



Državni center za storitve zaupanja



SI-TRUST
Državni center za storitve zaupanja

NAVODILA ZA PRIKLOP NA SISTEM SI-CeS

navodila za razvijalce

veljavnost: od 4. marca 2018

verzija: 2.1

Pripravil: OSI d.o.o.



Kazalo

Integracija WS storitve e-podpisa v zunanjo aplikacijo	2 -
Uporaba SicesSign v zunanji aplikaciji	2 -
Predpogoja	2 -
Spletni naslov (URL) za dostop do WSDL opisa Si-CeS (WS) storitve	5 -
Opis Metod SicesSign (WS)	5 -
Metoda putRequest	5 -
Grafični prikaz podpisa na PDF dokumentu	10 -
Rezultat klica metode putRequest	16 -
Metoda getSIGNEDData	18 -
Rezultat klica metode getSIGNEDData	18 -
Metoda validate	21 -
Rezultat klica metode validate	21 -
Metoda ping	22 -
Metoda hasValidCertificates	22 -
Rezultat klica metode hasValidCertificates	22 -
Metoda confirmSignedData	23 -
Rezultat klica metode confirmSignedData	24 -
Metoda createCertificateRequest	25 -
Rezultat klica metode createCertificateRequest	25 -
Podpis posredovanega povzetka z uporabo GET metode(signHash)	27 -
Vključitev spletnih metod v razvojna okolja	28 -
NetBeans	28 -
Eclipse	30 -
Visual studio	32 -
Uporaba fontov za vizualni podpis	33 -



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

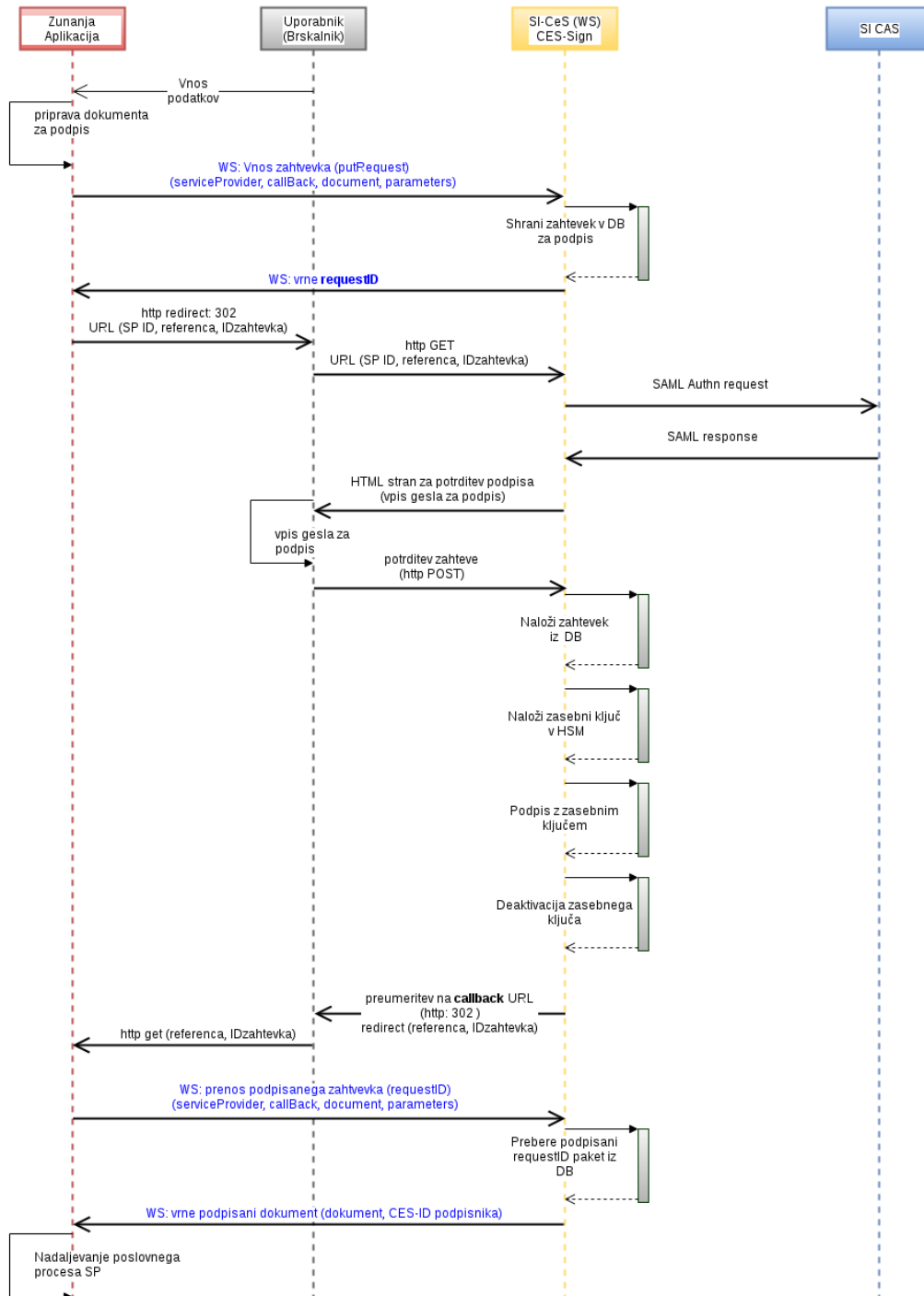
Predpogoja

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.





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 avtentificirati 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 tem 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
- **hasValidCertificates** – metoda, ki razvijalcu omogoči preveriti, če ima uporabnik ustrezno SI-PASS digitalno potrdilo za izvedbo željenega nivoja podpisa
- **createCertificateRequest** – metoda za kreiranje zahteve za izdajo digitalnega potrdila že želeni nivo podpisa
- **confirmSignedData** – metoda, ki razvijalcu omogoča potrditev prevzema podpisanega paketa

Metoda putRequest

Podatek	Števnost	Opomba
putRequest	1	Zahtevak
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[])
contentType	1	Mime tip
contentTypeString	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. <i>ref1</i>



uri		Oznaka elementa v XML dokumentu
visualSignature	1	Definicija pozicije grafičnega prikaza podpisa
visualSignatureImage	1	Slička v base64 kodirani obliki, ki je prikazna kot del grafičnega prikaza podpisa
includeSigningCertChain	1	Parameter, ki določa ali se v podpisu vključijo vsa digitalna potrdila: poleg podpisnega digitalnega potrdila, tudi vsa potrdila verige izdajateljev. Privzeto se v c/x/pADES vključuje celotna veriga, če pa
signerLocation	0-1	Kraj podpisnika
city	1	Mesto
country	1	Država
locality	1	Kraj
postalAddress	1-n	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

includeSigningCertChain Parameter, ki določa ali se v podpisu vključijo vsa digitalna potrdila: poleg podpisnega digitalnega potrdila, tudi vsa potrdila verige izdajateljev. Privzeto ima vrednost **true**, kar pomeni dosedanje delovanje. V primeru vrednosti **false** pa x/p/c/ADES podpis vključi v podpis le certifikat podpisnika, brez verige izdajateljev.

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>SPI</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 dokumenta ni prikazana)



```
<item>
  <document>
    <bytes>PHRlc3Q+CiAgPHBvZ29kYmEgawQ9InBvZDEiPmJsYWJsYSB4IDE8L3BvZ29kYmE+CiAgPHBvZ29kYmEgawQ9InBvZDIiPmJsYWJsYSB4IDI8L3BvZ29kYmE+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

```
<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/2wBDAAEBAQFBAYFBQYJBgUGCQsIBgY . . .
  </visualSignatureImage>
</parameters>
</item>
<trustLevel>Low</trustLevel>
</ws:putRequest>
</soapenv:Body>
</soapenv:Envelope>
```



Primer zahteve **putRequest** z vsebino zahteve, ki posreduje podatke za grafični prikaz elektronskega podpisa. Grafično vizualizacija podpisa je smiselna za PDF dokumente. Končna aplikacija, ki posreduje **putRequest** klic s parametroma *visualSignature* in *visualSignatureImage* posreduje podatke za vizualizacijo podpisa:

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

- *visualSignatureImage*: dodatna opsijska slička, ki se pripne na vizualizirani prikaz podpisa

Spodaj je primer prikaza vizualnega prikaza podpisa, pri čemer je slička 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.

DSS-detailed-Report-signed.pdf

Nek template

Podpisal Marko Šmid!
Dne 14.06.2017
od: CN=OSI TestCA001, O=osi.si,
dn: SURNAME=Šmid + SERIALNUM

b204e9800998ecf8427e

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

Vsebinska *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 kateri 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 dokumenta),
- "y":Y (podatek pozicije Y (vertikalno) grafične podobe na izbrani strani PDF dokumenta),
- "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" (slička).

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:

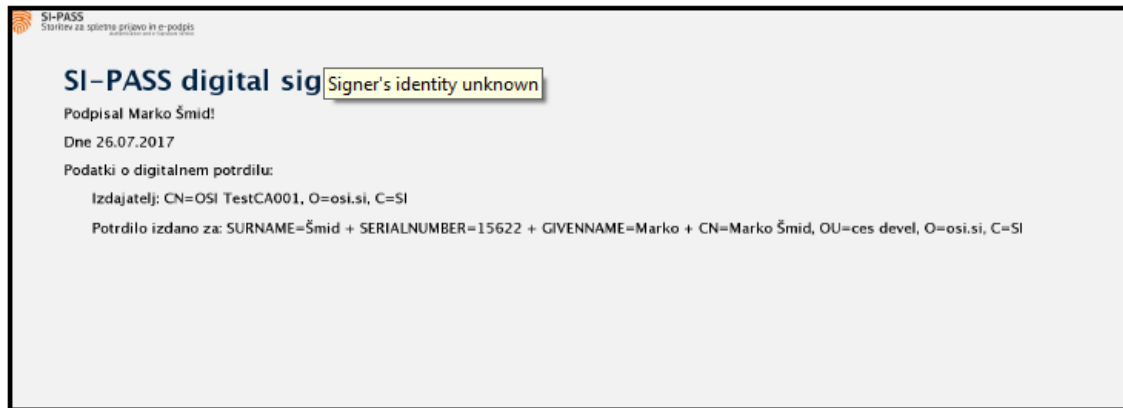
- x: odmik x v točkah od levega robu;
- y: odmik y v točkah od levega robu;
- data: tekst, ki bo prikazan v vrstici;
- font: font, ki bo uporabljen za prikaz teksta vrstice (uporabimo pdf poprte fonte);



- 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>iVBORwOKGgoAAAANSUHEUgAAAbIAAAA1CAAAAAksW7IA....

</visualSignatureImage>



Dinamične spremenljivke, ki se lahko uporabijo pri oblikovanju vizualnega podpisa so:

Ime spremenljivke	pomen
firstname	ime podpisnika
lastname	priimek podpisnika
ts	datum in čas podpisa, ki se lahko oblikuje pri izpisu s funkcijo date.format
issuer	DN izdajatelja digitalnega potrdila
issuer_cn	CN del celotne issuerDN vrednosti
subject	subjectDN lastnika digitalnega potrdila
subject_cn	CN del celotne subjectDN vrednosti
serial	serijska številka digitalnega potrdila

Vsa imena spremenljivk vsebujejo le male črke.

V predlogi besedila se te spremenljivke uporabijo s predpono \$, torej \$issuer_cn,....



```
<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>
```



Rezultat klica metode putRequest

Podatek	Števnost	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=ad2729f1fe388d6a1b1e6f85323be2737bd896366a2ae5a63ba4c621b0c46f3f5ac75855b057a6c857873ad21066613a09356b199cb1d90588d477b3a238c3cfe7284e2de6e8d81eb09415627daef4bdfc6e88c72bfd2d5cc98937fe6cf48207bee4b>
- **requestid**, ki predstavlja id podpisnega paketa v katerem so vsebovani elementi, ki smo

```
<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>
```



jih posredovali prek putRequest zahteve.

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	Števnost	Opomba
<code>getSignedData</code>	1	Zahtevek
<code>serviceProvider</code>	1	Enoznačna oznaka aplikacije
<code>requestId</code>	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>18c80afd450c4bd6e9e83bb75747069a9e97920fcef318e68139257e9a2d66b6f467649bce80c95ccfc467cc87f786f53645ab47e5fb697152bd73ff70ba6c36cfc8c0b8195cfab
      eea841a41c9a6401a260955cc1c59287944771640959fa9b0d8e2174da370959e3101ef2629818a77669ab279a4e959109232fa9ee3025fff6125291d2c0cb6a2053981bfebaa5b3 </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	Števnost	Opomba
<code>getSignedDataResponse</code>	1	Odgovor
<code>return</code>	1	Rezultat
<code>status</code>	1	Status podpisa
<code>cesId</code>	1	Id podpisnika
<code>document</code>	1-n	Dokument
<code>bytes</code>	1	Vsebina podpisanega dokumenta
<code>mimeType</code>	1	Mime tip
<code>mimeTypeString</code>	1	Oznaka mime tipa
<code>name</code>	1	Ime datoteke
<code>certificateChain</code>	1	Veriga potrdil
<code>certificate</code>	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 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>A5U2VyaWfsTnVtYmVpPjE1MDI3MzA1Mjc4NTMwMzA5MTMwMjI0MTE5ODU3MjYyOTI3NTYwMDYzMTYENdC3NDwvZHM6WDUwOVNlcmhlbE51bWJlcj48L3hhZGVzOkIzc3
          VlcNIcmhlbD48L3hhZGVzOkNlcQ+PC94YWRLczpTaWduaW5nQ2VydGhmaWNhdGU+.....
        </bytes>
        <mimeType>
          <mimeTypeString>text/xml</mimeTypeString>
        </mimeType>
        <name>A2.xml</name>
      </document>
      <certificateChain>
        <certificate>MIIFIDCCAwigAwIbAgIUIGJ6C5Mp5OATpGLOAAAAFWgUyYwDQYJKoZIhvcNAQELBQAwNjELMAkGA1UEBhMCU0kxZzANBgNVBAoTBm9zaS5zaTEWMBQGA1UEAxMN
        T1NlIFRlc3RDQTAwMTAeFw0xNTA5MjExOTQ4NDlaFw0xODA5MjEyMDE4NDlaMIGBMQswCQYDVQQGEwJTSTEPMA0GA1UEChMGb3NpLnNpMRIwEAYDVQQLEwljZXMgZGV2ZWwxdG90
        TAMBgNVBAQMBcWgbWlkMAwGA1UEKhhMFTWFya28wEgYDVQQDDAtN.....
        </certificate>
        <certificate>MIIFcJCCA1qgAwIbAgIUcvoeRE/yFY+VYzB8AAAAFWgSocwDQYJKoZIhvcNAQELBQAwNjELMAkGA1UEBhMCU0kxZzANBgNVBAoTBm9zaS5zaTEWMBQGA1UEAxMNT1
        NlIFRlc3RDQTAwMTAeFw0xNTA3MTAyMjE0MjFhFw0zNTA3MTAyMjQ0MjFhMDYxChZAJBgNVBAYTAiNlMQ8wDQYDVQQKEwZvc2kuc2kxZjAUBgNVBAMTDU9TS5BUZXR0Q0EwMDEw
        ggliMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDEKPSNq8hgPxt25e.....
        </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	Števnost	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 datoteke

```
<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	Števnost	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	Števnost	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	Števnost	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	Števnost	Opomba
<code>confirmSignedData</code>	1	Zahtevek
<code>requestId</code>	1	Enoznačen id podpisanega paketa, katere prevzem s tem klicem aplikacija potrjuje.
<code>success</code>	1	Z vrednostjo "true" aplikacija potrjuje uspešen prevzem.
<code>ServiceProvider</code>	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	Števnost	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>
```



Metoda createCertificateRequest

Podatek	Števnost	Opomba
createCertificateRequest	1	Zahtevek
serviceProvider	1	Enoznačna oznaka aplikacije
callback	1	Spletni naslov za preusmeritev po končani registraciji digitalnega potrdila
trustLevel	1	Nivo zaupanja

Metoda createCertificateRequest omogoča aplikaciji, da tvori prek SicesSign WS storitve, zahtevek za tvorbo digitalnega potrdila. WS storitev ob uspešnem sprejemu zahteve za tvorbo strežniškega podpisnega digitalnega potrdila vrne id zahteve in URL. URL je namenjen preusmeritvi uporabnika na CES-RM registracijski modul. Aplikacija uporabnika preusmeri na vrnejni URL s http 302 odgovorom.

ServiceProvider vhodni podatek je ime, ki ga ponudniku/aplikaciji dodeli ponudnik storitve SI-PASS.

Callback vhodni podatek je URL na katerem pričakuje aplikacija uporabnika po končani registraciji.

TrustLevel je vhodni podatek z zalogo vrednosti (spodaj), ki vsebuje nivo želenega potrdila:

- LOW: nekvalificirano potrdilo
- MEDIUM: kvalificirano potrdilo
- HIGH: potrdilo za kvalificirani podpisa
-

Zaloge vrednosti

trustLevel: LOW, MEDIUM, HIGH

Rezultat klica metode createCertificateRequest

Podatek	Števnost	Opomba
createCertificateRequest	1	Odgovor
return	1	Sestavljeni odgovor
requestId	1	Id zahteve za tvorbo digitalnega potrdila
URL	1	URL, ki kaže na CES-RM vhod za preusmeritve uporabnika, ki bo po ustrezni avtentikaciji lahko registriral potrdilo.

Primer rezultata klica metode putRequest



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

- **requestId:** id, ki ga tvori SicesSign ob uspešnem sprejemu zahteve
- **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.sigov.si/CES-RM/medium/requestws.htm?requestid=3456ergdfhgrkztoeizterighsdkgldkfgkl>

Končna aplikacija uporabi URL v odgovoru in uporabnika s 302 http odgovorm preusmeri na ta URL.

Po uspešni ali neuspešni registraciji digitalnega potrdila bo CES-RM preusmeril uporabnika nazaj na *callback* URL, pri čemer je v URL-ju dodan parameter *status*, ki vsebuje status tvorbe strežniškega digitalnega potrdila. V primeru *status=true*, je bilo potrdilo uspešno registrirano, v primeru *status=false* pa digitalno potrdilo ni bilo registrirano, bodisi zaradi neizpolnjenih pogojev za registracijo, bodisi zaradi sistemske napake.



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://somesomewhere.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.somesomewhere.com/?requestid=1234567890&status=true&signed=2f66bd6dd66c4ddb39cac9ddbd57a4373176eed449f2ae17c3700df0b6319fcd8ac98a32a8cca80016652d5762df46447b4dafcf18017d0f36bcd5232a07dfecb293c865ee85328f0c66baf76e34d973dbb14ca5e979e3f0fe1ce44d9eb77e146f3d11aa7474a62a31bc98c988a1d4ed37138d69c54e4dec014ba94e5951c530>

Parametri odgovora so:



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

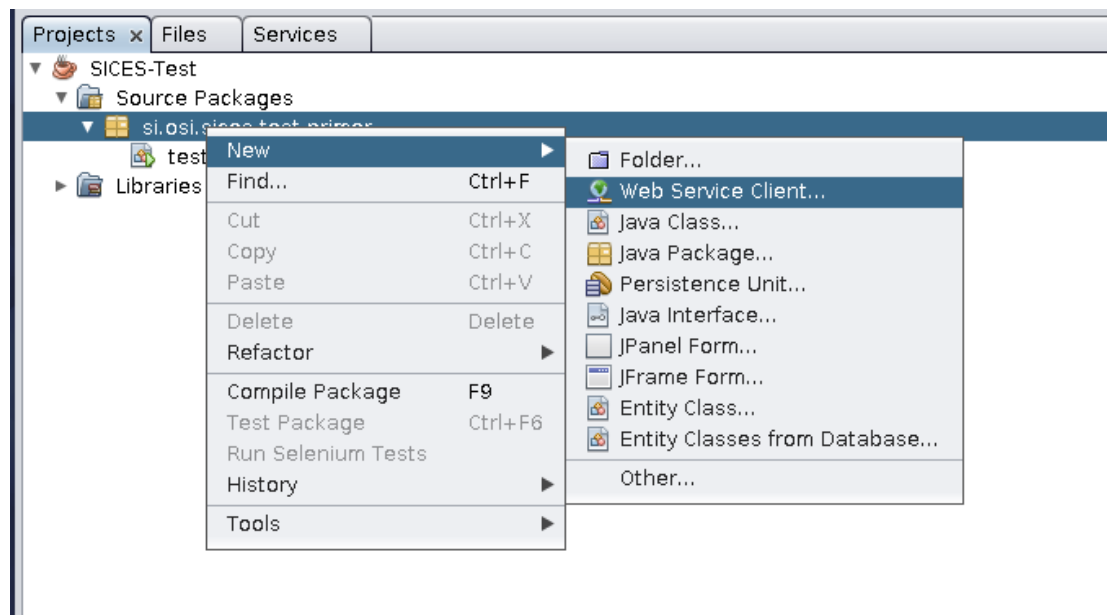
status = true | false : status true v primeru uspešnega podpisa

signed=podpisana vrednost

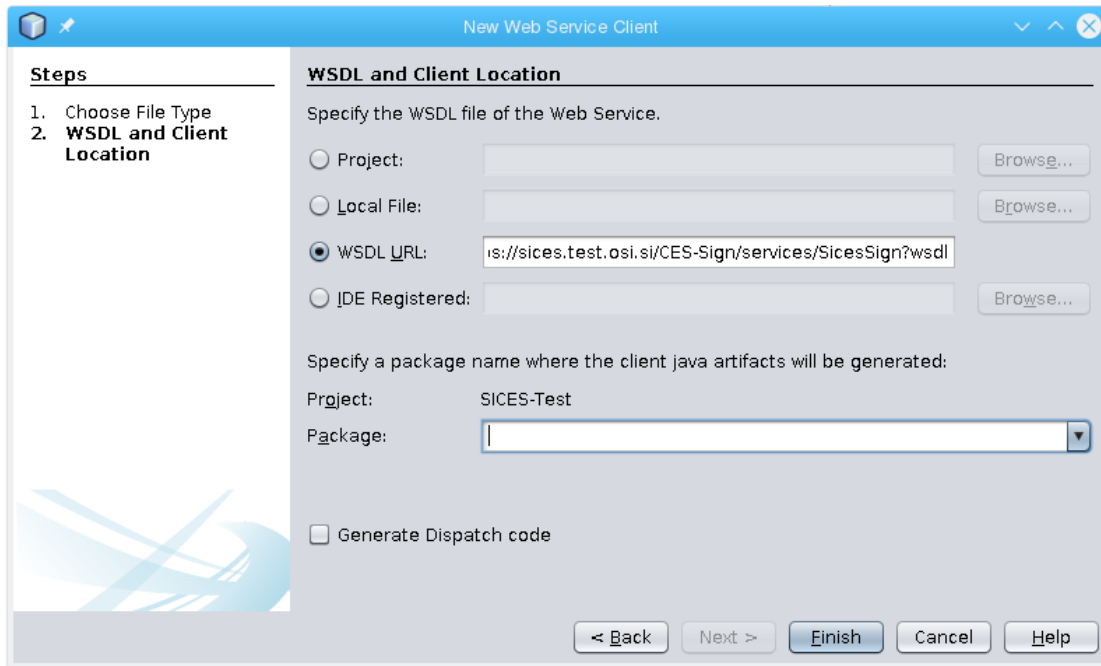
Vključitev spletnih metod v razvojna okolja

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.

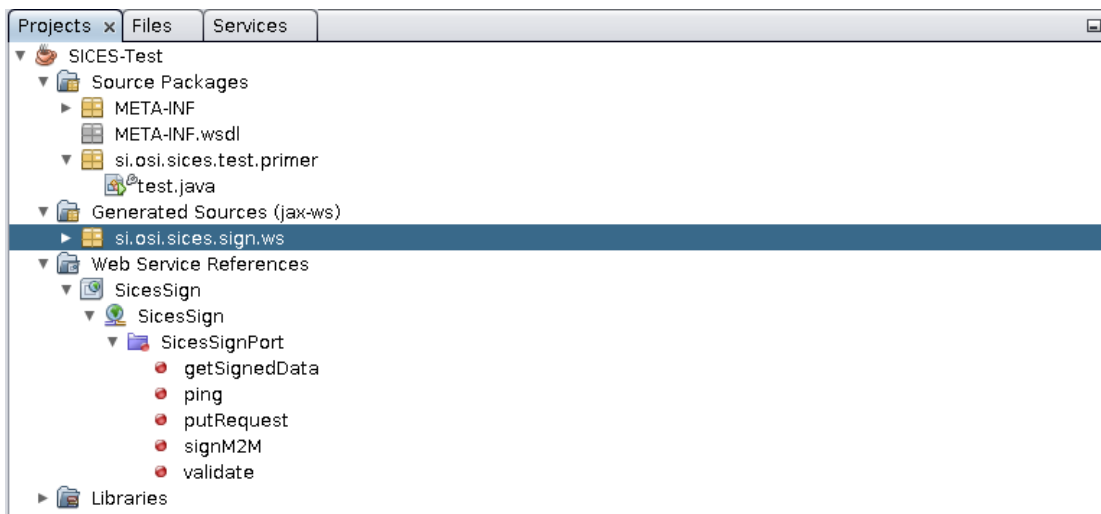
NetBeans



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



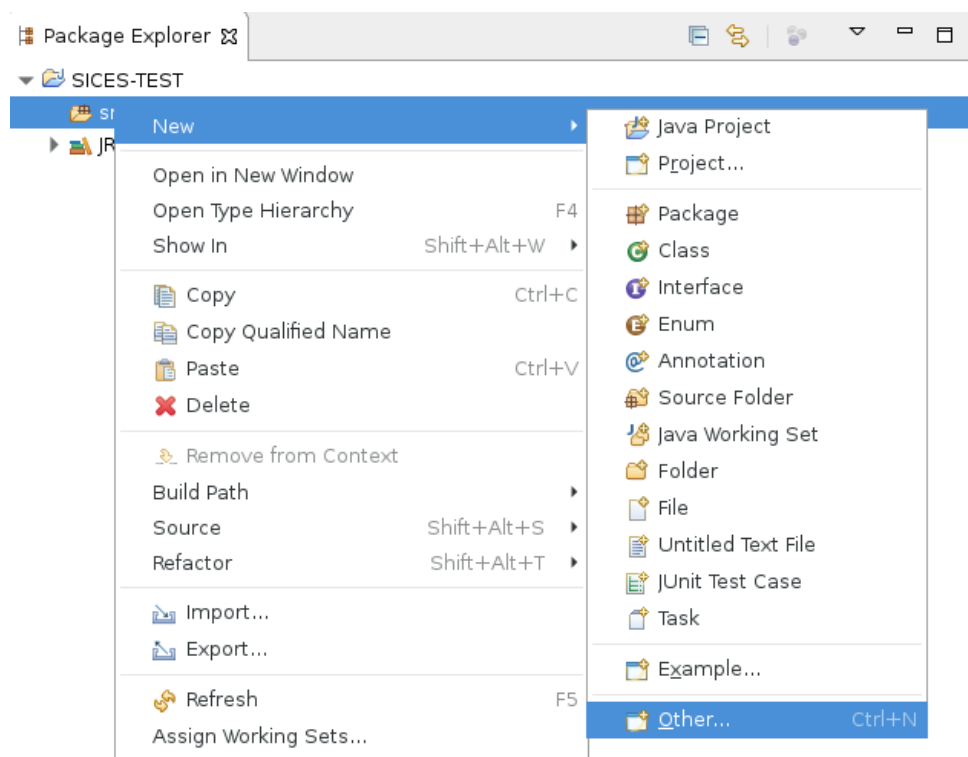
Vpišemo URL WSDL-ja, za katerega želimo narediti klienta->Finish.



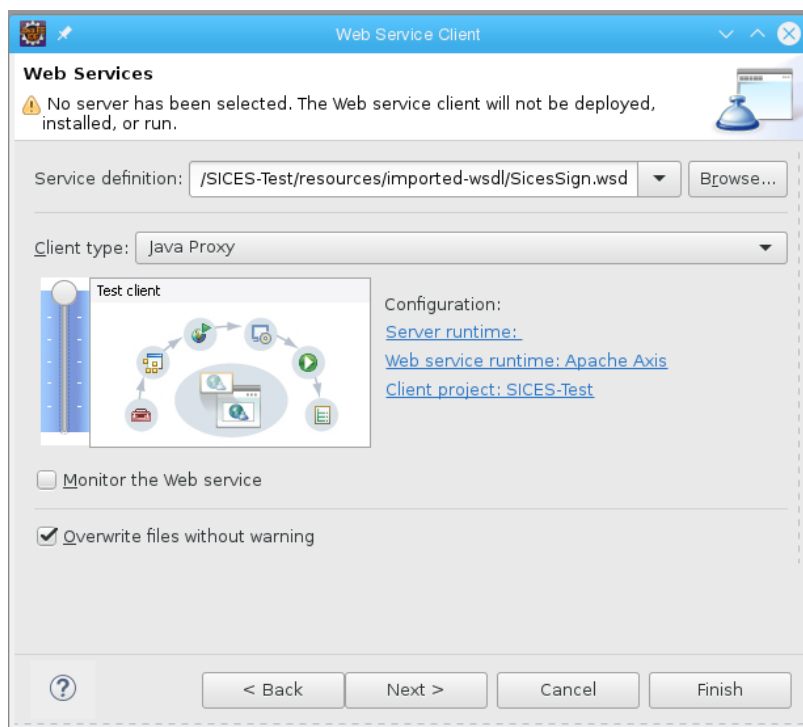
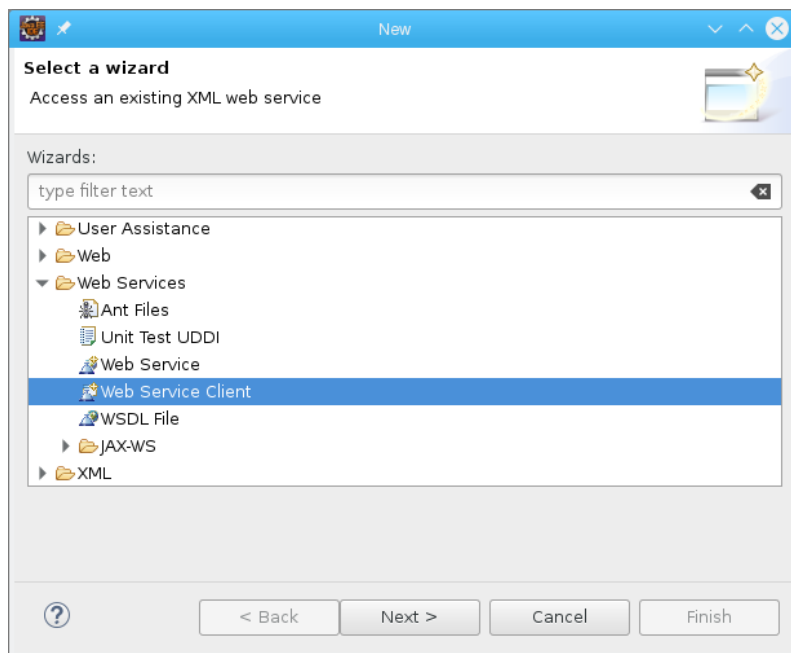
Čarovnik uvozi in generira vse potrebne datoteke.

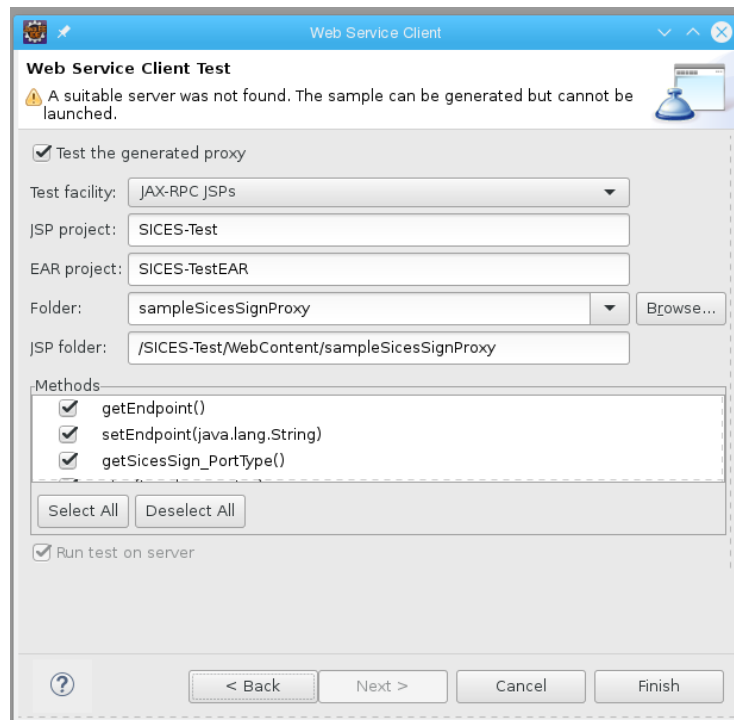


Eclipse



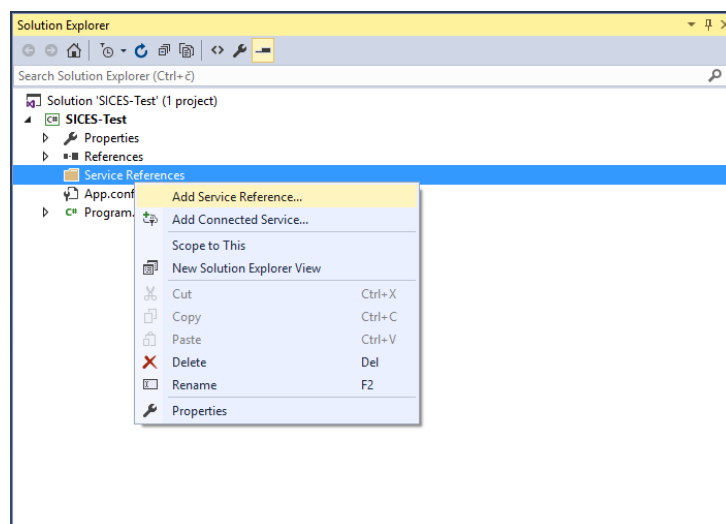
V projekt dodamo novega WS klienta s pomočjo čarovnika za dodajanje WS klientov.



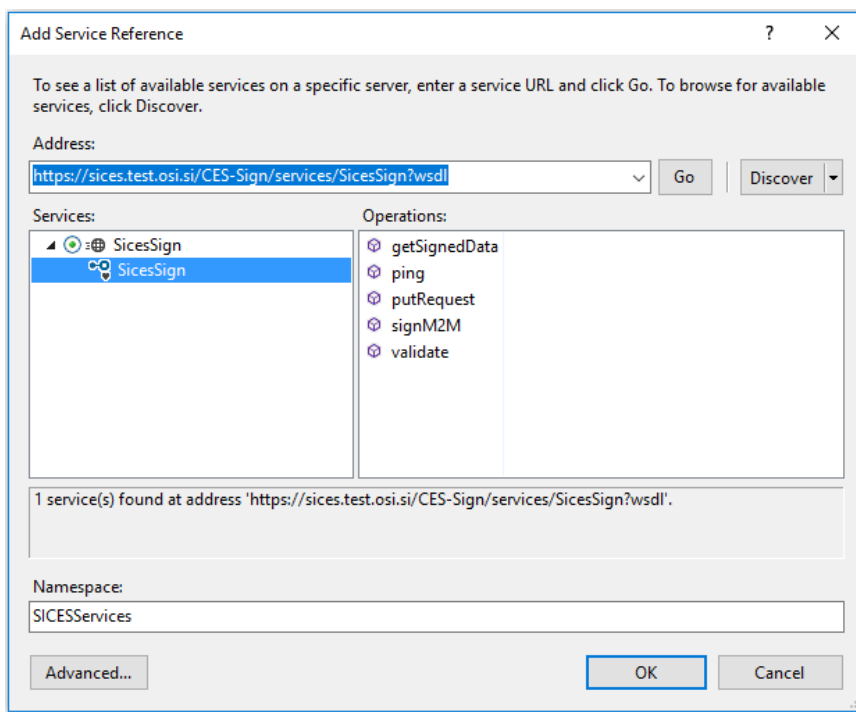


Omeniti velja, da je pri dodajanju spletnega klienta v razvojno okolje Eclipse potrebno skopirati WSDL in shemo (XSD datoteko) na lokalni direktorij znotraj projekta ter ustrezno popraviti pot do sheme v WSDL datoteki.

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.

Uporaba fontov za vizualni podpis

Vizualni podpis v PDF dokumentu vsebuje fonte, ki jih podpira operacijski sistem SicesSign storitve. Seznam podprtih fontov je na voljo pri naročniku.