożenie podpisu w formacie:

- PAdES - służy do złożenia podpisu dla pliku w formacie *.pdf.; podpis można sprawdzić po otwarciu podpisanego pliku
- XAdES - służy do złożenia podpisu dla większości pozostałych formatów plików, np. *.doc, *.docx, *.odt, *.xls. *.jpg, *.png, *.xml ale i *.pdf; po złożeniu podpisu powstaje plik XML, w którym zawarte będą dane dokument i podpisu; do odczytania podpisu potrzebne jest odpowiednie oprogramowanie od dostawców usług kwalifikowanych.

W ramach formatu XAdES możliwe jest złożenie podpisu:

- XAdES otoczony (enveloped) - podpis znajduje się w strukturze dokumentu – jest „otoczony" treścią dokumentu. Jeśli taki dokument podpisuje więcej osób, ich podpisy zostaną umieszczone w strukturze dokumentu obok siebie i mogą zostać odczytane jednocześnie.
- XAdES otaczający (enveloping) - treść dokumentu znajduje się w strukturze podpisu – jest „otoczona" podpisem. Jeśli taki dokument podpisuje więcej osób, struktura każdego podpisu będzie „otaczała" treść dokumentu z wcześniejszym podpisem. Oznacza to, że podczas odczytywania pliku nie zostaną wyświetlone wszystkie podpisy jednocześnie.

Proces podpisu z wykorzystaniem usługi `signing` przebiega w następujących krokach:

1. Klient usługi signing przy pomocy endpointu `POST service/api/sgws/signings` tworzy żądanie podpisu. Utworzone żądanie może od razu zawierać dokument.
2. Za pomocą endpointu `POST service/api/sgws/signings/{signRequestId}/documents`, można rozszerzyć istniejące żądanie o kolejne dokumenty.
3. Po złożeniu podpisu/ podpisów pod dokumentem/ dokumentami, za pomocą endpointu `GET /service/api/sgws/signings/{signRequestId}/documents/signed/{documentId}` możliwe jest pobranie podpisanego dokumentu/ dokumentów.

Pozostałe endpointy:

- `GET /external-service/api/sgws/signings/{signRequestId}/documents/signed` – zwraca metadane podpisanych dokumentów danego żądania podpisu
- `GET /external-service/api/sgws/signings/{signRequestId}/documents/unsigned` – zwraca niepodpisane dokumenty danego żądania podpisu

- `DELETE /external-service/api/sgws/signings/{signRequestId}/documents/remove` – usuwa dokumenty z żądania podpisu

5.1 Dokumentacja Swagger UI

Aktualna dokumentacja dla signing REST znajduje się pod adresem https://int.podpis.gov.pl/api-docs/sgws/swagger-ui/index.html

Pola istotne w komunikacji REST:

Pole	Uwagi
attachments	Lista załączników dla dokumentu (pole attachement). Każde wystąpienie załącznika musi posiadać unikalną wartość pola uri. Element może występować wielokrotnie.
cancelUrl	URL na który zostanie przekierowany użytkownik w przypadku anulowania podpisu dokumentu, będący poprawnym adresem URL.
content	Dokument do podpisu wysyłany jest w [string($byte)].
documentId	Identyfikator dokumentu
documentIds	Lista identyfikatorów dokumentów do usunięcia z żądania podpisu. Należy podać min jeden identyfikator dokumentu.
documents	Lista dokumentów do podpisania Zawiera informacje dotyczące podpisywanych dokumentów (pole document). Element może występować wielokrotnie.
externalRepositoryId	Dopuszczalne wartości identyfikatorów zewnętrznych repozytoriów. Enum EPUAP. Repozytorium ePUAP - elektroniczna Platforma Usług Administracji Publicznej
failureUrl	URL na który zostanie przekierowany użytkownik w przypadku niepowodzenia podpisu dokumentu, będący poprawnym adresem URL.
fileHash	skrót zapisanego pliku
fileId	Identyfikator pliku w repozytorium. *Jeśli występuje externalRepositoryId oraz fileId, to nie ma content.*
fileName	Pełna nazwa pliku (wraz z rozszerzeniem).
fileSize	Wielkość pliku podana w Bajt
information	Informacje dodatkowe o pliku.

mimeType	Typ MIME załącznika. W przypadku braku pola w żądaniu zostanie przyjęta domyślna wartość „application/octet-stream”.
signatureFormat	Format podpisu; dozwolone wartości: • XADES_ENVELOPED • XADES_ENVELOPING • PADES **XAdES enveloped** – (otoczony) to typ podpisu elektronicznego XAdES, gdzie dane podpisu są umieszczane wewnątrz struktury podpisywanego dokumentu XML. **XAdES enveloping** – podpis typu otaczającego, w którym struktura podpisywanego dokumentu zawarta jest w kodzie podpisu, a efektem jest jeden podpisany plik z rozszerzeniem xades lub xml. Rozwiązanie to jest rzadziej stosowane, bo pozwala złożyć na dokumencie tylko jeden podpis. **PAdES** - wykorzystuje się tylko przy podpisywaniu pliku PDF. Użycie tego formatu pozwala na zawarcie wielu podpisów pod dokumentem PDF.
signatureMethod	Dopuszczalne metody podpisu: • PZ_PZ – Podpis zaufany – autoryzacja za pomocą profilu zaufanego • PZ_SIE – Podpis zaufany - autoryzacja za pomocą profilu osobistego (eDowód) • PS – podpis osobisty • PQ – podpis kwalifikowany • MO – podpis za pomocą aplikacji mObywatel **Uwaga!** Dla podpisu jednego dokumentu w formacie XAdES dostępne są wszystkie metody podpisu. Dla podpisu wielu dokumentów w formacie XAdES dostępne metody podpisu to: PZ_PZ, PZ_SIE, MO. Dla podpisu jednego lub wielu dokumentów w formacie PAdES dostępne metody podpisu to: PZ_PZ, PZ_SIE, MO.
signatureMethods	Lista dopuszczalnych metod podpisu. Efektem jest wyświetlenie użytkownikowi, w ramach GUI, dostępnych metod podpisu (pole signatureMethod). Element może występować wielokrotnie.
signingRequestUrl	Url który przechodzi do WP
signRequestId	Identyfikator żądania podpisu.

successUrl	URL na który zostanie przekierowany użytkownik w przypadku gdy dokument zostanie poprawnie podpisany, będący poprawnym adresem URL.
uri	Identyfikator URI; unikalny w ramach dokumentu, np. nazwa dokumentu.
xsltUrl	URL transformaty określającej wygląd dokumentu elektronicznego w formacie xml. Wspierane są wyłącznie następujące domeny: • http://crd.gov.pl/ • https://test.epuap.gov.pl/ • https://test3.mobywatel.gov.pl/

6 Struktura XML podpisów wykonanych z użyciem systemu

UWAGA! Poniższe przykłady dotyczą wyłącznie protokołu SOAP. Dla protokołu REST przykłady zawarte są w dokumentacji SWAGGER IU *(patrz rozdz. 5)*

6.1 Podpis Zaufany – profil zaufany

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

Przykładowy prosty dokument XML zawierający prawidłowy Podpis Zaufany:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<a>a<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signature-79d8fd70-1fec-409a-a48c-200a6f2387cc">
                        <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 Id="r-79d8fd70-1fec-409a-a48c-200a6f2387cc-1" 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>mrkd4MdiaDrsm(...)</ds:DigestValue>
                                </ds:Reference>
                                <ds:Reference Type="http://uri.etsi.org/01903#SignedProperties" URI="#xades-79d8fd70-1fec-409a-a48c-200a6f2387cc">
                                        <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>+yaYYUtcUHuIsJyyOeJe9h/tj9EzM5ue7RCIoVU3mkI=</ds:DigestValue>
                                </ds:Reference>
                        </ds:SignedInfo>
                        <ds:SignatureValue Id="value-79d8fd70-1fec-409a-a48c-200a6f2387cc">X4lV03PnJDlBQzSlucaNLc(...)</ds:SignatureValue>
                        <ds:KeyInfo>
                                <ds:X509Data>
                                        <ds:X509Certificate>MIIC1jCCAb6gAwI(...)</ds:X509Certificate>
                                </ds:X509Data>
                        </ds:KeyInfo>
                        <ds:Object Id="QualifyingInfos-79d8fd70-1fec-409a-a48c-200a6f2387cc">
                                <xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.3.2#" Id="QualifyingProps-79d8fd70-1fec-409a-
a48c-200a6f2387cc" Target="#79d8fd70-1fec-409a-a48c-200a6f2387cc">
                                        <xades:SignedProperties Id="xades-79d8fd70-1fec-409a-a48c-200a6f2387cc">
                                                <xades:SignedSignatureProperties>
                                                        <xades:SigningTime>2023-09-28T10:22:22Z</xades:SigningTime>
                                                        <xades:SigningCertificate>
                                                                <xades:Cert>
                                                                        <xades:CertDigest>
                                                                                <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha512"/>
```

```
            <ds:DigestValue>2XZAorVmiYvbV4U(...)</ds:DigestValue>
                                                                                    </xades:CertDigest>
                                                                                    <xades:IssuerSerial>
            <ds:X509IssuerName>CN=myAlias</ds:X509IssuerName>
            <ds:X509SerialNumber>9(...)</ds:X509SerialNumber>
                                                                                    </xades:IssuerSerial>
                                                                            </xades:Cert>
                                                                    </xades:SigningCertificate>
                                                                    <xades:SignaturePolicyIdentifier>
                                                                            <xades:SignaturePolicyImplied/>
                                                                    </xades:SignaturePolicyIdentifier>
                                                                    <xades:SignerRole>
                                                                            <xades:ClaimedRoles>
                                                                                    <xades:ClaimedRole>
                                                                                            <ppZP:PodpisZP
xmlns:os="http://crd.gov.pl/xml/schematy/osoba/2009/03/06/" xmlns:ppZP="http://crd.gov.pl/xml/schematy/ppzp/">
                                                                                                    <ppZP:DaneZP>
            <ppZP:DaneZPOsobyFizycznej>
            <os:Nazwisko rodzajCzlonu="pierwszy">LastNameMock</os:Nazwisko>
            <os:Imie>NameMock</os:Imie>
            <os:ImieDrugie>SecondNameMock</os:ImieDrugie>
            <os:PESEL>80111100100</os:PESEL>
            <ppZP:IdZaufanegoProfilu>1</ppZP:IdZaufanegoProfilu>
            <ppZP:IdKontaUzytkownikaEpuap>123</ppZP:IdKontaUzytkownikaEpuap>
            </ppZP:DaneZPOsobyFizycznej>
                                                                                                    </ppZP:DaneZP>
                                                                                                    <ppZP:DanePodpisu>
            <ppZP:IdKontaUzytkownikaEpuap>123</ppZP:IdKontaUzytkownikaEpuap>
            <ppZP:IdPolitykiAutoryzacji>1</ppZP:IdPolitykiAutoryzacji>
                                                                                                    </ppZP:DanePodpisu>
                                                                                            </ppZP:PodpisZP>
                                                                                    </xades:ClaimedRole>
                                                                            </xades:ClaimedRoles>
                                                                    </xades:SignerRole>
                                                            </xades:SignedSignatureProperties>
                                                    </xades:SignedProperties>
                                            </xades:QualifyingProperties>
                                    </ds:Object>
            </ds:Signature>
</a>
```

6.1.1 Opis pól elementu ClaimedRole specyficznego dla Podpisu Zaufanego

Kod	Przyczyna
PodpisZP	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
DaneZPOsobyFizycznej	Sekcja informacji o osobie fizycznej, która złożyła Podpis Zaufany pod dokumentem
Nazwisko	Nazwisko osoby, która złożyła Podpis Zaufany pod dokumentem
Imie	Imię osoby, która złożyła Podpis Zaufany pod dokumentem
DrugieImie	Drugie imię osoby, która złożyła Podpis Zaufany pod dokumentem
PESEL	Numer identyfikacyjny osoby, która złożyła Podpis Zaufany pod dokumentem. W przypadku Polskiego Dostawcy Tożsamości PESEL.
DanePodpisu	Sekcja informacji o złożonym Podpisie Zaufanym
IdKontaUzytkownikaEpuap	Identyfikator profilu zaufanego
IdPolitykiAutoryzacji	Parametr autoryzacyjny

6.2 Podpis zaufany – eDowód

Schemat XML Podpisu Zaufanego wykonywanego za pośrednictwem systemu 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 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>
```

6.2.1 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

6.3 Podpis certyfikatem kwalifikowanym

Schemat XML podpisu certyfikatem kwalifikowanym wykonywanym za pośrednictwem system zawarty jest w plikach załączonych do instrukcji.

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="id-ca827b20788ba9202525febea6fca651">
                        <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 Id="ID-fba3f7e88910b50492b4d0565a074c4f" 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>uNt7B07VgdTf1NH1+FZiGGDXoRVHM0vMcSazRs9/gfo=</ds:DigestValue>
                                </ds:Reference>
                                <ds:Reference Type="http://uri.etsi.org/01903#SignedProperties" URI="#xades-id-ca827b20788ba9202525febea6fca651">
                                        <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>GDAE8Cu5RtHBZVeXB7nkZ6ajYE2q8H/4Ot+8mB/o5dc=</ds:DigestValue>
                                </ds:Reference>
                        </ds:SignedInfo>
                        <ds:SignatureValue Id="value-id-ca827b20788ba9202525febea6fca651">OZANZWMxie(…)ds:SignatureValue>
                        <ds:KeyInfo>
                                <ds:X509Data>
                                        <ds:X509Certificate>MIIFRzCCBC+(…) </ds:X509Certificate>
                                </ds:X509Data>
                        </ds:KeyInfo>
                        <ds:Object>
                                <xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.3.2#" Target="#id-
ca827b20788ba9202525febea6fca651">
                                        <xades:SignedProperties Id="xades-id-ca827b20788ba9202525febea6fca651">
                                                <xades:SignedSignatureProperties>
                                                        <xades:SigningTime>2023-12-04T20:43:44Z</xades:SigningTime>
                                                        <xades:SigningCertificate>
                                                                <xades:Cert>
                                                                        <xades:CertDigest>
                                                                                <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
        <ds:DigestValue>YG2beSASaGzSWJmP53SMUZfVSOJPovh2NSeE6TrZqbU=</ds:DigestValue>
                                                                        </xades:CertDigest>
                                                                        <xades:IssuerSerial>
```

```
            <ds:X509IssuerName>CN=INT_ePUAPiPZ</ds:X509IssuerName>
            <ds:X509SerialNumber>3527536865450121345</ds:X509SerialNumber>
                                                                        </xades:IssuerSerial>
                                                                    </xades:Cert>
                                                                </xades:SigningCertificate>
                                                            </xades:SignedSignatureProperties>
                                                            <xades:SignedDataObjectProperties>
                                                                <xades:DataObjectFormat ObjectReference="#ID-
fba3f7e88910b50492b4d0565a074c4f">
                                                                    <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>
```

6.4 Podpis certyfikatem podpisu osobistego

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

Przykładowy prosty dokument XML zawierający prawidłowy podpis certyfikatem osobistym:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<a>a
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="id-ae6678c70bb2879b699ea276e6bdc893">
                        <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-f213615427c6e6c38a9364204e52f783" 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>GIuwH/PGDfnTn6r+4SIC+vZIM1+JYUCEd6EkvUEwfvE=</ds:DigestValue>
                                    </ds:Reference>
                                    <ds:Reference Type="http://uri.etsi.org/01903#SignedProperties" URI="#xades-id-ae6678c70bb2879b699ea276e6bdc893">
                                                <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>FiSHJu7mAnJPrULxMDSsmX8ZBaXW+l8zoQjzJ1DG6SA=</ds:DigestValue>
                                </ds:Reference>
                        </ds:SignedInfo>
                        <ds:SignatureValue Id="value-id-ae6678c70bb2879b699ea276e6bdc893">AlsQoy/uJYNQ+(…) </ds:SignatureValue>
                        <ds:KeyInfo>
                                <ds:X509Data>
                                        <ds:X509Certificate>MIIDEzCCAp…)ds:X509Certificate>
                                </ds:X509Data>
                        </ds:KeyInfo>
                        <ds:Object>
                                <xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.3.2#" Target="#id-
ae6678c70bb2879b699ea276e6bdc893">
                                        <xades:SignedProperties Id="xades-id-ae6678c70bb2879b699ea276e6bdc893">
                                                <xades:SignedSignatureProperties>
                                                        <xades:SigningTime>2023-11-29T08:57:09Z</xades:SigningTime>
                                                        <xades:SigningCertificate>
                                                                <xades:Cert>
                                                                        <xades:CertDigest>
                                                                                <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
        <ds:DigestValue>hMUPwGlUCEW7gJ0lsfQu4/9puVHeXOmdZi+pte5ld8A=</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>245909386998551986871767194523247676 71</ds:X509SerialNumber>
                                                                        </xades:IssuerSerial>
                                                                </xades:Cert>
                                                        </xades:SigningCertificate>
                                                </xades:SignedSignatureProperties>
                                                <xades:SignedDataObjectProperties>
                                                        <xades:DataObjectFormat ObjectReference="#ID-
f213615427c6e6c38a9364204e52f783">
                                                                <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>
```

7 Załączniki

UWAGA! Sekcja załączników dotyczy wyłącznie protokołu SOAP.

1. signing.wsdl – schemat XML usługi sieciowej signing
2. wssec-policies.wsdl – schemat XML polityki WS Security
3. faults.xsd – schemat XML obsługi błędów
4. podpis_zp.xsd – schemat XML Podpisu Zaufanego
5. xmldsig-core-schema.xsd – schemat XML podpisu certyfikatem kwalifikowanym
6. create.xml – żądanie przychodzące signing.create
7. createReturn.xml – odpowiedź signing.createReturn
8. get.xml – żądanie przychodzące signing.get
9. getReturn.xml – odpowiedź signing.getReturn
10. add.xml – żądanie przychodzące signing.add
11. addReturn.xml – odpowiedź signing.addReturn
12. PZSignedDocument.xml – przykładowy podpisany Podpisem Zaufanym dokument XML
13. CKSignedDocument.xml – przykładowy podpisany Certyfikatem Kwalifikowanym dokument XML
14. PSSignedDocument.xml – przykładowy podpisany Certyfikatem Osobistym dokument XML