Državni center za storitve zaupanja

Navodila uporabe SOAP WS storitve SicesSign

API navodila za razvijalce za vključitev storitve SicesSign v zunanje aplikacije

veljavnost: od 12. septembra 2017

verzija: 1.7

Pripravil: OSI d.o.o.

Zgodovina sprememb dokumenta

datum	različica	avtor	Opis sprememb
03.09.2016	1.0	Marko Šmid	Prvi osnutek; osnovni načrt dokumenta
20.10.2016	1.1	Marko Šmid	Dopolnitev opisa metod v skladu s spremembami v delovanju storitve.
18.01.2017	1.2	Marko Šmid	Dopolnitev opisa metod v skladu s spremembami v delovanju storitve.
27.03.2017	1.3	Vilijem Križman	Priagoditev dokumentacije novemu URL-ju in dopolnitvam funkcionalnosti.
05.6.2017	1.4	Marko Šmid	Dopolnitve opisa funkcionalnosti putRequest, ki omogoča podpisovanje referenceId dokumenta in vizualnega prikaza podpisa. Opis dodatne metode hasValidCertificates.
15.06.2017	1.5	Marko Šmid	Opis funkcionalnosti signHash
20.07.2017	1.6	Marko Šmid	Opis podrobnosti grafičnega prikaza podpisa
12.9.2017	1.7	Marko Šmid	Opis nove metode confirmSignedData

Kazalo

Integracija WS storitve e-podpisa v zunanjo aplikacijo

CES-Sign aplikacija poleg spletnega dostopa do ad-hoc podpisa za končnega uporabnika, ponuja tudi API spletno storitev SicesSign. SicesSign je (WS) SOAP storitev za integracijo elektronskega podpisa v zunanje aplikacije.

Zunanje aplikacije morajo upoštevati navodila zapisana v nadaljevanju, saj le tako lahko uporabljajo storitev elektronskega podpisa kot zunanjo storitev.

Uporaba SicesSign v zunanji aplikaciji

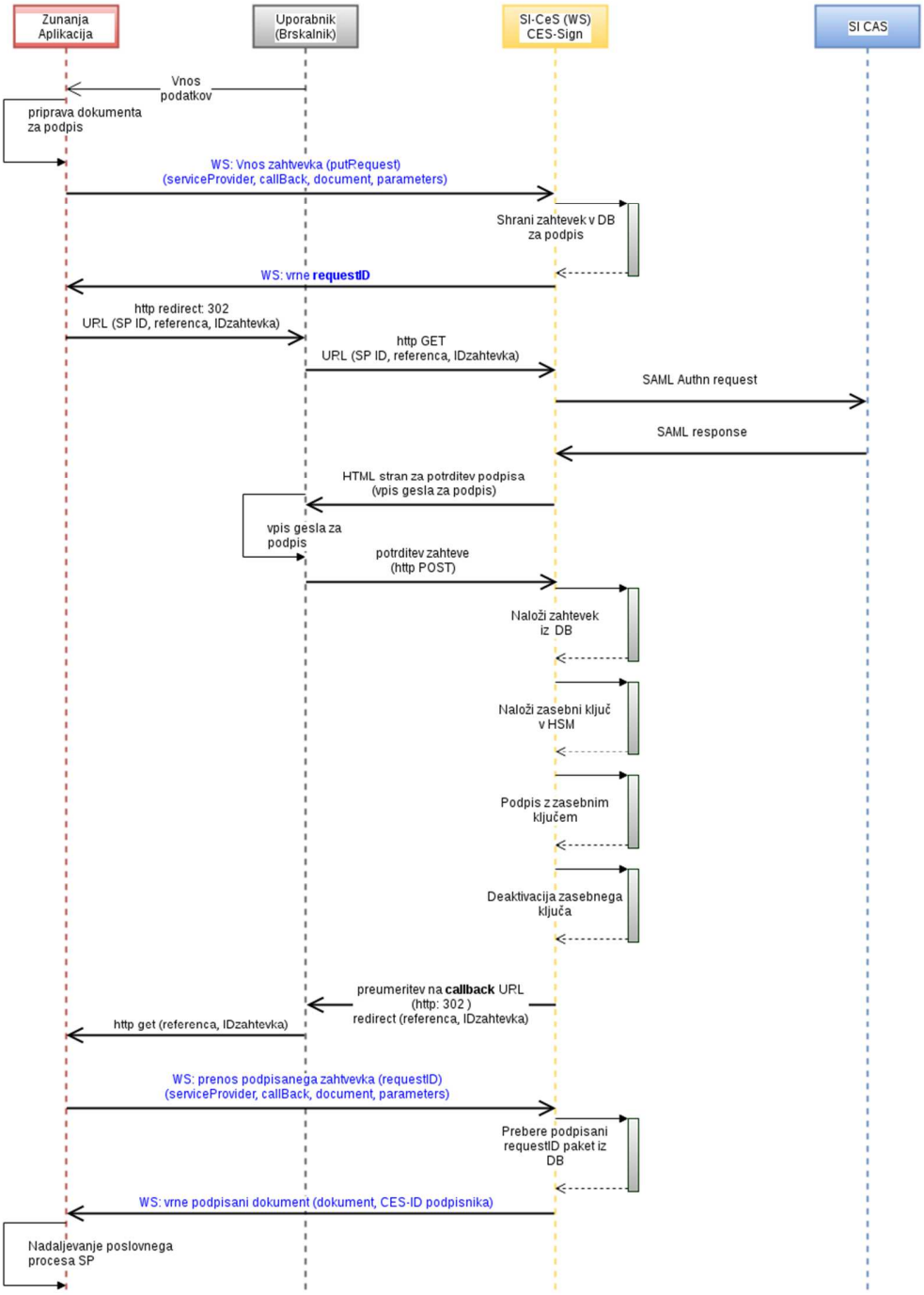
Predpogoja

Skrbnik storitve SicesSign omogoči dostop do storitve z registracijo X.509 digitalnega potrdila. Skrbnik izda in registrira digitalno potrdilo, ki se uporablja za "client X-509 authentication" in ga mora zunanja aplikacija uporabljati pri dostopu do servisa.

Ponudnik storitve SicesSign in lastnik zunanje aplikacije se dogovorita za enoznačno oznako zunanje aplikacije (serviceprovider). To oznako zunanja aplikacija uporablja v vseh klicih spletne storitve. Oznaka skupaj z digitalnim potrdilom predstavljata avtentikacijske parametre za dostop do storitve.

Delovni tok uporabe SicesSign spletne storitve v zunanji aplikaciji

Zunanja aplikacija mora izvajati delovni tok, ki je prikazan v nadaljevanju.


Zunanja Aplikacija
Uporabnik (Brskalnik)
SI-CeS (WS) CES-Sign
SI CAS
Vnos podatkov
priprava dokumenta za podpis
WS: Vnos zahtevka (putRequest)
(serviceProvider, callBack, document, parameters)
Shrani zahtevek v DB za podpis
WS: vrne requestID
http redirect: 302
URL (SP ID, referenca, IDzahtevka)
http GET
URL (SP ID, referenca, IDzahtevka)
SAML Authn request
SAML response
HTML stran za potrditev podpisa
(vpis gesla za podpis)
vpis gesla za podpis
potrditev zahteve
(http POST)
Naloži zahtevek iz DB
Naloži zasebni ključ v HSM
Podpis z zasebnim ključem
Deaktivacija zasebnega ključa
preumeritev na callback URL
(http: 302)
redirect (referenca, IDzahtevka)
http get (referenca, IDzahtevka)
WS: prenos podpisanega zahtevka (requestID)
(serviceProvider, callBack, document, parameters)
Prebere podpisani requestID paket iz DB
WS: vrne podpisani dokument (dokument, CES-ID podpisnika)
Nadaljevanje poslovnega procesa SP

1. Zunanja aplikacija pripravi vsebino za podpis in pokliče spletno storitev SicesSign (WS) .
2. SicesSign (WS) shrani vsebino v podatkovno skladišče, tvori enoznačen Id in ga vrne kot odgovor klicoči aplikaciji. Poleg id-ja vrne tudi URL, kamor mora končna aplikacija preusmeriti uporabnika, ki mora izvesti podpis z osebno kontrolo podpisa in dodatno potrditvijo z vpisom gesla/pin-a za dostop do lastnega digitalnega potrdila.
3. Zunanja aplikacija pripravi 302 preusmeritveni URL, s katerim brskalnik uporabnika preusmeri na storitev digitalnega podpisa CES-Sign (GET URL zahteva).
4. V kolikor uporabnik še nima veljavne seje za CES-Sign podpis, se mora avtenticirati z avtentikacijskim mehanizmom, ki je primeren za oblikovanje podpisa zahtevanega nivoja. Avtentikacija se izvede na storitvi SI-PASS.
5. Po uspešni avtentikaciji na SI-PASS, se preko SAML protokola atributi uporabnika posredujejo aplikaciji CES-Sign.
6. Ob ujemanju posredovanih atributov z atributi lastnika podpisnega zahtevka se v brskalniku uporabnika prikaže stran z vsebino za podpis.
7. Uporabnik za podpis vsake datoteke vtipka osebno geslo, s katerim je varovan zasebni podpisni ključ.
8. CES-Sign po vnosu uporabnikovega gesla izvede klic zalednega strežnika, ki izvede naslednje operacije:
   a) Naloži zahtevek (Id zahtevka) iz DB;
   b) Naloži zasebni ključ v HSM;
   c) V HSM proži dešifriranje ključa in tvorbo podpisa;
   d) Ukine sejo na HSM-ju in s stem izbriše podatke ključa s HSM-ja.
9. Po končani operaciji podpisa na zalednem HSM-ju CES-Sign prejme XML odgovor o uspešnosti operacije.
10. V primeru uspešnega podpisa se za brskalnik uporabnika pripravi URL s *CallBack* povezavo nazaj na zunanjo aplikacijo in Id-jem podpisnega zahtevka.
11. Brskalniku se pošlje HTTP: 302 zahteva za preusmeritev z URL-jem, pripravljenim v prejšnjem koraku - preusmeritev (vrnitev) nazaj na zunanjo aplikacijo z Id-jem zahteve.
12. Aplikacija prevzame podpisani paket s klicem SicesSign (WS) storitve, ki se ji kot vhodni parameter posreduje Id zahtevka.
13. SicesSign prebere paket iz DB podatkovnega skladišča in ga v ustrezni obliki vrne kot odgovor na getSignedData zahtevo. Po uspešnem prevzemu podpisanega paketa SicesSign izbriše paket iz podatkovnega skladišča
14. SicesSign (WS) storitev vrne aplikaciji vsebino paketa in uporabnikov sices_id, ki ga aplikacija lahko uporabi za dodatno potrditev (avtorizacijo) lastnika paketa.

Spletni naslov (URL) za dostop do WSDL opisa Si-CeS (WS) storitve

testni sistem: https://sicas-test.sigov.si/CES-Sign/SicesSign?wsdl

produkcijski sistem: https://sicas.gov.si/CES-Sign/SicesSign?wsdl

Opis Metod SicesSign (WS)

-putRequest - metoda za oddajo podpisnega zahtevka

-getSignedData - metoda za pridobitev podpisanih dokumentov

-validate - metoda za preverjanje podpisa

-ping - preverjanje delovanja servisa

Metoda putRequest

Podatek	Številnost	Opomba
putRequest	1	Zahtevek
serviceProvider	1	Enoznačna oznaka aplikacije
callback	1	Spletni naslov za preusmeritev po končanem podpisu
item	1-n	Podpisni element/paket
document	1	Podatki dokumenta za podpis
bytes	1	Vsebina dokumenta (podatki byte[])
mimeType	1	Mime tip
mimeTypeString	1	Oznaka mime tipa
name	1	Ime datoteke
parameters	1	Parametri podpisa
digestAlgorithm	1	Zgoščevalni algoritem
encryptionAlgorithm	1	Šifrirni algoritem
signatureLevel	1	Nivo podpisa
signaturePackaging	1	Tip pakiranja
references	1	Seznam referenc v klicu putRequest zahteve
reference	1-n	Posamezna referenca
id	1	Enoznačna oznaka reference npr. *ref1*
uri		Oznaka elementa v XML dokumentu
visualSignature	1	Definicija pozicije grafičnega prikaza podpisa
visualSignatureImage	1	Sličica v base64 kodirani obliki, ki je prikazna kot del grafičnega prikaza podpisa
signerLocation	0-1	Kraj podpisnika
city	1	Mesto
country	1	Država
locality	1	Kraj
postalAddress	1	Poštni naslov
postalCode	1	Poštna številka
stateOrProvince	1	Regija
trustLevel	1	Nivo zaupanja

Zaloge vrednosti

digestAlgorithm: SHA1, SHA224, SHA256, SHA384, SHA512, RIPEMD160, MD2, MD5

encryptionAlgorithm: RSA, DSA, ECDSA, HMAC

signatureLevel: XML_NOT_ETSI, XAdES_C, XAdES_X, XAdES_XL, XAdES_A, XAdES_BASELINE_LTA, XAdES_BASELINE_LT, XAdES_BASELINE_T, XAdES_BASELINE_B, CMS_NOT_ETSI, CAdES_BASELINE_LTA, CAdES_BASELINE_LT, CAdES_BASELINE_T, CAdES_BASELINE_B, CAdES_101733_C, CAdES_101733_X, CAdES_101733_A, PDF_NOT_ETSI, PAdES_BASELINE_LTA, PAdES_BASELINE_LT, PAdES_BASELINE_T, PAdES_BASELINE_B, PAdES_102778_LTV, ASiC_S_BASELINE_LTA, ASiC_S_BASELINE_LT, ASiC_S_BASELINE_T, ASiC_S_BASELINE_B, ASiC_E_BASELINE_LTA, ASiC_E_BASELINE_LT, ASiC_E_BASELINE_T, ASiC_E_BASELINE_B

(podrobnejši opis vrednosti: http://dss.nowina.lu/doc/dss-documentation.html)

signaturePackaging: ENVELOPED, ENVELOPING, DETACHED

trustLevel: LOW, MEDIUM, HIGH

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ws="http://ws.sign.sices.osi.si/">
<soapenv:Header/>
<soapenv:Body>
    <ws:putRequest>
        <serviceProvider>SP1</serviceProvider>
        <callback>http://app.test.osi.si/cb/</callback>
        <item>
            <document>
                <bytes>cid:b</bytes>
                <mimeType>
                    <mimeTypeString>XML</mimeTypeString>
                </mimeType>
                <name>A2.xml</name>
            </document>
            <parameters>
                <digestAlgorithm>SHA256</digestAlgorithm>
                <encryptionAlgorithm>RSA</encryptionAlgorithm>
                <signatureLevel>XAdES_BASELINE_B</signatureLevel>
                <signaturePackaging>ENVELOPED</signaturePackaging>
                <signerLocation>
                    <city>Ljubljana</city>
                    <country>Slovenija</country>
                    <locality>Rudnik</locality>
                    <postalAddress>Ukmarjeva 2</postalAddress>
                    <postalCode>1000</postalCode>
                    <stateOrProvince>Ljubljana</stateOrProvince>
                </signerLocation>
            </parameters>
        </item>
        <trustLevel>Medium</trustLevel>
    </ws:putRequest>
</soapenv:Body>
</soapenv:Envelope>
```

Primer zahteve za *XAdES podpis* - Klic SI-CeS (WS) servisa s strani končne aplikacije - POST putRequest(vsebina dolumenta ni prikazana)

```
         <item>
             <document>
<bytes>PHRlc3Q+CiAgPHBvZ29kYmEgaWQ9InBvZDEiPmJsYWJsYSB4IDE8L3BvZ29kYmE+CiAgPHBvZ29kYmEgaWQ9InBvZDIiPmJsYWJsYSB4IDI8L3BvZ29
kYmE+CiAgPHJla2xhbWE+S3VwaSBzdHVmZiE8L3Jla2xhbWE+CjwvdGVzdD4K</bytes>
               <!--Optional:-->
               <mimeType>
                  <mimeTypeString>application/xml</mimeTypeString>
               </mimeType>
               <name>testni-podpis.xml</name>
            </document>
            <parameters>
               <digestAlgorithm>SHA256</digestAlgorithm>
               <encryptionAlgorithm>RSA</encryptionAlgorithm>
               <signatureLevel>XAdES_BASELINE_T</signatureLevel>
               <signaturePackaging>ENVELOPED</signaturePackaging>
               <references>
                  <reference>
                     <id>ref1</id>
                     <uri>#pod1</uri>
                  </reference>
                  <reference>
                     <id>ref2</id>
                     <uri>#pod2</uri>
                  </reference>
               </references>
               <signerLocation>
                 <city>Ljubljana</city>
                 <country>Slovenija</country>
                 <locality>Rudnik</locality>
                 <postalAddress>Ukmarjeva 2</postalAddress>
                 <postalCode>1000</postalCode>
                 <stateOrProvince>Ljubljana</stateOrProvince>
               </signerLocation>
            </parameters>
         </item>
         <trustLevel>High</trustLevel>
      </ws:putRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Primer dela zahteve **putRequest** v kateri zahtevamo podpis posameznih elementov XML dokumenta. Osnovni dokument, ki ga z zahtevo posredujemo v podpis ima vsebino:

```
<test>
 <pogodba id="pod1">blabla x 1</pogodba>
```

```
 <pogodba id="pod2">blabla x 2</pogodba>
 <reklama>Kupi stuff!</reklama>
</test>
```

Z *references* naslavljamo posamezne elemente XML dokumenta, tako da vsaki referenci damo posebno oznako (*id)* in podatek o elementu dokumenta, ki ga naslavljamo z naslovom s katerim je element označen v dokumentu (*uri*).

Grafični prikaz podpisa na PDF dokumentu

Primer zahteve **putRequest** z vsebino zahteve, ki posreduje podatke za grafični prikaz elektronskega podpisa.

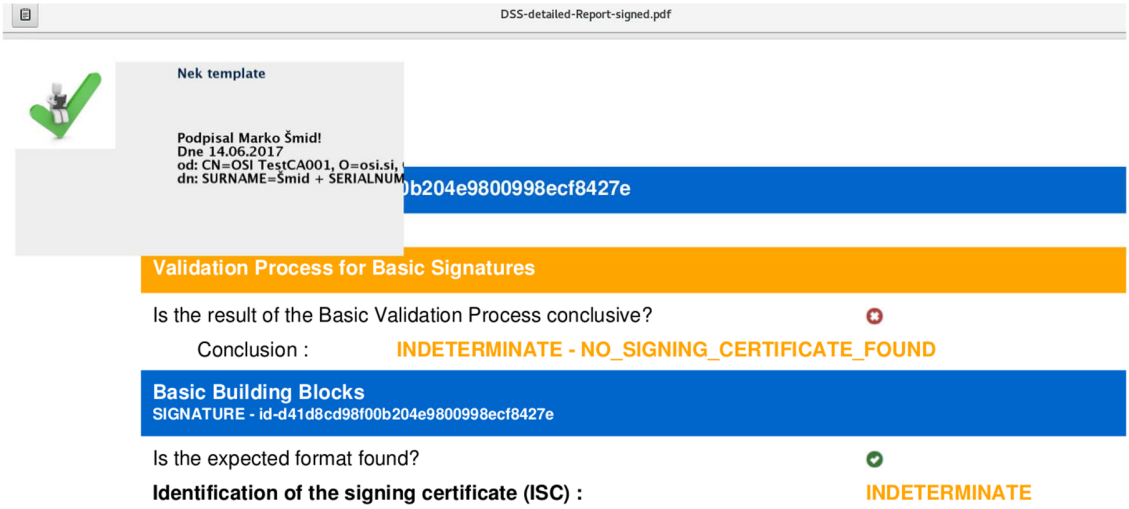
```
      <item>
        <document>
          <bytes> base64 encoded file content</bytes>
          <mimeType>
            <mimeTypeString>application/xml</mimeTypeString>
          </mimeType>
          <name>DSSdetailedReport.PDF</name>
        </document>
        <parameters>
           <digestAlgorithm>SHA1</digestAlgorithm>
           <encryptionAlgorithm>RSA</encryptionAlgorithm>
           <signatureLevel>PAdES_BASELINE_B</signatureLevel>
           <signaturePackaging>ENVELOPED</signaturePackaging>
           <signerLocation>
                  <city>Ljubljana</city>
                  <country>Slovenija</country>
                  <locality>Rudnik</locality>
                  <postalAddress>Ukmarjeva 2</postalAddress>
                  <postalCode>1000</postalCode>
                  <stateOrProvince>Ljubljana</stateOrProvince>
           </signerLocation>
           <visualSignature>
      {  "page":1, "dpi":720, "x":10,"y":10,"width":1440,"height":720,"background":"#FFFFFF",
          "instructions":[ {"code":"image","x":0,"y":0},
      {"code":"text","data":"Nek template","font":"Arial-BOLD-48","color":"#002244","x":600,"y":60},
                    {"code":"text","data":"Podpisal $firstname $lastname!","font":"Arial-BOLD-
48","color":"#000000","x":600,"y":300},
                 {"code":"text","data":"Dne $date.format('dd.MM.yyyy', $ts)","font":"Arial-BOLD-
48","color":"#000000","x":600,"y":350},
      {"code":"text","data":"od: $issuer","font":"Arial-BOLD-48","color":"#000000","x":600,"y":400},
      {"code":"text","data":"dn: $subject","font":"Arial-BOLD-48","color":"#000000","x":600,"y":450}
                    ] }
             </visualSignature>
             <!--Optional:-->
             <visualSignatureImage>/9j/4AAQSkZJRgABAQEASABIAAD/2wBDAAYEBAQFBAYFBQYJBgUGCQsIBgY . . .
</visualSignatureImage>
          </parameters>
      </item>
      <trustLevel>Low</trustLevel>
    </ws:putRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

Grafično vizualizacija podpisa je smiselna za PDF dokumente. Končna aplikacija, ki posreduje **putRequest** klic s parametroma *visualSignature* in *visualSignatureImage* posreduje podatke za vitualizacijo podpisa:

- visualSignature: vsebuje seznam elementov, ki določajo pozicijo podpisa in vsebino teksta v prikazani grafični podobi elektronskega podpisa.

- visualSignatureImage: dodatna opcijska sličica, ki se pripne na vizualizirani prikaz podpisa

Spodaj je primer prikaza vizualnega prikaza podpisa, pri čemer je sličica v levem kotu posredovana v parametru visualSignatureImage, tekstovni podatki podpisa pa so dinamični: podpisnik, ki je podpisal dokument, datum podpisa, izdajatelj digitalnega potrdila podpisnika in dn digitalnega potrdila, katerega lastnik je podpisnik.



Vsebina visualSignature polja: polje ima podatke v json notaciji, ki se prične s predklepajem { in konča z zaklepajem }. Polje vsebuje naslednje obvezne elemente:

- "page": PAGE (podatek na kater strani (PAGE) bo viden grafični povzetek podpisa),
- "dpi":DPI (podatek resolucije grafične podobe podpisa)
  - A4: 600 dpi (print) = 4960 X 7016 pixels,
- "x":X (podatek pozicije X (horizontalno) grafične podobe na izbrani strani PDF dooumenta),
- "y":Y podatek pozicije Y (vertikalno) grafične podobe na izbrani strani PDF dooumenta),
- "width":WIDTH (širina grafične podobe podpisa v točkah),
- "height":HEIGHT (višina grafične podobe podpisa v točkah),
- "background":BACKGROUND (barva ozadja grafičnega prikaza podpisa. BACKGROUND podatek je zapisan znotraj “ v RGB hexa obliki, npr. #FFFFFF),
- "instructions": [json tabela] (navodila vsebine vizualne podobe podpisa). Ta tabela lahko vsebuje elemente:
  - “code":"text" (tekstovna vrstica),
  - “code”:”image” (sličica).

page	1
dpi	720
x	10
y	10
width	1440
height	720
background	#FFFFFF

instructions

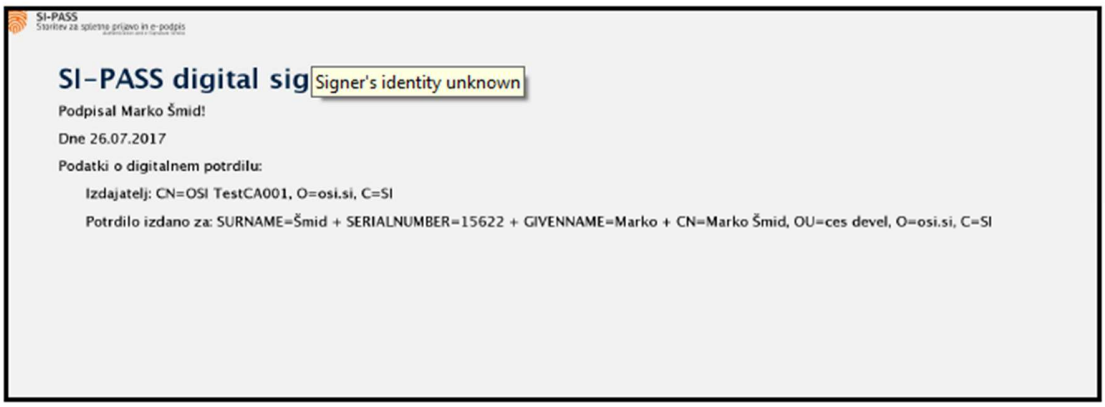
code	x	y	data	font	color
image	0	0			
text	600	60	Nek template	Arial-BOLD-48	#002244
text	600	300	Podpisal $firstname $lastname!	Arial-BOLD-48	#000000
text	600	350	Dne $date.format('dd.MM.yyyy', $ts)	Arial-BOLD-48	#000000
text	600	400	od: $issuer	Arial-BOLD-48	#000000
text	600	450	dn: $subject	Arial-BOLD-48	#000000

“code":"text" in “code”:”image” vsebujeta dodatne podatke, ki se navedejo kot elementi posameznega elementa polja:

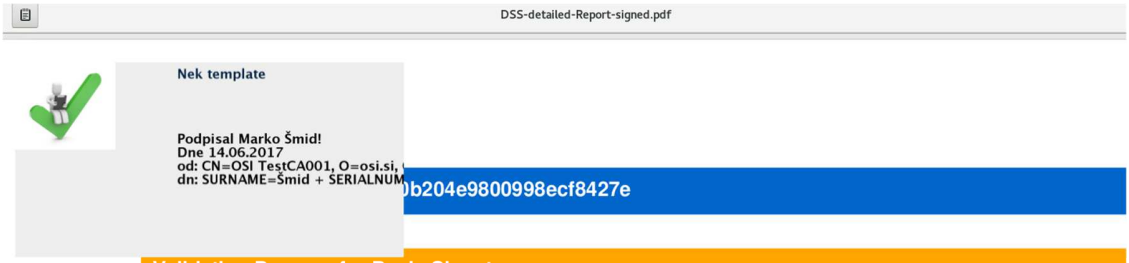
- x: odmik x v točkah od levega robu;
- y: odmik y v točkah od levega robu;
- data: tekst, ki bo prikazan v vrstici;
- font: font, ki bo uporabljen za prikaz teksta vrstice (uporbimo pdf poprte fonte);
- color: barva teksta vrstice v RGB hexa formatu;

“code”:”image” vsebuje podrobnosti prikaza sličice, ki je vsebovana v podatku **visualSignatureImage,** zato nima kolone **data** in dodatno vsebuje le pozicijo sličice znotraj polja grafičnega prikaza podpisa.

Primer podatkov, ki tvorijo podpis na spodnji sličici:



<visualSignature>
{ "page":1, "dpi":600, "x":10,"y":10,"width":2000,"height":720,"background":"#F2F2F2",
"instructions":[{"code":"image","x":0,"y":0},
{"code":"text","data":"SI-PASS digital signature","font":"Arial-BOLD-48","color":"#002244","x":100,"y":150},
{"code":"text","data":"Podpisal $firstname $lastname!","font":"Arial-BOLD-24","color":"#000000","x":100,"y":200},
{"code":"text","data":"Dne $date.format('dd.MM.yyyy', $ts)","font":"Arial-BOLD-24","color":"#000000","x":100,"y":250},
{"code":"text","data":"Podatki o digitalnem potrdilu:","font":"Arial-BOLD-24","color":"#000000","x":100,"y":300},
{"code":"text","data":"Izdajatelj: $issuer","font":"Arial-BOLD-24","color":"#000000","x":150,"y":350},
{"code":"text","data":"Potrdilo izdano za: $subject","font":"Arial-BOLD-24","color":"#000000","x":150,"y":400}
] }
</visualSignature>
<visualSignatureImage>iVBORw0KGgoAAAANSUhEUgAAAbIAAAA1CAYAAAAksW7IA....
</visualSignatureImage>



Validation Process for Basic Signatures

Is the result of the Basic Validation Process conclusive?

Conclusion : INDETERMINATE - NO_SIGNING_CERTIFICATE_FOUND

Basic Building Blocks
SIGNATURE - id-d41d8cd98f00b204e9800998ecf8427e

Is the expected format found?

Identification of the signing certificate (ISC) : INDETERMINATE

```
            <city>Ljubljana</city>
            <country>Slovenija</country>
            <locality>Rudnik</locality>
            <postalAddress>Ukmarjeva 2</postalAddress>
            <postalCode>1000</postalCode>
            <stateOrProvince>Ljubljana</stateOrProvince>
         </signerLocation>
         <visualSignature>
      {  "page":1, "dpi":720, "x":10,"y":10,"width":1440,"height":720,"background":"#FFFFFF",
         "instructions":[ {"code":"image","x":0,"y":0},
      {"code":"text","data":"Nek template","font":"Arial-BOLD-48","color":"#002244","x":600,"y":60},
      {"code":"text","data":"Podpisal $firstname $lastname!","font":"Arial-BOLD-48","color":"#000000","x":600,"y":300},
               {"code":"text","data":"Dne $date.format('dd.MM.yyyy', $ts)","font":"Arial-BOLD-
48","color":"#000000","x":600,"y":350},
      {"code":"text","data":"od: $issuer","font":"Arial-BOLD-48","color":"#000000","x":600,"y":400},
      {"code":"text","data":"dn: $subject","font":"Arial-BOLD-48","color":"#000000","x":600,"y":450}
                ] }
         </visualSignature>
         <!--Optional:-->
         <visualSignatureImage>/9j/4AAQSkZJRgABAQEASABIAAD/2wBDAAYEBAQFBAYFBQYJBgUGCQsIBgY . . . </visualSignatureImage>
      </parameters>
   </item>
   <trustLevel>Low</trustLevel>
  </ws:putRequest>
 </soapenv:Body>
</soapenv:Envelope>
```

Rezultat klica metode putRequest

Podatek	Številnost	Opomba
putRequestResponse	1	Odgovor
return	1	Sestavljeni odgovor
requestId	1	Id paketa na storitvi SicesSign, pod katerim CSS strežnik shrani posredovane dokumente
URL	1	URL, ki kaže na CSS strežnik, kamor aplikacija usmeri uporabnika za podpis paketa

Primer rezultata klica metode putRequest

Odgovor, ki ga aplikacije prejme v polju return, je sestavljeni odgovor, ki vsebuje:

- **URL** naslov z Id-jem paketa. URL naslovi za posamezne nivoje podpisa so določeni v konfiguraciji. Aplikacija po prejemu URL naslova + Id paketa uporabnikovem brskalniku pošlje zahtevo za preusmeritev (HTTP status: 302) na spletno stran CES-Sign storitve za izvedbo podpisa. S preusmeritvijo se uporabniku vrne možnost interakcije s spletno storitvijo podpisa.
  - Primer URLja v odgovoru (<URL>), ki ga aplikacija uporabi za preusmeritev uporabniškega brskalnika:
    - https://sices.test.osi.si/CES-Sign/signws.htm?requestid=ad2729f1fe388d6a1b1e6f85323be2737bd896366a2aea7071aa94b4db6076c851a718ce81b536439e40f15df2f682f951f6a94c382df0a91d9d95f63ca44a47562f2d3017e35a28c38fe086e1724fa59940198d4e300930946c4caec2ccd70b3f79cbac3ddbaba55ba564ff9c2c2f7f80d7750fa3e633c16e5a9c21fee1e6bf147c18b2ab2167f1a5474534a0aa0d41
- **requestid**, ki predstavlja id podpisnega paketa v katerem so vsebovani elementi, ki smo jih posredovali prek putRequest zahteve.

```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
<S:Body>
<ns2:putRequestResponse xmlns:ns2="http://ws.sign.sices.osi.si/">
<return>
    <requestId>3aecd656a4af1157f445c6f917619a011d2dab71b6a3f71352db924712caf470c76105bed2f6c6cd31d628af0c76e76209064828b43c3d435962f05063543350133d3bae5a63ba4c621b0c46f3f5ac75855b057a6c857873ad21066613a09356b199cb1d90588d477b3a238c3cfe7284e2de6e8d81eb09415627daef4bdfc6e88c72bfd2d5cc98937fe6cf48207bee4b</requestId>
    <URL>https://sices.test.osi.si/CES-Sign/low/signws.htm?requestid=3aecd656a4af1157f445c6f917619a011d2dab71b6a3f71352db924712caf470c76105bed2f6c6cd31d628af0c76e76209064828b43c3d435962f05063543350133d3bae5a63ba4c621b0c46f3f5ac75855b057a6c857873ad21066613a09356b199cb1d90588d477b3a238c3cfe7284e2de6e8d81eb09415627daef4bdfc6e88c72bfd2d5cc98937fe6cf48207bee4b</URL>
 </return>
</ns2:putRequestResponse>
</S:Body>
</S:Envelope>
```

Po izvedenem podpisu v CES-Sign aplikaciji se uporabnikovem brskalniku ponovno pošlje zahteva za preusmeritev, tokrat za vrnitev v aplikacijo. URL preusmeritve je sestavljen iz posredovanega *callback* URL-ja pri klicu metode putRequest in Id paketa, ter rezultata podpisa v polju status:

http://app.test.osi.si/cb/?*requestid*=ad2729f1fe388d6a1b1e6f85323be2737bd896366a2aea7071aa94b4db6076c851a718ce81b536439e40f15df2f682f951f6a94c382df0a91d9d95f63ca44a47562f2d3017e35a28c38fe086e1724fa59940198d4e300930946c4caec2ccd70b3f79cbac3ddbaba55ba564ff9c2c2f7f80d7750fa3e633c16e5a9c21fee1e6bf147c18b2ab2167f1a5474534a0aa0d41&status=true

Metoda getSignedData

Podatek	Številnost	Opomba
getSignedData	1	Zahtevek
serviceProvider	1	Enoznačna oznaka aplikacije
requestId	1	Id paketa, ki ga aplikacija dobi kot parameter ob preusmeritvi iz CES-Sign

Spletni naslov aplikacije, na katerega se je vrnil uporabnik, prek *callback* preusmeritve prejme podatek (paket Id) **requestid**. Ta podatek aplikacija uporabi za klic metode *getSignedData* spletne storitve SI-CeS (WS)

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ws="http://ws.sign.sices.osi.si/">
<soapenv:Header/>
<soapenv:Body>
<ws:getSignedData>
<serviceProvider>SP1</serviceProvider>
<requestId>18c80afd450c4bd6e9e83bb75747069a9e97920fcef318e68139257e9a2d66b6f467649bce80c95ccfc467cc87f786f53645ab47e5fb697152bd73ff70ba6c36cffc8c0b8195cfabeea841a41c9a6401a260955cc1c59287944771640959fa9b0d8e2174da370959e3101ef2629818a77669ab279a4e959109232fa9ee3025fff6125291d2c0cb6a2053981bfebaa5b3</requestId>
</ws:getSignedData>
</soapenv:Body>
</soapenv:Envelope>
```

Primer zahteve vsebuje **requestId -** podatek, ki ga je aplikacija prejela prek posredovanega parametra.

Rezultat klica metode getSignedData

Podatek	Številnost	Opomba
getSignedDataResponse	1	Odgovor
return	1	Rezultat
status	1	Status podpisa
cesId	1	Id podpisnika
document	1-n	Dokument
bytes	1	Vsebina podpisanega dokumenta
mimeType	1	Mime tip
mimeTypeString	1	Oznaka mime tipa
name	1	Ime datoteke
certificateChain	1	Veriga potrdil
certificate	1-n	Posamezno potrdilo

Rezultat klica metode vrne sledeče podatke:

status: status podpisa (SIGNED/NOTSIGNED)

cesId: identifikator podpisnika. Ta podatek služi za preverjanje, ali je vrnjen cesid podpisnika enak cesid-ju, ki ga je aplikacija sprejela ob avtentikaciji uporabnika pri dostopu do aplikacije. S tem aplikacija lahko prepreči možno zlorabo, da bi dokument podpisala ena oseba, avtentikacijo pa izvedla druga.

document: vsebina podpisanega dokumenta

certificateChain: veriga potrdil, ki predstavljajo podpisnika in izdajatelja (CA), ki je izdal potrdilo podpisnika.


```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
  <S:Body>
    <ns2:getSignedDataResponse xmlns:ns2="http://ws.sign.sices.osi.si/">
      <return>
        <status>SIGNED</status>
        <cesid>00000000000000000002</cesid>
        <document>
<bytes>A5U2VyaWFsTnVtYmVyPjE1MDI3MzA1Mjc4NTMwMzA5MTMwMjI0MTE5ODU3MjYyOTI3NTYwMDYzMTEyNDc3NDwvZHM6WDUwOVNlcmlhbE51bWJlcj48L3hhZGVzOklzc3VlclNlcmlhbD48L3hhZGVzOkNlcnQ+PC94YWRlczpTaWduaW5nQ2VydGlmaWNhdGU+.....
</bytes>
          <mimeType>
            <mimeTypeString>text/xml</mimeTypeString>
          </mimeType>
          <name>A2.xml</name>
        </document>
        <certificateChain>
<certificate>MIIFIDCCAwigAwIBAgIUGIJ6C5Mp5OATpGLOAAAAAFWgUyYwDQYJKoZIhvcNAQELBQAwNjELMAkGA1UEBhMCU0kxDzANBgNVBAoTBm9zaS5zaTEWMBQGA1UEAxMNT1NJIFRlc3RDQTAwMTAeFw0xNTA5MjExOTQ4NDlaFw0xODA5MjEyMDE4NDlaMIGBMQswCQYDVQQGEwJTSTEPMA0GA1UEChMGb3NpLnNpMRIwEAYDVQQLEwljZXMgZGV2ZWwxTTAMBgNVBAQMBcWgbWlkMAwGA1UEKhMFTWFya28wEgYDVQQDDAtN.....
</certificate>
<certificate>MIIFcjCCA1qgAwIBAgIUCvoeRE/yFY+VYzB8AAAAAFWgSocwDQYJKoZIhvcNAQELBQAwNjELMAkGA1UEBhMCU0kxDzANBgNVBAoTBm9zaS5zaTEWMBQGA1UEAxMNT1NJIFRlc3RDQTAwMTAeFw0xNTA3MTAyMjE0MjFaFw0zNTA3MTAyMjQ0MjFaMDYxCzAJBgNVBAYTAlNJMQ8wDQYDVQQKEwZvc2kuc2kxFjAUBgNVBAMTDU9TSSBUZXN0Q0EwMDEwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDEkPSNq8hgPxt25e.....
</certificate>
        </certificateChain>
      </return>
    </ns2:getSignedDataResponse>
  </S:Body>
</S:Envelope>
```


Primer rezultata klica metode getSignedData (vsebina dokumenta - polji bytes in certificate nista prikazani v celoti)

Metoda validate

Metoda je namenjena preverjanju veljavnosti podpisa v dokumentu.

Podatek	Številnost	Opomba
validate	1	Zahtevek
serviceProvider	1	Enoznačna oznaka aplikacije
document	1	Podatki dokumentov za podpis
bytes	1	Vsebina dokumenta (podatki byte[])
mimeType	1	Mime tip
mimeTypeString	1	Oznaka mime tipa
name	1	Ime datotetke

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ws="http://ws.sign.sices.osi.si/">
<soapenv:Header/>
<soapenv:Body>
    <ws:validate>
        <serviceProvider>SP1</serviceProvider>
        <document>
            <bytes>cid:b</bytes>
            <mimeType>
                <mimeTypeString>XML</mimeTypeString>
            </mimeType>
            <name>A2.xml</name>
        </document>
    </ws:validate>
</soapenv:Body>
</soapenv:Envelope>
```

Primer klica metode validate

Rezultat klica metode validate

Podatek	Številnost	Opomba
validateResponse	1	Odgovor
return	1	Rezultat
ok	1	Boolean vrednost izida preverjanja
resultcode	1	Koda rezultata
simplereport	1	Enostavno poročilo preverjanja
detailedreport	1	Detaljno poročilo preverjanja
diagnosticdata	1	Diagnostično poročilo preverjanja

Metoda ping

Metoda ping je namenjena preverjanju delovanja spletnega servisa. Kot parameter sprejme poljuben string in vrne vhodni string, kateremu je spredaj dodana besedica pong ter dvopičje. Zaradi enostavnosti metode le-ta ni opisana.

Metoda hasValidCertificates

Metoda *hasValidCertificates* je namenjena preverjanju ali ima uporabnik ustrezno digitalno potrdilo za izvedbo podpisa želenega nivoja.

Podatek	Številnost	Opomba
hasValidCertificates	1	Zahtevek
cesid	1	Enoznačen podatek o CSS uporabniku
trustLevel	1	Minimalni "nivo podpisa"

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ws="http://ws.sign.sices.osi.si/">
<soapenv:Header/>
<soapenv:Body>
        <ws:hasValidCertificates xmlns="http://ws.sign.sices.osi.si/">
            <cesid xmlns="">[string?]</cesid>
            <trustLevel xmlns="">[string?]</trustLevel>
        </ws:hasValidCertificates>
    </Body>
</Envelope>
</soapenv:Body>
</soapenv:Envelope>
```

Primer klica metode hasValidCertificates

Rezultat klica metode hasValidCertificates

Podatek	Številnost	Opomba
hasValidCertificatesResponse	1	Odgovor
return	1	String vrednost YES/NO, odvisno rezultata izračuna, če ima uporabnik ustrezno SI-PASS potrdilo za pričakovani nivo podpisa.

Metoda confirmSignedData

Pri zaključnem prevzemu podpisanega paketa z metodo getSignedData, se je do verzije 1.7, status podpisanega paketa spremenil na vrednost END. Vsebina celotnega paketa s statusom END se nato izbriše.

Od verzije 1.7 naprej pa je omogočeno potrjevanje prevzetega podpisanega paketa. Ob prevzemu podpisanega paketa se status paketa ne spremeni, dokler končna aplikacija ne potrdi uspešnega prevzema paketa prek klica metode *confirmSignedData*.

Podatek	Številnost	Opomba
confirmSignedData	1	Zahtevek
requestId	1	Enoznačen id podpisanega paketa, katere prevzem s tem klicem aplikacija potrjuje.
success	1	Z vrednostjo "true" aplikacija potrjuje uspešen prevzem.
ServiceProvider	1	Enoznačna oznaka končne aplikacije, ki mu jo je dodelil ponudnik storitve ob prvi registraciji.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ws="http://ws.sign.sices.osi.si/">
   <soapenv:Header/>
   <soapenv:Body>
      <ws:confirmSignedData>
         <!--Optional:-->
         <serviceProvider>ExternalProvider</serviceProvider>
         <!--Optional:-->
         <requestId>6b5f64a73e:::f331b</requestId>
         <success>true</success>
      </ws:confirmSignedData>
   </soapenv:Body>
</soapenv:Envelope>
```

Primer klica metode confirmSignedData

Rezultat klica metode confirmSignedData

Ob uspešni potrditvi s klicem confirmSignedData, se paketu status spremeni na END. Ta status se vrne tudi v rezultatu ob klicu metode conformSignedData. Poleg statusa pa metoda vrne še podatek cesid uporabnika, ki je izvedel podpisa paketa.

Podatek	Številnost	Opomba
confirmSignedDataResponse	1	Odgovor
status	1	String vrednost "END", ki pove končni status zahteve. S tem je obdelava zahteve zaključena in zahteva se izbriše iz SicesSign struktur.
cesid	1	cesid uporabnika, ki je izvedel podpis paketa prek spletne aplikacije za podpis.

Primer odgovora ob uspešnem klicu metode confirmSignedData.

```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
   <S:Body>
      <ns2:confirmSignedDataResponse xmlns:ns2="http://ws.sign.sices.osi.si/">
         <return>
            <status>END</status>
            <cesid>1190632409</cesid>
         </return>
      </ns2:confirmSignedDataResponse>
   </S:Body>
</S:Envelope>
```

Ob napaki pri klicu metode confirmSignedData, klic vrne HTTP status 500 in informacijo o tipu napake:

- ob neobstoječem id-ju paketa, metoda vrne faultstring: DB_error
- ob nedelovanju sistemskih storitve pa faultstring: SYSTEM_error

```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
   <S:Body>
      <S:Fault xmlns:ns4="http://www.w3.org/2003/05/soap-envelope">
         <faultcode>S:Server</faultcode>
         <faultstring>DB_error</faultstring>
         <detail>
            <ns2:SignException xmlns:ns2="http://ws.sign.sices.osi.si/">
               <message>DB_error</message>
            </ns2:SignException>
         </detail>
      </S:Fault>
   </S:Body>
</S:Envelope>
```

Podpis posredovanega povzetka z uporabo GET metode(signHash)

Aplikacija CES-Sign omogoča podpis posredovanega povzetka (HASH), ki ga končna aplikacija posreduje prek HTTPS preusmeritve z vsemi parametri v GET HTTP zahtevi.

Koraki podpisa HASH-a so naslednji:

Korak 1:

Aplikacija posreduje zahtevo prek preusmeritve uporabnika na URL povezavo:

https://sices.test.osi.si/CES-Sign/low/signhash.htm?requestid=1234567890&hash=6B546F536A43476A795935634D4545484F6B7672622F2F7A6E773D&callback=http://somewhere.com&serviceprovider=OSI&name=optional_descriptive_name

Zahtevani nivo podpisa aplikacija zahteva z imenom v URL-ju: low, medium, high

Parametri URL zahteve:

hash=povzetek, ki bo podpisan, v Hexadecimalni obliki

callback=URL naslov, kamor mora CES-Sign vrniti uporabnika, po uspešnem podpisu

serviceprovider=oznaka service providerja, ki jo je naročniku storitve dodelil MJU skupaj z digitalnim potrdilom

requestid=id zahteve, ki jo tvori naročnik storitve

name=opcijsko opisno ime zahteve, ki se uporabniku prikaže v uporabniškem vmesniku.

Korak 2:

Uporabnik izvede podpis po uspešnem vstopu v aplikacijo CES-Sign. Če uporabnik nima veljavne seje, se mora avtenticirati na CAS-u za zahtevani nivo podpisa. Zahtevani nivo

Korak 3:

CES-Sign, vrne uporabnika nazaj v aplikacijo na mesto callback URL-ja. V posredovani zahtevi, ki jo CES-Sign posreduje prek 302 preusmeritve je podpisana vsebina:

https://www.somewhere.com/?requestid=1234567890&status=true&signed=2f66bd6dd66c4ddb39cac9ddbd57a4373176eed449f2ae17c3700df0b6319fcd8ac98a32a8cca80016652d5762df46447b4dafcf18017d0f36bcdb232a07dfecb293c865ee85328f0c66baf76e34d973dbb14ca5e979e3f0fe1ce44d9eb77e146f3d11aa7474a62a31bc98c988a1d4ed37138d69c54e4dec014ba94e5951c530

Parametri odgovora so:

requestid = id, ki ga je naročnik posredoval v GET zahtevi v prvem koraku.

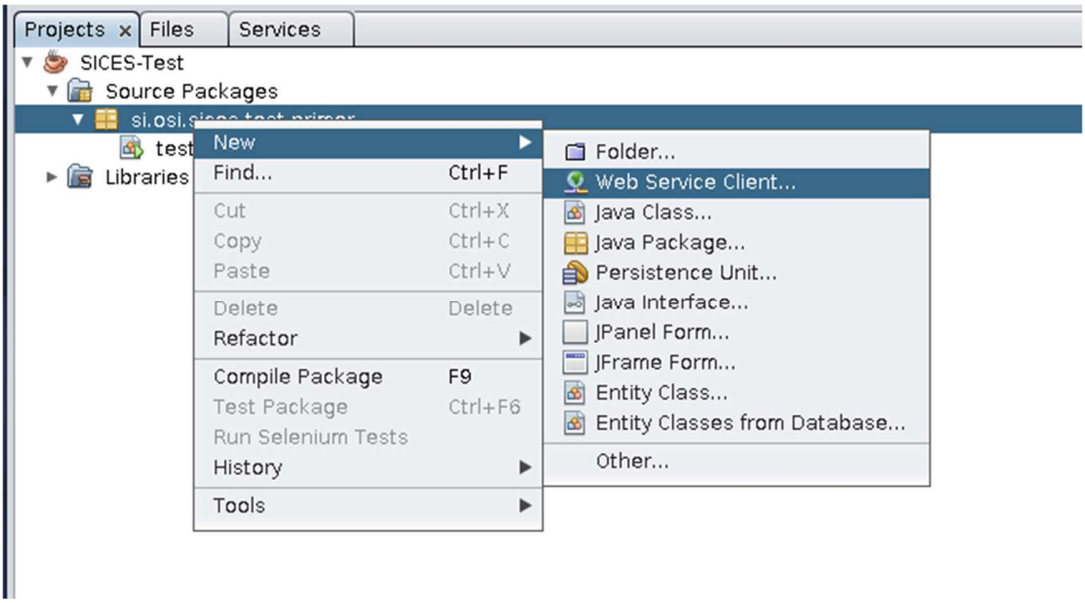
status = true | false : status true v primeru uspešnega podpisa

signed=podpisana vrednost

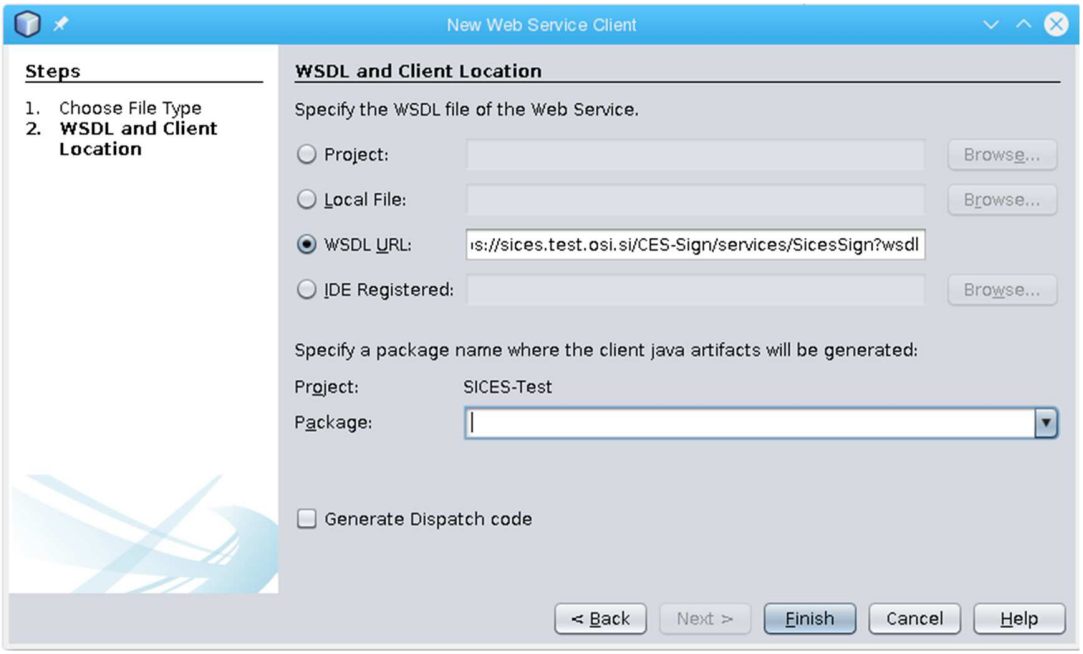
Vključitev spletnih metod v razvojna okolja

Vsa razvojna okolja omogočajo zelo enostavn način vključitve spletnega servisa v obstoječe ali nove projekte. Vsa orodja omogočajo vključitev na način dodajanja novega klienta za spletni servis. V nadaljevanju je slikovno prikazana vključitev v razvojna okolja NetBeans, Eclipse in Visual Studio.

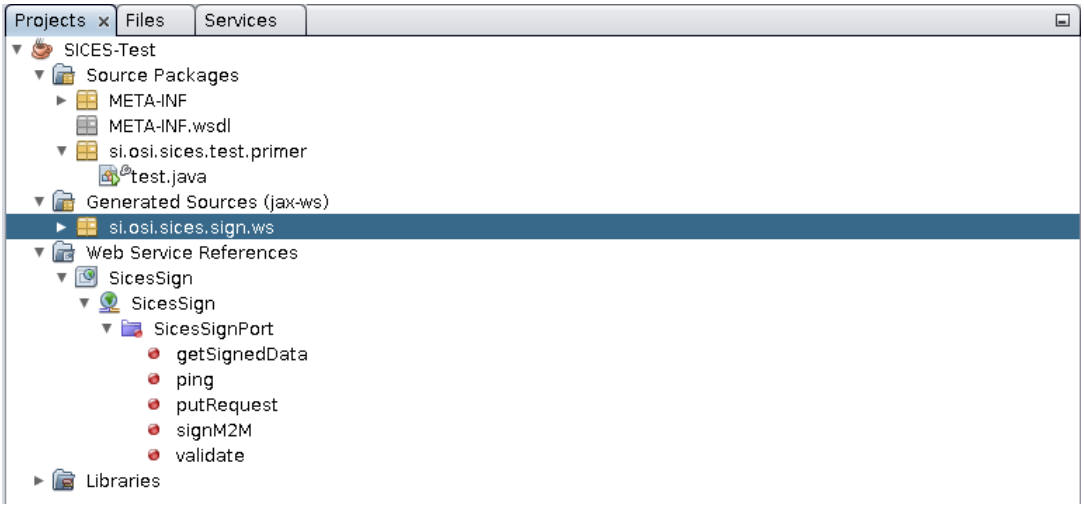
NetBeans



V projekt dodamo novega WS klienta s pomočjo čarovnika za dodajanje WS klientov (desni klik -> new -> web service client).

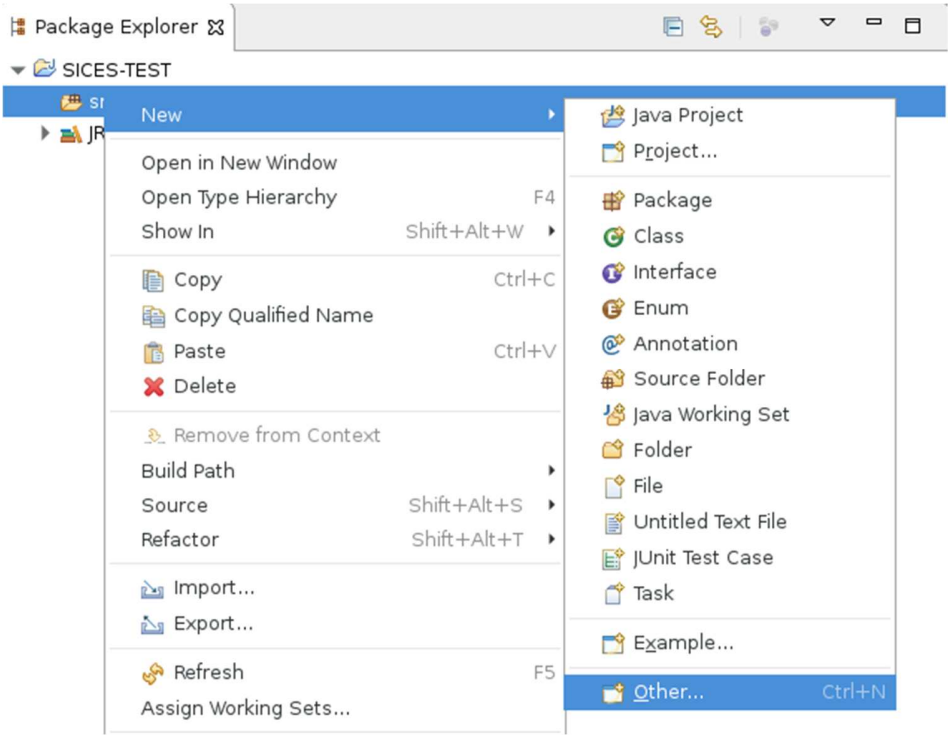


Vpišemo URL WSDL-ja, za katerega želimo narediti klienta->Finish.

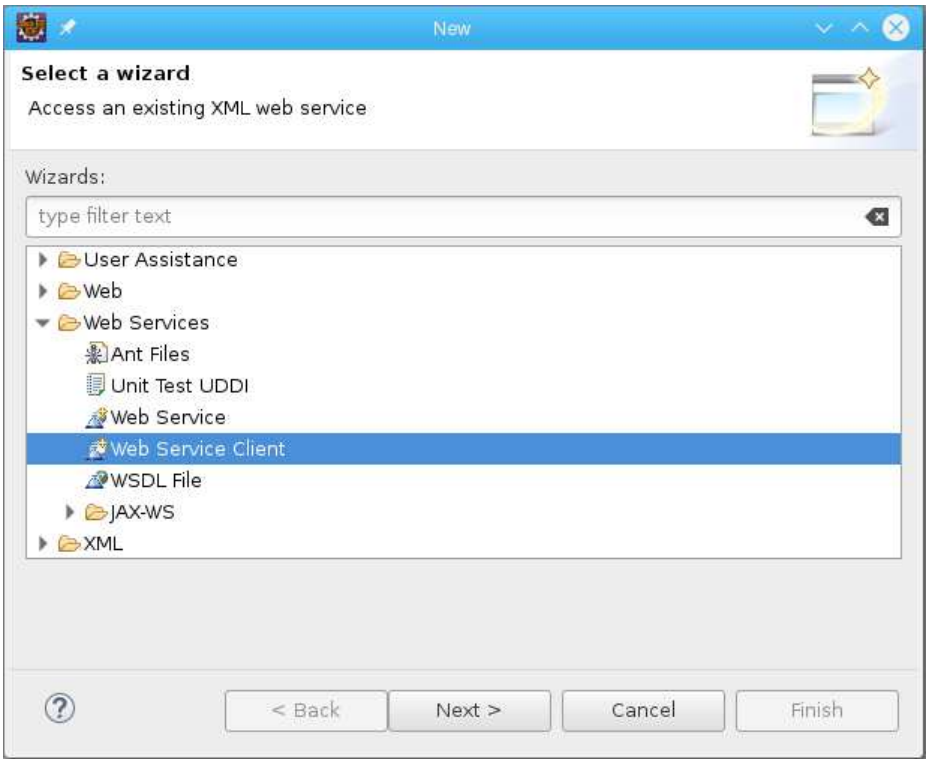


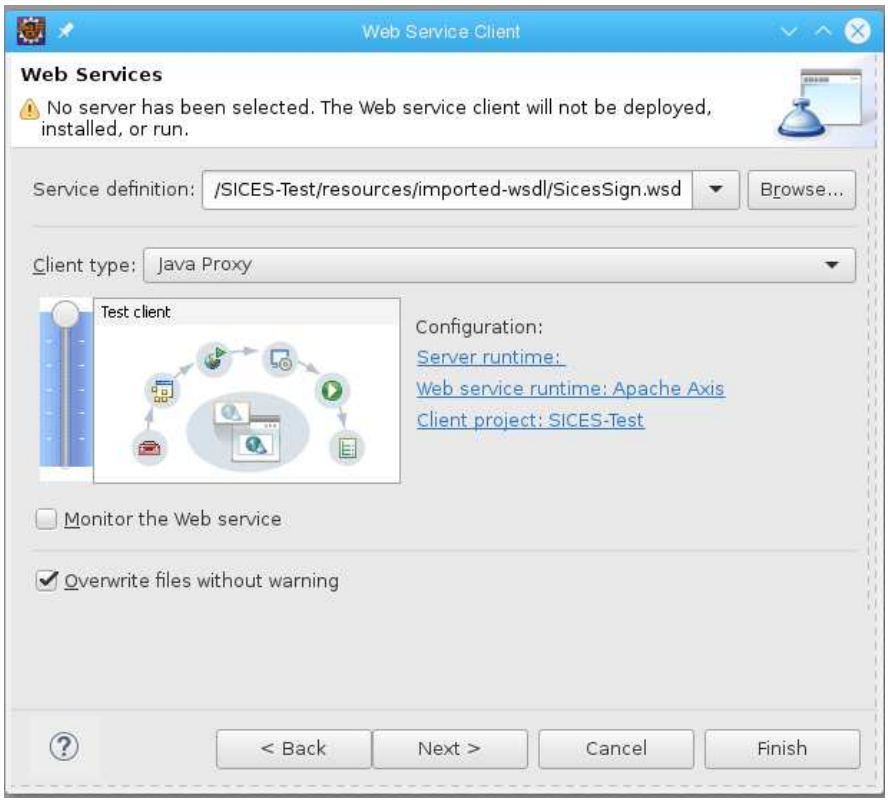
Čarovnik uvozi in generira vse potrebne datoteke.

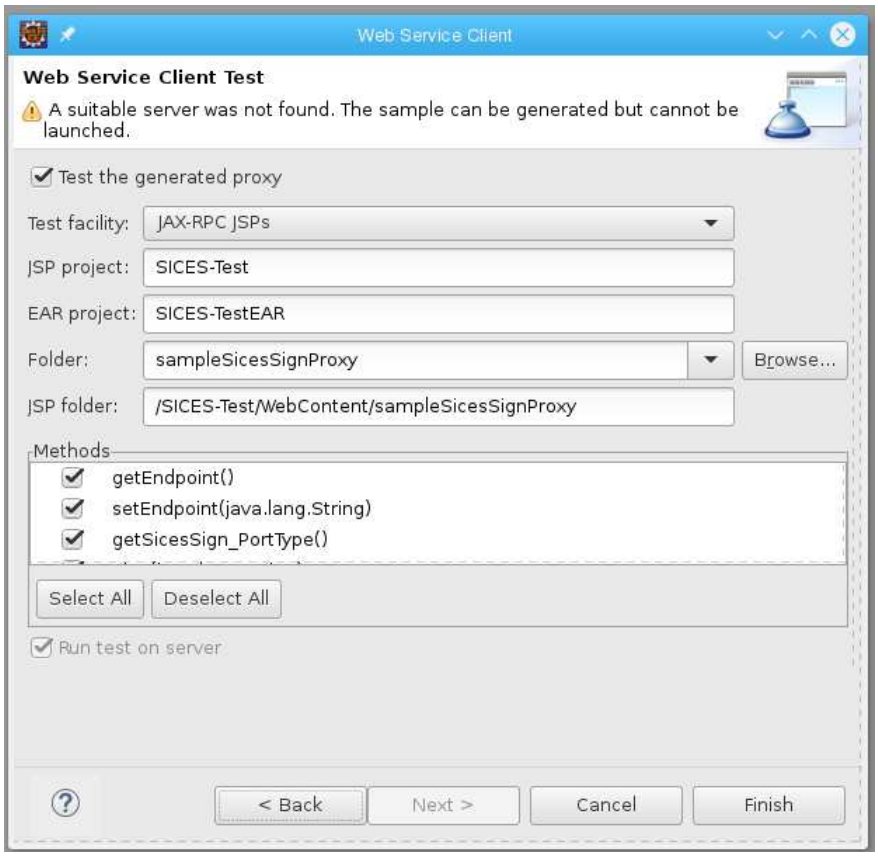
Eclipse



V projekt dodamo novega WS klienta s pomočjo čarovnika za dodajanje WS klientov.

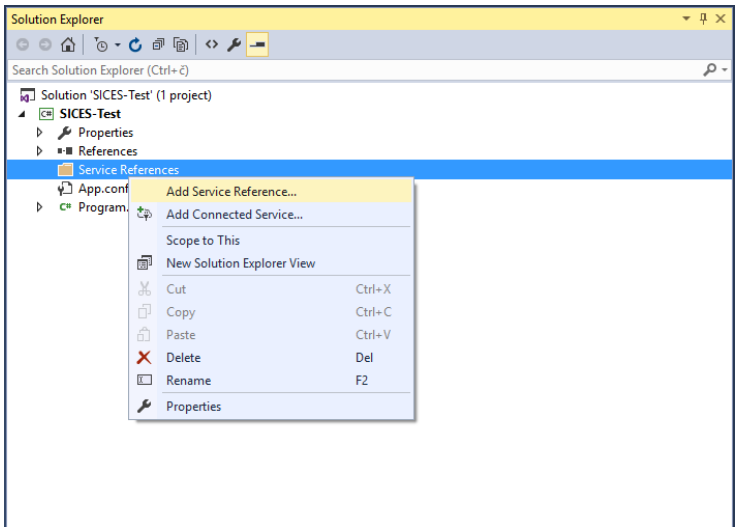

New
Select a wizard
Access an existing XML web service
Wizards:
type filter text
User Assistance
Web
Web Services
Ant Files
Unit Test UDDI
Web Service
Web Service Client
WSDL File
JAX-WS
XML
< Back
Next >
Cancel
Finish


Web Service Client
Web Services
No server has been selected. The Web service client will not be deployed, installed, or run.
Service definition:
/SICES-Test/resources/imported-wsdl/SicesSign.wsd
Browse...
Client type:
Java Proxy
Test client
Configuration:
Server runtime:
Web service runtime: Apache Axis
Client project: SICES-Test
Monitor the Web service
Overwrite files without warning
< Back
Next >
Cancel
Finish

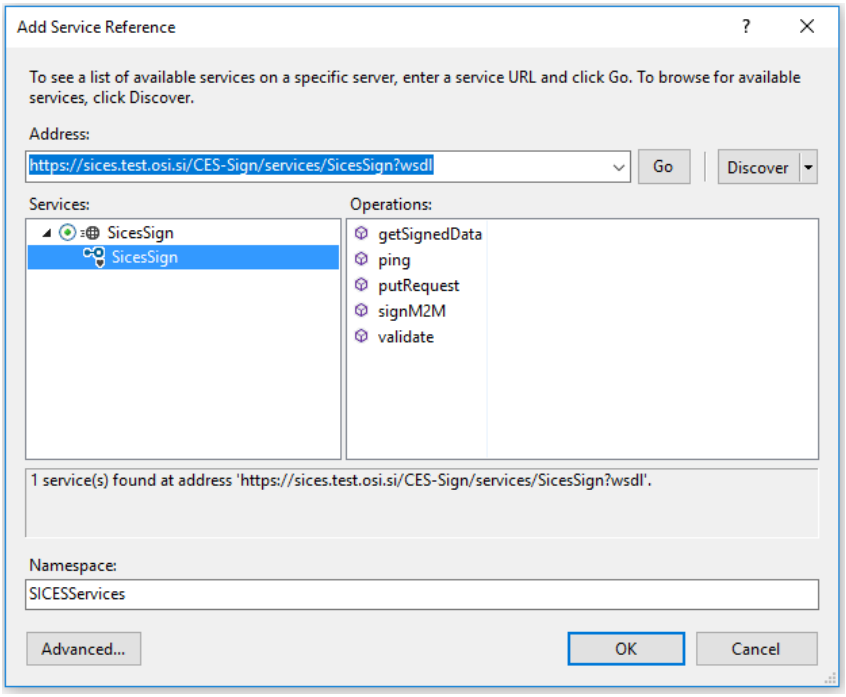


Omeniti velja, da je pri dodajnaju spletnega klienta v razvojno okolje Eclipse potrebno skopirati WSDL in shemo (XSD datoteko) na lokalni direktorij znotraj projekta ter ustrezno popraviti pot do sheme v WSDL datoteki.

Visual studio



V Solution Explorerju z desnim klikom na Service Reference izberemo dodajanje novega servisa.



Vpišemo le še URL WSDLja in kliknemo gumb Go ter gumb OK.