SecuSign

Technická dokumentace SDK pro webové služby a .NET rozhraní

Aktualizováno
30.03.2022

Software602 a. s.
Hornokrčská 15
140 00 Praha 4

IČO: 63078236
DIČ: CZ63078236

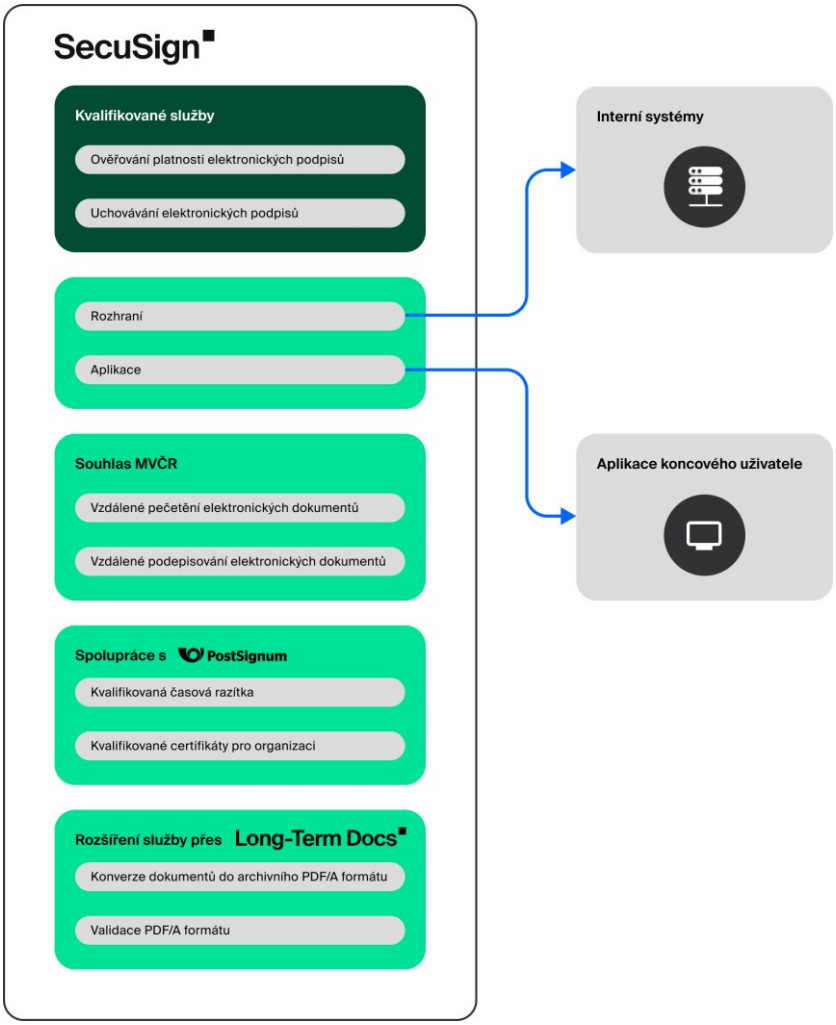
www.602.cz
e-mail: info@602.cz
ID datové schránky: 7dcsfzg

Telefon: +420 222 011 602
Helpdesk: +420 222 011 254

Obsah

1 Služby SecuSign - digitální důvěra kvalifikovaně

Kvalifikované služby vytvářející důvěru ve shodě s Nařízením eIDAS přinášejí bezpečí pro všechny organizace, které pracují s elektronickým podpisem nebo pečetí. SecuSign – služby, za které neseme zodpovědnost.



1.1 Kvalifikované služby SecuSign vytvářející důvěru

Uvedené služby jsou poskytovány v rámci dodávaného SDK.

1.1.1 Ověřování podpisů

Kvalifikovaná služba ověřování zajistí pro vaše systémy úplné a správné ověření platnosti podepsaných dokumentů a dat. V souladu s evropskou legislativou a respektováním českého právního prostředí.

1.1.2 Uchovávání podpisů

Elektronické podpisy je třeba udržovat. Vyhněte se výměně celých systémů a stávajících úložišť. Uchovávejte elektronické podpisy v souladu s eIDAS s kvalifikovanou službou SecuSign.

1.2 Další služby SecuSign vytvářející důvěru

Uvedené služby jsou poskytovány v rámci dodávaného SDK, případně přímým voláním vzdálené služby.

1.2.1 Podpis a pečeť podle eIDAS

Služby SecuSign umožní správně vytvářet elektronické dokumenty (pečeť, podpis, razítko), zejména při výstupu z organizace. Certifikát podpisu a pečeti je bezpečně umístěn v kvalifikovaném prostředku HSM v prostředí O2 (Tier III), nebo Key Vault v prostředí Microsoft Azure (pouze pro pečeť).

1.2.2 Konverzní a jiné služby - vždy čitelné PDF/A dokumenty

Součástí služeb je i zajištění dlouhodobé čitelnosti PDF dokumentů konverzí do PDF/A podle všech specifikací. Centrální konverzní server (LTD SDK) poskytuje i autorizovanou konverzi z moci úřední s autentizací přes JIP/KAAS.

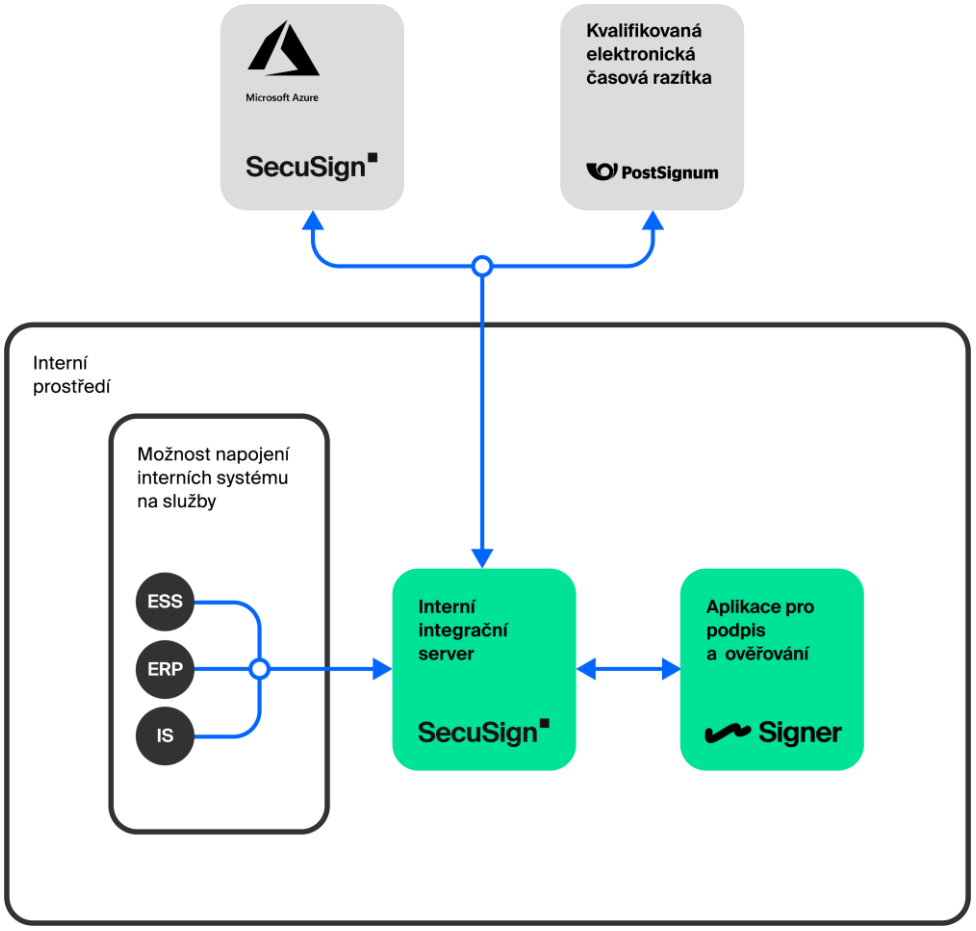
1.3 Rozhraní a aplikace

Celý ekosystém rozhraní a aplikací je nastaven tak, že služby je možné čerpat přímo z libovolných informačních systémů. Díky auditovanému integračnímu SDK dokumenty neopouštějí perimetr klienta.

SecuSign SDK umožňuje integraci funkcí a operací nad dokumenty pomocí následujících rozhraní:

- Webové služby (SOAP)
- .NET

.NET knihovny (`SecuSign_NET.dll` a další) jsou obsaženy po instalaci SDK v instalačním adresáři. Rozhraní .NET metod je opatřeno komentáři ve formě XML dokumentace (`SecuSign_NET.xml`). Většina metod .NET assembly má stejné rozhraní jako metody webových služeb, které jsou detailně popsány níže. Díky tomu je snadná integrace do jiných informačních systémů či webových aplikací.



2 Pojmy a zkratky

- **eIDAS** – zkratka pro nařízení Evropské unie č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu. Toto nařízení ruší směrnici Evropské unie 1999/93/EC. Aktuální a platná verze eIDAS byla publikována Evropským parlamentem a Evropskou radou dne 23. 7. 2014.
- **ETSI** - Evropský ústav pro telekomunikační normy, anglicky European Telecommunications Standards Institute (ETSI), je nezávislá, nezisková organizace pro standardizaci informačních a komunikačních technologií (ICT) v Evropě s celosvětovým dosahem.
- **HTTPS** - HTTPS (Hypertext Transfer Protocol Secure) je v informatice protokol umožňující zabezpečenou komunikaci v počítačové síti. HTTPS využívá protokol HTTP spolu s protokolem SSL nebo TLS. HTTPS je využíván především pro komunikaci webového prohlížeče s webovým serverem. Zajišťuje autentizaci, důvěrnost přenášených dat a jejich integritu. Standardní port na straně serveru je 443 TCP.
- **ISO** – Mezinárodní organizace pro normalizaci se zabývá tvorbou mezinárodních norem (ISO) a jiných druhů dokumentů ve všech oblastech normalizace kromě elektrotechniky.
- **PAdES** – elektronicky podepsané PDF dokumenty podle normy ISO-32000-1 nebo standardů rodiny PAdES[4][8].
- **CMS, PKCS7, CAdES** – elektronicky podepsaná (interně i externě) obecná data ve formátu CMS/PKCS7/CAdES. Může se například jednat o podepsanou emailovou komunikaci, audio nebo video záznamy apod. Jedním z příkladů interně podepsaných dat podle CAdES[5][10] jsou také Datové zprávy ISDS.
- **XAdES** – elektronicky podepsané XML dokumenty podle standardu rodiny XAdES[3][9][11].

- **PDF** – souborový formát pro ukládání dokumentů nezávisle na software a hardware, na kterém byly pořízeny. Řízen normou ISO 32000-1:2008.
- **PDF/A** – oficiální archivační verze souborového formátu PDF. Jedná se o zúžení definice formátu PDF tak, aby bylo možné soubory uložené v PDF/A otevřít beze ztráty informace i všemi budoucími verzemi softwarových nástrojů. Definována v standardech ISO 19005:1-2008, ISO 19005-2:2011 a ISO 19005-3:2012.
- **Dokument** – podepsaný PDF dokument nebo jiná podepsaná data.
- **ISDOC** – Information System Document - formát elektronické fakturace v ČR
- **ISDS** – Informační systém datových schránek
- **OID** – zkratka Object Identifier ve výpočetní technice jsou identifikátory objektů nebo li OID mechanismem identifikace, který je standardizován Mezinárodní telekomunikační unií (ITU) a ISO / IEC pro pojmenování jakéhokoli objektu, koncepce nebo "věci" s globálně jednoznačným trvalým názvem.
- **OCSP** –Online Certificate Status Protocol (OCSP) je internetový protokol používaný pro získání stavu odvolání digitálního certifikátu X.509. Je popsán ve standardu RFC 6960[13]. Byla vytvořen jako alternativa k seznamům zneplatněných certifikátů (CRL), konkrétně řeší určité problémy spojené s používáním CRL v infrastruktuře veřejného klíče (PKI).
- **602 ID** – registrovaný účet uživatele (zákazníka), na kterém jsou aktivovány zakoupené služby a produkty.
- **SDK** - Software development kit je typicky sada vývojových nástrojů umožňující vytváření aplikací pro jisté softwarové balíčky, frameworky, platformy, počítačové systémy, herní konzole, operační systémy nebo podobnou platformu.
- **TSL** – Trusted List je Seznam důvěryhodných vydavatelů certifikátů (kvalifikovaných poskytovatelů služeb vytvářejících důvěru)
- **HSM** – Hardware Security Module, bezpečný prostředek pro šifrování a správu generovaných a ukládaných klíčů (privátních, veřejných) certifikátů.
- **Certifikát -** Datová struktura X509 obsahující veřejný klíč spolu s údaji o držiteli klíče, vydavateli klíče, dovoleném způsobu užití a další relevantní informace definované příslušející politice CA.
- **CA** - Certifikační autorita, poskytovatel služeb elektronických certifikátů pro elektronický podpis/pečeť/razítka/certifikáty webových stránek.
- **TLS** - Transport Layer Security a jeho předchůdce Secure Sockets Layer (SSL) jsou kryptografické protokoly, poskytující možnost zabezpečené komunikace na Internetu pro služby jako WWW, elektronická pošta, internetový fax a další datové přenosy.
- **URI** - Uniform Resource Identifier - česky „jednotný identifikátor zdroje“ - je textový řetězec s definovanou strukturou, který slouží k přesné specifikaci zdroje informací (ve smyslu dokument nebo služba), hlavně za účelem jejich použití pomocí počítačové sítě, zejména Internetu.
- **WSDL** – Web Services Description Language je jazykem pro popis funkcí, jež nabízí tzv. webová služba, a dále pro popis vstupů a výstupů těchto funkcí (jinými slovy, co webová služba poskytuje a jak si o to říci). Jelikož webová služba v principu komunikuje protokolem SOAP, WSDL zpravidla popisuje SOAP komunikaci. WSDL vychází z formátu XML.
- **PSD2** - PSD2 je zkratka pro Payment Service Directive 2 (Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu), která nahrazuje předchozí směrnici. Více informací o směrnici naleznete zde.
- **QTSP** – Qualified Trust Service Provider, kvalifikovaný poskytovatel služeb vytvářejících důvěru jak jej stanovuje eIDAS (č. 910/2014) a národní legislativa (pro ČR č. 297/2016 Sb.)

3 Reference

[1] ETSI EN 319 102-1 v1.0.0 – Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures
[2] ETSI EN 319 102-1 v1.1.1 – Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures
[3] ETSI TS 103 171 – Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile
[4] ETSI TS 103 172 - Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile
[5] ETSI TS 103 173 - Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile
[6] ETSI TS 103 174 - Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile
[7] ETSI TS 319 401 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Provider
[8] ETSI EN 319 142-1 - Electronic Signatures and Infrastructures (ESI); PAdES Digital Signatures
[9] ETSI EN 319 132 - Electronic Signatures and Infrastructures (ESI); XAdES Digital Signatures
[10] ETSI EN 319 122 - Electronic Signatures and Infrastructures (ESI); CAdES Digital Signatures
[11] ETSI EN 319 162 - Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)
[12] RFC3647 – Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework
[13] RFC 6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP
[14] ETSI TS 119 495 V1.4.1 - Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366

4 Technické a bezpečnostní požadavky

- 64-bitový operační systém Microsoft Windows Server 2012 R2, Windows Server 2016 nebo Windows Server 2019
- Dvou nebo více jádrový procesor na frekvenci 3 GHz nebo vyšší
- Webový Server (IIS)
- ASP.NET 4.6 nebo vyšší
- .NET Framework 4.6.2 nebo vyšší
- Webové služby běžící na protokolu HTTPS a zamezení neoprávněným přístupům k serveru (mj. autentizací s dostatečně silným heslem)

Vzhledem k zajištění vysoké prostupnosti je vhodné zajistit adekvátní velikost operační paměti RAM a rychlost komunikačních rozhraní. Detailněji bude specifikováno v příloze ke smlouvě.

Pro správnou funkčnost SecuSign SDK je zapotřebí, aby server (popřípadě firewall, proxy, apod.) nebránil komunikaci s následujícími adresami a porty:

Prostředí	Doménové jméno	IP adresa	Port	Protokol
PROD (QS)	awsc.secusign.cz	13.73.167.130	443	https

PROD (HSM)	rsm.secusign.eu	194.228.175.135	443	https
TEST (QS)	awsctest.secusign.cz	52.178.28.175	443	https
TEST (HSM)	rsmtest.secusign.eu	194.228.175.135	443	https

V případě povolené kontroly revokace certifikátu vzdáleného serveru je třeba mít povolenou adresu distribučního místa vystavitele zprostředkujícího certifikátu (Thawte RSA CA 2018) a vystavitele kořenového certifikátu (DigiCert Global Root CA):

Doménové jméno	IP adresa	Port	Protokol
cdp.thawte.com	93.184.220.29	80	http
crl3.digicert.com	93.184.220.29	80	http

4.1 Související požadavky

Licenční certifikát pro autentizaci, vydaný Software602 a.s. ke konzumaci zakoupených služeb.

Vytvořený a aktivní uživatelský účet na portálu 602 ID, ke kterému je aktivován licenční certifikát pro konzumaci zakoupených služeb.

5 Kvalifikovaná služba ověřování elektronických podpisů

Kvalifikovaná služba ověřování elektronických podpisů umožňuje ověřit platnost elektronických podpisů, pečetí, časových razítek v podepsaném dokumentu, včetně dokumentu podepsaného externím podpisem, a dat. Akceptované formáty podpisů jsou v souladu s požadavky na rozšířený formát elektronického podpisu definovaného dle ETSI, nelze ověřit formáty typu DOC či XLS.

Ověření je prováděno vůči OCSP nebo odpovídajícím CRL listům, které poskytují kvalifikovaní poskytovatelé služeb vytvářejících důvěru, jež jsou uvedeni na EU Trust Listu.

5.1 Název metody: Validate

Popis služby včetně WSDL schématu a příklad požadavku a odpovědi pro SOAP 1.1 a SOAP 1.2 je umístěn na https://localhost/secusign/default.asmx?op=Validate *

* localhost je název používaný pro lokální počítač; namísto něj zvolte jméno/IP adresu SDK serveru (dle nastavení v IIS)

5.1.1 Požadavek v rozhraní SOAP 1.1

```
POST /secusign/default.asmx HTTP/1.1
Host: localhost
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://software602.com/secusign/Validate"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <Validate xmlns="http://software602.com/secusign/">
      <FileName>string</FileName>
      <FileData>base64Binary</FileData>
      <FileType>UNKNOWN or CMSPKCS7 or CMSPKCS7Ext or PDF or XML or XML602FORM or
XMLISDOC or ASiC_S_CAdES or ASiC_S_XAdES or ASiC_S_Tst or ASiC_E_CAdES_Tst or
ASiC_E_XAdES or MS_WORD or MS_EXCEL or MS_PWR_PNT or ODF or EML or MSG
</FileType>
      <ExternalSignatureFileName>string</ExternalSignatureFileName>
      <ExternalSignature>base64Binary</ExternalSignature>
      <Properties>
        <ReportLanguage>string</ReportLanguage>
        <GetReport>boolean</GetReport>
        <GetXMLReport>boolean</GetXMLReport>
        <GetHTMLReport>boolean</GetHTMLReport>
        <GetPDFReport>boolean</GetPDFReport>
        <ValidationTime>dateTime</ValidationTime>
        <IgnoreNoPOE>boolean</IgnoreNoPOE>
        <UseClaimedTimeIfNoTS>boolean</UseClaimedTimeIfNoTS>
        <DontUseGracePeriodForQCerts>boolean</DontUseGracePeriodForQCerts>
      </Properties>
      <Params>string</Params>
    </Validate>
  </soap:Body>
</soap:Envelope>
```

5.1.2 Vstupní parametry metody

5.1.2.1 <FileName>

[povinný element]

Vstup	Popis
String	Název vstupního souboru (včetně přípony), který se má ověřit. Příklad: Dokument.pdf Max. 260 znaků.

5.1.2.2 <FileData>

[povinný element]

Vstup	Popis
Base64Binary	Data vstupního souboru kódovaná v Base64

5.1.2.3 <FileType>

[povinný element]

Vstup	Popis
UNKNOWN	Neznámý typ dokumentu
CMSPKCS7	Dokument podepsaný interním CMS/PKCS7 podpisem
CMSPKCS7Ext	Dokument podepsaný externím CMS/PKCS7 podpisem
PDF	PDF dokument
XML	XML data
XML602FORM	Datové zprávy z Informačního systému datových schránek a FO/ZFO formuláře aplikace Software602 Form Filler
XMLISDOC	XML ISDOC data
ASiC_S_CAdES	ASiC-Simple s CAdES podpisem
ASiC_S_XAdES	ASiC-Simple s XAdES podpisem
ASiC_S_Tst	ASiC-Simple s Timestamp
ASiC_E_CAdES_Tst	ASiC-Extended s CAdES podpisem nebo s Timestamp
ASiC_E_XAdES	ASiC-Extended s XAdES podpisem
MS_WORD	Dokument aplikace MS Word
MS_EXCEL	Dokument aplikace MS Excel
MS_PWR_PNT	Dokument aplikace MS Powerpoint
ODF	OpenDocumentFormat (OpenOffice)
EML	Elektronická mailová zpráva*
MSG	Elektronická mailová zpráva, kontakt, schůzka nebo úloha vytvořená nebo uložená v Microsoft Outlook*

** Experimentální podpora. V případě zájmu o povolení nás kontaktujte.*

5.1.2.4 <ExternalSignatureFileName>

[nepovinný element]

Vstup	Popis
string	Název souboru externího podpisu. Pouze v případě, že k dokumentu byl takový podpis vytvořen.

5.1.2.5 <ExternalSignature>

[nepovinný element]

Vstup	Popis
Base64Binary	Data externího podpisu kódovaná v base64. Pouze v případě, že k dokumentu byl takový podpis vytvořen.

5.1.2.6 <Properties>

[povinný element včetně jednoho z GetReport na true]

5.1.2.6.1 <ReportLanguage>

[nepovinný element]

Vstup	Popis
String	Lokalizace textových informací ve výstupní doložce. Hodnoty: `cz`, `en` Výchozí hodnota: `cz`

5.1.2.6.2 <GetReport>

[nepovinný element]

Vstup	Popis
Boolean	Definuje získání <Report> v odpovědi. Výchozí hodnota: `true`

5.1.2.6.3 <GetXMLReport>

[nepovinný element]

Vstup	Popis
Boolean	Definuje získání podepsaného reportu ověření v XML. Výchozí hodnota: `true`

5.1.2.6.4 <GetHTMLReport>

[nepovinný element]

Vstup	Popis
Boolean	Definuje získání reportu ověření v HTML. Výchozí hodnota: `true`

5.1.2.6.5 <GetPDFReport>

[nepovinný element]

Vstup	Popis
Boolean	Definuje získání podepsaného reportu ověření v PDF. Výchozí hodnota: `false`

5.1.2.6.6 <ValidationTime>

[nepovinný element]

Vstup	Popis
dateTime	Definuje rozhodný okamžik, ke kterému se má ověřovat platnost podpisu. Příklad hodnoty: `2018-11-09T07:35:00+02:00` *(vč. časové zóny)* Pro odpovídající vyhodnocení musí být nastaven parametr `IgnoreNoPoe` na `true`. Pokud údaj `ValidationTime` není zadán, nebo s tímto údajem není nastaven parametr `IgnoreNoPoe` na `true`, nastaví se rozhodný okamžik na datum a čas připojení časového razítka nebo, v případě chybějícího časového razítka, na aktuální. V případě nastavení hodnoty `ValidationTime` je tato informace vyznačena červeným textem ve výstupním PDF reportu. Výchozí hodnota: *Now* (aktuální čas ze SecuSign SDK serveru)

5.1.2.6.7 <IgnoreNoPOE>

[nepovinný element]

Vstup	Popis
Boolean	Umožní vyhodnotit platnost podpisu i bez prokazatelného času existence (časového razítka) a to buď k aktuálnímu času nebo, v případě nastavení `ValidationTime`, ke zvolenému času rozhodného okamžiku. Hodnoty: `false, true` V případě nastavení hodnoty `IgnoreNoPoe` na `true` je tato informace vyznačena červeným textem ve výstupním PDF reportu. Výchozí hodnota: `false`

5.1.2.6.8 <UseClaimedTimeIfNoTs>

[nepovinný element]

Vstup	Popis
Boolean	Umožní vyhodnotit platnost podpisu k deklarovanému času, jestliže u podpisu chybí časové razítko. Deklarovaný čas je získán ze signingTime atributu podpisu. Hodnoty: `false, true` Pro odpovídající vyhodnocení musí být nastaven parametr `IgnoreNoPoe` na `true`. Pokud parametr `UseClaimedTimeIfNoTs` není zvolen, a podpis neobsahuje časové razítko, je k vyhodnocení platnosti podpisu použit aktuální čas. V případě nastavení hodnoty `UseClaimedTimeIfNoTs` na `true` je tato informace vyznačena červeným textem ve výstupním PDF reportu. Výchozí hodnota: `false`

5.1.2.6.9 <DontUseGracePeriodForQCerts>

[nepovinný element]

Vstup	Popis
Boolean	Umožní vyhodnotit platnost podpisu bez nutnosti čekat 24 hodin (grace period) na jeho ověření. Pro kontrolu revokace využijeme informaci z OCSP nebo v případě nedostupnosti OCSP z prvního dostupného CRL vydaného po rozhodném okamžiku. Výchozí hodnota: `true`

5.1.2.7 </Properties>

5.1.2.8 <Params>

[nepovinný element]

Vstup	Popis
String	Volitelné, obsahuje další parametry. Zatím se nevyužívá.

5.1.3 Struktura odpovědi na požadavek

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <ValidateResponse xmlns="http://software602.com/secusign/">
      <ValidateResult>int</ValidateResult>
      <Report>
        <CreationDateTime>dateTime</CreationDateTime>
        <FileName>string</FileName>
        <FileSize>long</FileSize>
        <ExtSigFileName>string</ExtSigFileName>
        <ExtSigFileSize>long</ExtSigFileSize>
        <PDFVersion>string</PDFVersion>
        <PDFNumOfPages>int</PDFNumOfPages>
        <docType>string</docType>
        <expiration>dateTime</expiration>
        <docDataHash>base64Binary</docDataHash>
        <docDataHashAlg>string</docDataHashAlg>
        <currSignHashAlg>string</currSignHashAlg>
        <globalStatus>string</globalStatus>
        <validationProperties>
          <ValidationTime>dateTime</ValidationTime>
          <CustomValidationTime>boolean</CustomValidationTime>
          <IgnoreNoPOE>boolean</IgnoreNoPOE>
          <UseClaimedTimeIfNoTS>boolean</UseClaimedTimeIfNoTS>
          <DontUseGracePeriodForQCerts>boolean</DontUseGracePeriodForQCerts>
        </validationProperties>
        <sigInfos>
          <SigInfo>
            <id>unsignedInt</id>
            <sid>string</sid>
            <sigTimestamps xsi:nil="true" />
            <sigType>string</sigType>
            <xmlSignedReferences xsi:nil="true" />
            <pdfByteRange xsi:nil="true" />
            <hasFurtherChanges>boolean</hasFurtherChanges>
            <Reason>string</Reason>
            <Location>string</Location>
            <Contact>string</Contact>
          </SigInfo>
          <SigInfo>
            <id>unsignedInt</id>
            <sid>string</sid>
            <sigTimestamps xsi:nil="true" />
            <sigType>string</sigType>
```

```
            <xmlSignedReferences xsi:nil="true" />
            <pdfByteRange xsi:nil="true" />
            <hasFurtherChanges>boolean</hasFurtherChanges>
            <Reason>string</Reason>
            <Location>string</Location>
            <Contact>string</Contact>
          </SigInfo>
        </sigInfos>
      </Report>
      <XMLReport>base64Binary</XMLReport>
      <HTMLReport>base64Binary</HTMLReport>
      <PDFReport>base64Binary</PDFReport>
      <StatusMessage>string</StatusMessage>
    </ValidateResponse>
  </soap:Body>
</soap:Envelope>
```

5.1.4 Výstupní parametry metody

5.1.4.1 <ValidateResult>

Návratová hodnota	Popis
Int	Výsledek metody Validate (ověření podpisů). 0 = v pořádku, jinak Návratové kódy všech metod a chyba popsaná ve StatusMessage.

5.1.4.2 <Report>

5.1.4.2.1 <CreationDateTime>

Návratová hodnota	Popis
dateTime	Datum a čas, kdy došlo k vytvoření ověřovacího reportu

5.1.4.2.2 <FileName>

Návratová hodnota	Popis
string	Název vstupního souboru (včetně přípony), ze kterého byly ověřeny podpisy nebo ke kterému náleží externí podpis. Max. 260 znaků.

5.1.4.2.3 <FileSize>

Návratová hodnota	Popis
long	Velikost vstupního souboru (v bajtech)

5.1.4.2.4 <ExtSigFileName>

Návratová hodnota	Popis
string	Název vstupního souboru externího podpisu (včetně přípony), ze kterého byl ověřen podpis

5.1.4.2.5 <ExtSigFileSize>

Návratová hodnota	Popis

long	Velikost vstupního souboru externího podpisu (v bajtech)

5.1.4.2.6 <PDFVersion>

Návratová hodnota	Popis
String	Verze PDF dokumentu. Např. 1.4, 1.5, 1.7

5.1.4.2.7 <PDFNumOfPages>

Návratová hodnota	Popis
Int	Počet stránek v PDF dokumentu

5.1.4.2.8 <docType>

Návratová hodnota	Popis
UNKNOWN	Neznámý typ dokumentu
CMSPKCS7	Dokument podepsaný interním CMS/PKCS7 podpisem
CMSPKCS7Ext	Dokument podepsaný externím CMS/PKCS7 podpisem
PDF	Podepsaný PDF dokument
XML	Podepsaná XML data
XML602FORM	Podepsané datové zprávy z Informačního systému datových schránek a FO/ZFO formuláře aplikace Software602 Form Filler
XMLISDOC	Podepsaná XML ISDOC data
ASiC_S_CAdES	ASiC-Simple s CAdES podpisem
ASiC_S_XAdES	ASiC-Simple s XAdES podpisem
ASiC_S_Tst	ASiC-Simple s Timestamp
ASiC_E_CAdES_Tst	ASiC-Extended s CAdES podpisem nebo s Timestamp
ASiC_E_XAdES	ASiC-Extended s XAdES podpisem
MS_WORD	Podepsaný dokument aplikace MS Word
MS_EXCEL	Podepsaný dokument aplikace MS Excel
MS_PWR_PNT	Podepsaný dokument aplikace MS Powerpoint
ODF	Podepsaný OpenDocumentFormat (OpenOffice)

5.1.4.2.9 <expiration>

Návratová hodnota	Popis
DateTime	Datum a čas vypršení ověřitelnosti celého dokumentu. Po tomto datu nebude možné ověřit platnost podpisových certifikátů a zajistit další ověřitelnost, uchování a platnost dokumentu.

5.1.4.2.10 <docDataHash>

Návratová hodnota	Popis

Base64Binary	Hash analyzovaného dokumentu v kódování Base64. Algoritmus výpočtu hashe je v následujícím elementu docDataHashAlg.

5.1.4.2.11 <docDataHashAlg>

Návratová hodnota	Popis
String	Algoritmus výpočtu hashe analyzovaného dokumentu. Ve tvaru například: 2.16.840.1.101.3.4.2.1.

5.1.4.2.12 <currSignHashAlg>

Návratová hodnota	Popis
String	Algoritmus výpočtu hashe posledního podpisu. Příklad: 2.16.840.1.101.3.4.2.1

5.1.4.2.13 <globalStatus>

Návratová hodnota	Popis
String	Sumarizuje stav dokumentu na základě všech podpisů a časových razítek. Může nabývat hodnot: OK = 0 (Všechny podpisy a dokumentová časová razítka jsou platná; TOTAL_PASSED dle normy ETSI[2]) WARNING = 1 (Nelze určit platnost některých podpisových certifikátů nebo dokumentových časových razítek; INDETERMINATE dle normy ETSI[2])) ERROR = 2 (Některé podpisy nebo dokumentová časová razítka jsou neplatná, např. odvolaný certifikát, poškozený hash dokumentu, změny po podepsání atd.; TOTAL_FAILED dle normy ETSI[2])) NO_SIGNATURES = 3 (Dokument neobsahuje žádné podpisy ani dokumentová časová razítka)

5.1.4.2.14 <validationProperties>

5.1.4.2.14.1 <ValidationTime>

Návratová hodnota	Popis
dateTime	Rozhodný okamžik – čas, ke kterému byla ověřena platnost podpisu. Příklad hodnoty: `2018-11-09T07:35:00.085+01:00` Výchozí hodnota *Now* (aktuální čas z SecuSign SDK serveru)

5.1.4.2.14.2 <CustomValidationTime>

Návratová hodnota	Popis
Boolean	Určuje, zda byl pro ověření platnosti podpisu nastaven vlastní rozhodný okamžik – `ValidationTime` Výchozí hodnota `false`

5.1.4.2.14.3 <IgnoreNoPOE>

Návratová hodnota	Popis

Boolean	Určuje, zda byla vyhodnocena platnost podpisu bez prokazatelného času existence (časového razítka). Výchozí hodnota `false`

5.1.4.2.14.4 <UseClaimedTimeIfNoTs>

Návratová hodnota	Popis
Boolean	Určuje, zda byla vyhodnocena platnost podpisu k deklarovanému času. Deklarovaný čas je případně získán ze signingTime atributu podpisu. Výchozí hodnota `false`

5.1.4.2.14.5 <DontUseGracePeriodForQCerts>

Návratová hodnota	Popis
Boolean	Určuje, zda byla vyhodnocena platnost podpisu bez nutnosti čekat 24 hodin (grace period) na jeho ověření. Pro kontrolu revokace se využila informace z OCSP nebo, v případě nedostupnosti OCSP, z prvního dostupného CRL vydaného po rozhodném okamžiku. Výchozí hodnota `true`

5.1.4.2.15 </validationProperties>

5.1.4.2.16 <sigInfos>

5.1.4.2.16.1 <SigInfo>

informace o podpisu (opakující se element v případě více podpisů)

5.1.4.2.16.1.1 <status>

Návratová hodnota	Popis
String	Výsledný stav ověření podpisu podle první verze ETSI normy[1] týkající se ověřování PAdES, CAdES, XAdES a ASiC.

5.1.4.2.16.1.2 <statusEN>

Návratová hodnota	Popis
String	Výsledný stav ověření podpisu podle aktuální verze ETSI normy[2] týkající se ověřování PAdES, CAdES, XAdES a ASiC, viz hodnoty Indication a subIndication v Preserve_register/update/getInfo

5.1.4.2.16.1.3 <message>

Návratová hodnota	Popis
String	Podrobnosti ověření stavu podpisu/pečeti/razítka, pokud jsou u daného stavu k dispozici.

5.1.4.2.16.1.4 <certType>

Návratová hodnota	Popis

String	Typ certifikátu podpisu/pečeti/razítka. Může nabývat hodnot: COMMERCIAL = Komerční certifikát pro autentizaci QUALIFIED = Kvalifikovaný certifikát pro elektronický podpis/pečeť TRUSTED = Certifikát pro elektronický podpis vydaný kvalifikovaným poskytovatelem služeb vydávání certifikátů INTERNAL = Privátní certifikát UNKNOWN = Neznámý OST = Důvěryhodný certifikát operačního systému

5.1.4.2.16.1.5 <adesType>

Návratová hodnota	Popis
String	Typ podpisového certifikátu dle standardu AdES (Advanced Electronic Signature)

5.1.4.2.16.1.6 <eidasType>

Návratová hodnota	Popis
String	Typ podpisového certifikátu dle nařízení eIDAS. Může nabývat hodnot: ADVANCED_SIGNATURE = Zaručený elektronický podpis ACREDITED_SIGNATURE = Uznávaný elektronický podpis (Zaručený elektronický podpis založený na kvalifikovaném certifikátu) QUALIFIED_SIGNATURE = Uznávaný elektronický podpis (Kvalifikovaný elektronický podpis založený na kvalifikovaném certifikátu a vytvořený na kvalifikovaném prostředku) ADVANCED_SEAL = Zaručená elektronická pečeť TRUSTED_SEAL = Zaručená elektronická pečeť, založená na certifikátu pro elektronické pečeti od kvalifikovaného poskytovatele služeb vytvářejících důvěru ACREDITED_SEAL = Uznávaná elektronická pečeť (Zaručená elektronická pečeť založená na kvalifikovaném certifikátu pro elektronické pečeti) QUALIFIED_SEAL = Kvalifikovaná eletronická pečeť založená na kvalifikovaném certifikátu od kvalifikovaného poskytovatele služeb vytvářejících důvěru TIMESTAMP = Elektronické časové razítko QUALIFIED_TIMESTAMP = Kvalifikované elektronické časové razítko SYSTEM_SIGNATURE = Elektronická značka založená na systémovém certifikátu

5.1.4.2.16.1.7 <baselineType>

Návratová hodnota	Popis
String	Typ podpisového certifikátu dle Baseline profilu. Může nabývat hodnot: BaselineType_LEGACY=Neodpovídá žádnému Baseline profilu CADES_B = CAdES B-B (Baseline B) CADES_T = CAdES B-T (Baseline T)

	CADES_LT = CAdES B-LT (Baseline LT) CADES_LTA = CAdES B-LTA (Baseline LTA) PADES_B = PAdES B-B (Baseline B) PADES_T = PAdES B-T (Baseline T) PADES_LT = PAdES B-LT (Baseline LT) PADES_LTA = PAdES B-LTA (Baseline LTA) XADES_B = XAdES B-B (Baseline B) XADES_T = XAdES B-T (Baseline T) XADES_LT = XAdES B-LT (Baseline LT) XADES_LTA = XAdES B-LTA (Baseline LTA) ASIC_B = ASiC B-B (Baseline B) ASIC_T = ASiC B-T (Baseline T) ASIC_LT = ASiC B-LT (Baseline LT) ASIC_LTA = ASiC B-LTA (Baseline LTA)

5.1.4.2.16.1.8 <signCert>

5.1.4.2.16.1.9 <Name>

Návratová hodnota	Popis
String	Jméno podepisujího tak, jak je uvedeno v certifikátu

5.1.4.2.16.1.10 <Subject>

Návratová hodnota	Popis
String	Informace z certifikátového atributu Subjekt, např.: CN = Common Name (Běžné jméno) GN = Given Name (Křestní jméno) SN = Surname (Příjmení) SERIALNUMBER = Sériové číslo C = Country (Země) L = Locality (Lokalita) E = Email O = Organization (Organizace) OU = Organizational unit (Organizační jednotka) Pseudonyme = pseudonym

5.1.4.2.16.1.11 <IssuerName>

Návratová hodnota	Popis
String	Jméno vystavitele certifikátu z CN v atributu Issuer

5.1.4.2.16.1.12 <Issuer>

Návratová hodnota	Popis

String	Kompletní informace o vystaviteli certifikátu z atributu Issuer

5.1.4.2.16.1.13 <Serial>

Návratová hodnota	Popis
String	Sériové číslo certifikátu

5.1.4.2.16.1.14 <NotBefore>

Návratová hodnota	Popis
String	Platnost certifikátu od

5.1.4.2.16.1.15 <NotAfter>

Návratová hodnota	Popis
String	Platnost certifikátu do

5.1.4.2.16.1.16 <Hash>

Návratová hodnota	Popis
String	Hash veřejného klíče certifikátu algoritmu SHA256

5.1.4.2.16.1.17 <ServiceStatusUri>

Návratová hodnota	Popis
String	Obsahuje celou Uri stanovující servisní stav autority na TSL, např. http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

5.1.4.2.16.1.18 <ServiceTypeUri>

Návratová hodnota	Popis
String	Obsahuje celou Uri stanovující servisní typ autority na TSL, např. http://uri.etsi.org/TrstSvc/Svctype/CA/QC

5.1.4.2.16.1.19 <IsTrustAnchor>

Návratová hodnota	Popis
Boolean	Definuje, zda je certifikát uveden na TSL

5.1.4.2.16.1.20 <Data>

Návratová hodnota	Popis
String	Data veřejného klíče certifikátu

5.1.4.2.16.1.21 </signCert>

5.1.4.2.16.2 <qcStatements>

5.1.4.2.16.2.1 <string>

Návratová hodnota	Popis
String	Prohlášení vystavitele kvalifikovaného certifikátu ve formě OID.

5.1.4.2.16.3 </qcStatements>

5.1.4.2.16.4 <qcType>

Návratová hodnota	Popis
String	Typ certifikátu podpisu/pečeti/razítka dle eIDAS. Může nabývat následujících hodnot, jejichž význam se může lišit i podle certType: QUALIFIED – kvalifikovaný certifikát vydaný kvalifikovaným poskytovatelem služeb vydávání certifikátů LEGACY – neznámý/elektronický certifikát ESEAL – certifikát pro elektronickou pečeť ESIGN – certifikát pro elektronický podpis WEB – pro autentizaci internetových stránek

5.1.4.2.16.5 <signCertIsPseudonyme>

Návratová hodnota	Popis
Boolean	Určuje, zda je certifikát (podpisu/pečeti/razítka) vystaven na pseudonym

5.1.4.2.16.6 <time>

Návratová hodnota	Popis
dateTime	Důvěryhodný časový údaj podpisu/pečeti/razítka

5.1.4.2.16.7 <timeFromComputerClock>

Návratová hodnota	Popis
dateTime	Časový údaj podpisu/pečeti/razítka z hodin počítače autora

5.1.4.2.16.8 <validTo>

Návratová hodnota	Popis
dateTime	Platnost podpis/pečeti/razítka do

5.1.4.2.16.9 <certPath>

5.1.4.2.16.9.1 <CertInfo>

Návratová hodnota	Popis
dateTime	Platnost podpis/pečeti/razítka do

5.1.4.2.16.9.2 <Name>

Návratová hodnota	Popis

String	Jméno podepisujího tak, jak je uvedeno v certifikátu

5.1.4.2.16.9.3 <Subject>

Návratová hodnota	Popis
String	Informace z atributu certifikátu Subjekt, např.: CN=Common Name (Běžné jméno) GN=Given Name (Křestní jméno) SN=Surname (Příjmení) SERIALNUMBER=seriové číslo certifikátu C=Country (Země) L=Locality (Lokalita) E=Email O= Organization (Organizace) OU=Organizational unit (Organizační jednotka) Pseudonym=pseudonym

5.1.4.2.16.9.4 <IssuerName>

Návratová hodnota	Popis
String	Jméno vystavitele certifikátu z CN= v atributu Issuer

5.1.4.2.16.9.5 <Issuer>

Návratová hodnota	Popis
String	Kompletní informace o vystaviteli certifikátu z atributu Issuer

5.1.4.2.16.9.6 <Serial>

Návratová hodnota	Popis
String	Seriové číslo certifikátu

5.1.4.2.16.9.7 <NotBefore>

Návratová hodnota	Popis
String	Platnost certifikátu od

5.1.4.2.16.9.8 <NotAfter>

Návratová hodnota	Popis
String	Platnost certifikátu do

5.1.4.2.16.9.9 <Hash>

Návratová hodnota	Popis
String	Hash veřejného klíče certifikátu algoritmu SHA256

5.1.4.2.16.9.10 <ServiceStatusUri>

Návratová hodnota	Popis
String	Obsahuje celou Uri stanovující servisní stav certifikátu na TSL, např. http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

5.1.4.2.16.9.11 <ServiceTypeUri>

Návratová hodnota	Popis
String	Obsahuje celou Uri stanovující servisní typ certifikátu na TSL, např. http://uri.etsi.org/TrstSvc/Svctype/CA/QC

5.1.4.2.16.9.12 <IsTrustAnchor>

Návratová hodnota	Popis
Boolean	Definuje, zda je certifikát uveden na TSL

5.1.4.2.16.9.13 <Data>

Návratová hodnota	Popis
String	Data veřejného klíče certifikátu

5.1.4.2.16.10 </certPath>

5.1.4.2.16.11 <crlPath>

5.1.4.2.16.11.1 <RevocationData>

5.1.4.2.16.11.2 <Type>

Návratová hodnota	Popis
String	Typ revokačních dat. Může být: CRL, OCSP

5.1.4.2.16.11.3 <Issuer>

Návratová hodnota	Popis
String	Vystavitel revokačních dat (pouze u CRL)

5.1.4.2.16.11.4 <Serial>

Návratová hodnota	Popis
String	Sériové číslo revokačních dat (pouze u CRL)

5.1.4.2.16.11.5 <ThisUpdate>

Návratová hodnota	Popis
dateTime	Datum a čas poslední aktualizace revokačních dat.

5.1.4.2.16.11.6 <NextUpdate>

Návratová hodnota	Popis
dateTime	Datum a čas následující aktualizace revokačních dat.

5.1.4.2.16.11.7 <Hash>

Návratová hodnota	Popis
String	Hash revokačních dat.

5.1.4.2.16.11.8 <Data>

Návratová hodnota	Popis
String	Revokační data CRL v base64 na základě kterých se ověřovala platnost podpisu/pečeti/razítka

5.1.4.2.16.11.9 <Source>

Návratová hodnota	Popis
String	Zdroj revokačních dat, nabývá hodnot: SECUSIGN - v případě revokačních dat stažených ze serveru Secusign ONLINE - v případě revokačních dat stažených z jejich online zdroje CUSTOM - v případě revokačních dat poskytnutých uživatelem PADES_DSS_VRI - v případě revokačních dat uložených v PDF dokumetu XADES_UNSIGNED_SIGNATURE_PROPERTIES - v případě revokačních dat uložených v nepodepsané části XAdES podpisu CADES_SIGNED_DATA - v případě revokačních dat uložených v podepsané části CAdES podpisu CADES_UNSIGNED_ATTRIBUTES - v případě revokačních dat uložených v nepodepsané části CAdES podpisu UNKNOWN - neznámý zdroj revokačních dat nebo není vyplněno CERTIFICATE_FROM_SIGNATURE - certifikát pocházející z dokumentu/podpisu TS_CERTIFICATE_FROM_SIGNATURE - certifikát TS pocházející z dokumentu/podpisu DOC_INFO - certifikáty pocházející z DocInfo -> DocInfoTslProvider

5.1.4.2.16.11.10 <DistributionPointChecked>

Návratová hodnota	Popis
Boolean	Informace, zda byl kontrolován distribuční bod CRL/OCSP. Není vždy potřebné.

5.1.4.2.16.11.11 <DistributionPoint>

Návratová hodnota	Popis
String	URL distribučního bodu.

5.1.4.2.16.11.12 <DistributionPointCheckDate>

Návratová hodnota	Popis
dateTime	Datum a čas kontroly distribučního bodu.

5.1.4.2.16.11.13 <DistributionPointThisUpdate>

Návratová hodnota	Popis
dateTime	Informace z distribučního bodu CRL/OCSP o datumu a času vydání této aktualizace. Pokud CRL/OCSP pro časové razítko byl vydán před rozhodným okamžikem, hledá se novější na DistributionPoint a pokud není k dispozici novější, nebyl v uvedený DistributionCheckDate certifikát časového razítka revokován.

5.1.4.2.16.11.14 <DistributionPointHash>

Návratová hodnota	Popis
String	Hash distribučního bodu CRL/OCSP.

5.1.4.2.16.11.15 </RevocationData>

5.1.4.2.16.12 </crlPath>

5.1.4.2.16.13 <lastHashAlgOid>

Návratová hodnota	Popis
dateTime	Jedná se o poslední použitý OID digest algoritmus v SignerInfo (CMS, PDF). Příklad pro SHA256 algoritmus: 2.16.840.1.101.3.4.2.1

5.1.4.2.16.14 <id>

Návratová hodnota	Popis
unsignedInt	Pořadové číslo podpisu tak, jak byl přidán do dokumentu. Počítáno od nuly.

5.1.4.2.16.15 <sid>

Návratová hodnota	Popis
String	Unikátní identifikátor podpisu.

5.1.4.2.16.16 <counterSignsSignatureSid>

Návratová hodnota	Popis
String	Unikátní identifikátor podpisu, který tento podepisuje

5.1.4.2.16.17 <DecisiveMoment>

Návratová hodnota	Popis
dateTime	Rozhodný okamžik je čas, ke kterému rozhodujeme o dané entitě (podpisu/razítku). Jedná se vlastně o Proof of Existence, ke kterému entitu ověřujeme. Pokud není k dispozici datum a čas časového razítka použije se ValidationTime (případně aktuální datum).

5.1.4.2.16.18 <DecisiveMomentSource>

Návratová hodnota	Popis
string	Informace o původu času rozhodného okamžiku pro vyhodnocení podpisu. Hodnoty: VALIDATION_DATE - ověřovalo se k datu validace, CUSTOM_VALIDATION_DATE - ověřovalo se k datu validace zadaného uživatelem, TIMESTAMP - ověřovalo se k datu z razítka, CLAIMED_TIME - ověřovalo se k datu z tzv. claimedTime tedy hodnoty pocházející z hodin počítače autora podpisu

<sigTimestamps> *nepovinný element, je závislý na existenci časového razítka u podpisu*

Návratová hodnota	Popis
XML struktura	Informace o časovém razítku přidaném jako atribut k digitálnímu podpisu. Stejná XML struktura informací jako u nadřazeného podpisu. Tedy obsahuje element *SigInfo*, viz výše, včetně všech jeho potomků. Informace v potomcích se váží k certifikátu časového razítka.

5.1.4.2.16.19 <sigType>

Návratová hodnota	Popis
Enum	Typ podpisu. Může nabývat hodnot: UNKNOWN – neznámý STANDARD – standardní XML602FORM_TECHNICAL – formulářový Software602

<xmlSignedReferences> *nepovinný element, je závislý na formátu vstupního souboru (jen pro XML/ZFO)*

Návratová hodnota	Popis
XML struktura	Data podpisu. Může obsahovat id, uri, digAlg a digest.

<pdfByteRange> *nepovinný element, je závislý na formátu vstupního souboru (jen pro PDF)*

Návratová hodnota	Popis
XML struktura	Bytový rozsah PDF podpisů

5.1.4.2.16.20 <hasFurtherChanges>

Návratová hodnota	Popis
Boolean	Údaj, zda byly v dokumentu provedeny změny po podpisu. Hodnoty: false, true

5.1.4.2.16.21 <Reason>

Návratová hodnota	Popis
String	Důvod podepsání dokumentu.

5.1.4.2.16.22 <Location>

Návratová hodnota	Popis
String	Místo podepsání dokumentu.

5.1.4.2.16.23 <Contact>

Návratová hodnota	Popis
String	Kontaktní informace k podepsání dokumentu.

5.1.4.2.17 </SigInfo>

5.1.4.3 </sigInfos>

5.1.4.4 </Report>

5.1.4.5 <XMLReport>

Návratová hodnota	Popis
Base64Binary	XML data výstupního ověření kódovaná v Base64

5.1.4.6 <HTMLReport>

Návratová hodnota	Popis
Base64Binary	HTML data výstupního ověření kódovaná v Base64

5.1.4.7 <PDFReport>

Návratová hodnota	Popis
Base64Binary	PDF data výstupního ověření kódovaná v Base64

5.1.4.8 <StatusMessage>

Návratová hodnota	Popis
String	Textová zpráva odpovídající celkovému výsledku ověření všech popisů. Hodnota je naplněna pouze v případě problematického výsledku.

6 Kvalifikovaná služba uchovávání elektronických podpisů

Kvalifikovaná služba uchovávání elektronických podpisů obsahuje rozšířenou sadu metod webových služeb pro:

- registrování dokumentu, který je opatřený ověřitelným elektronickým podpisem, pečetí a/nebo časovým razítkem do služby SecuSign (Preserve_register),
- prodloužení platnosti a ověřitelnosti podpisu, pečeti, časového razítka novým časovým razítkem (Preserve_update),
- zjištění informací o registrovaném dokumentu a jeho elektronických podpisech (Preserve_getInfo),
- zjištění informací o registrovaných dokumentech a jeho elektronických podpisech, pečetích, časových razítkách, které je nutné před vypršením jejich platnosti prodloužit (Preserve_getForUpdate),
- a pro odregistrování dokumentu a uchovaných elektronických podpisů z kvalifikované služby SecuSign (Preserve_unregister).

Registrovaný dokument s elektronickým podpisem, pečetí, časovým razítkem je opatřen elektronickým kvalifikovaným časovým razítkem od kvalifikovaného poskytovatele služeb vytvářejících důvěru – PostSignum (Česká pošta). Při uchování služba připojí k podpisu revokační data a metadata vyhovující specifikaci PAdES, CAdES nebo XAdES. Registrovaný dokument má přidělené unikátní identifikační číslo (DocID) podle kterého lze zjistit informace o uchovaných podpisech. Pro připojení revokačních dat/metadat do registrovaného dokument je nutné, aby podpis nebyl příliš čerstvý (nedošlo k podepsání několik milisekund či sekund před).

6.1 Sada metod

- Metoda Preserve_getForUpdate
- Metoda Preserve_getInfo
- Metoda Preserve_register
- Metoda Preserve_unregister
- Metoda Preserve_update

6.1.1 Metoda Preserve_register

Umožňuje v kvalifikované službě SecuSign uchovat elektronické podpisy v dokumentu, jež je opatřen uznávaným, kvalifikovaným nebo zaručeným elektronickým podpisem, značkou a/nebo kvalifikovaným elektronickým časovým razítkem. Při registraci je dokument opatřen kvalifikovaným elektronickým časovým razítkem pro jednoznačné určení časového údaje, kdy služba převzala dokument do evidence.

Popis služby včetně WSDL schématu a příklad požadavku a odpovědi pro SOAP 1.1 a SOAP 1.2 je umístěn na https://localhost/secusign/default.asmx?op=Preserve_register *

* localhost je název používaný pro lokální počítač; namísto něj zvolte jméno/IP adresu SDK serveru (dle nastavení v IIS)

6.1.1.1 Požadavek v rozhraní SOAP 1.1

```
POST /secusign/default.asmx HTTP/1.1
Host: localhost
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://software602.com/secusign/Preserve_register"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <Preserve_register xmlns="http://software602.com/secusign/">
      <FileName>string</FileName>
      <FileData>base64Binary</FileData>
      <FileType>UNKNOWN or CMSPKCS7 or CMSPKCS7Ext or PDF or XML or XML602FORM or
XMLISDOC or ASiC_S_CAdES or ASiC_S_XAdES or ASiC_S_Tst or ASiC_E_CAdES_Tst or
ASiC_E_XAdES or MS_WORD or MS_EXCEL or MS_PWR_PNT or ODF</FileType>
      <ExternalSignatureFileName>string</ExternalSignatureFileName>
      <ExternalSignature>base64Binary</ExternalSignature>
      <SigValidityCondition>ALL or AT_LEAST_ONE or LAST</SigValidityCondition>
      <Properties>
        <AddTimeStampIfNeeded>boolean</AddTimeStampIfNeeded>
      </Properties>
      <SortInfo>string</SortInfo>
      <UserComment>string</UserComment>
      <Params>string</Params>
    </Preserve_register>
  </soap:Body>
</soap:Envelope>
```

6.1.1.2 Vstupní parametry metody

6.1.1.2.1 <FileName>

[povinný element]

Vstup	Popis
String	Název vstupního souboru (včetně přípony) pro uchování. Příklad: Dokument.pdf

	Max. 260 znaků.

6.1.1.2.2 <FileData>

[povinný element]

Vstup	Popis
Base64Binary	Data vstupního souboru kódovaná v base64

6.1.1.2.3 <FileType>

[povinný element]

Vstup	Popis
UNKNOWN	Neznámý typ dokumentu
CMSPKCS7	Dokument podepsaný interním CMS/PKCS7 podpisem
CMSPKCS7Ext	Dokument podepsaný externím CMS/PKCS7 podpisem
PDF	PDF dokument
XML	XML data
XML602FORM	Datové zprávy z Informačního systému datových schránek a FO/ZFO formuláře aplikace Software602 Form Filler
XMLISDOC	Podepsaná XML ISDOC data
ASiC_S_CAdES	ASiC-Simple s CAdES podpisem
ASiC_S_XAdES	ASiC-Simple s XAdES podpisem
ASiC_S_Tst	ASiC-Simple s Timestamp
ASiC_E_CAdES_Tst	ASiC-Extended s CAdES podpisem nebo s Timestamp
ASiC_E_XAdES	ASiC-Extended s XAdES podpisem
MS_WORD	Dokument aplikace MS Word
MS_EXCEL	Dokument aplikace MS Excel
MS_PWR_PNT	Dokument aplikace MS Powerpoint
ODF	OpenDocumentFormat (OpenOffice)

6.1.1.2.4 <ExternalSignatureFileName>

[nepovinný element]

Vstup	Popis
string	Název souboru (včetně přípony) externího podpisu. Pouze v případě, že k dokumentu byl takový podpis vytvořen.

6.1.1.2.5 <ExternalSignature>

[nepovinný element]

Vstup	Popis
Base64Binary	Data externího podpisu kódovaná v Base64. Pouze v případě, že k dokumentu byl takový podpis vytvořen.

6.1.1.2.6 <SigValidityCondition>

[povinný element]

Vstup	Popis
String	Podmínky platnosti podpisu. Hodnoty: ALL – všechny podpisy musí být ověřitelné AT_LEAST_ONE – alespoň jeden podpis musí být ověřitelný LAST – poslední podpis musí být ověřitelný Ověřitelný znamená platný nebo revokovaný. Není akceptován stav, kdy není možné jednoznačně rozhodnout o stavu certifikátu.

6.1.1.2.7 <Properties>

6.1.1.2.7.1 <AddTimestamplfNeeded>

[nepovinný element]

Vstup	Popis
Boolean	Pokusí se provést prezervaci nad podepsaným souborem, který je bez razítka (BaseLine-B). Pokud je podpis jinak validní, tak se přidá razítko a dokument se zaeviduje pro uchování. V opačném případě se vrátí chyba, že nebylo možné provést uchování souboru.

6.1.1.2.8 </Properties>

6.1.1.2.9 <SortInfo>

[nepovinný element]

Vstup	Popis
String	Zatřiďovací informace – např. název složky, nebo struktura vnořených složek, ve kterých je dokument u uživatele evidován. Max. 100 znaků.

6.1.1.2.10 <UserComment>

[nepovinný element]

Vstup	Popis
String	Vlastní komentář nebo popis uživatele k uchovanému dokumentu

6.1.1.2.11 <Params>

[nepovinný element]

Vstup	Popis
String	Volitelné, obsahuje další parametry. Zatím se nevyužívá.

6.1.1.3 Struktura odpovědi na požadavek

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
```

```
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <Preserve_registerResponse xmlns="http://software602.com/secusign/">
      <Preserve_registerResult>int</Preserve_registerResult>
      <OutputData>base64Binary</OutputData>
      <PreservationInfo>
        <CreationDateTime>dateTime</CreationDateTime>
        <docId>string</docId>
        <fileName>string</fileName>
        <fileSize>long</fileSize>
        <sortInfo>string</sortInfo>
        <lastUpdate>dateTime</lastUpdate>
        <expiration>dateTime</expiration>
        <docDataHash>base64Binary</docDataHash>
        <docDataHashAlg>string</docDataHashAlg>
        <currSignHashAlg>string</currSignHashAlg>
        <sigValidityCondition>ALL or AT_LEAST_ONE or LAST</sigValidityCondition>
        <sigsPreservationStatus>
          <PreservationInfo>
            <sid>string</sid>
            <sigStatus xsi:nil="true" />
            <extendedValidationEndDate>dateTime</extendedValidationEndDate>
            <signingCertSubject>string</signingCertSubject>
            <bIsDocTimeStamp>boolean</bIsDocTimeStamp>
            <procesStatus>string</procesStatus>
          </PreservationInfo>
          <PreservationInfo>
            <sid>string</sid>
            <sigStatus xsi:nil="true" />
            <extendedValidationEndDate>dateTime</extendedValidationEndDate>
            <signingCertSubject>string</signingCertSubject>
            <bIsDocTimeStamp>boolean</bIsDocTimeStamp>
            <procesStatus>string</procesStatus>
          </PreservationInfo>
        </sigsPreservationStatus>
        <preservationHistory>
          <PreservationRecord>
            <id>int</id>
            <operationTime>dateTime</operationTime>
            <operationType>REGISTER or UPDATE or UNREGISTER or UNKNOWN</operationType>
            <operationStatus>int</operationStatus>
            <operationStatusInfo>string</operationStatusInfo>
            <fileName>string</fileName>
            <fileSize>long</fileSize>
            <hashIn>string</hashIn>
            <hashOut>string</hashOut>
            <userComment>string</userComment>
          </PreservationRecord>
          <PreservationRecord>
            <id>int</id>
            <operationTime>dateTime</operationTime>
            <operationType>REGISTER or UPDATE or UNREGISTER or UNKNOWN</operationType>
            <operationStatus>int</operationStatus>
            <operationStatusInfo>string</operationStatusInfo>
            <fileName>string</fileName>
            <fileSize>long</fileSize>
            <hashIn>string</hashIn>
            <hashOut>string</hashOut>
            <userComment>string</userComment>
          </PreservationRecord>
        </preservationHistory>
        <docType>string</docType>
      </PreservationInfo>
      <DocInfo>
        <CreationDateTime>dateTime</CreationDateTime>
```

```
        <FileName>string</FileName>
        <FileSize>long</FileSize>
        <ExtSigFileName>string</ExtSigFileName>
        <ExtSigFileSize>long</ExtSigFileSize>
        <PDFVersion>string</PDFVersion>
        <PDFNumOfPages>int</PDFNumOfPages>
        <docType>string</docType>
        <expiration>dateTime</expiration>
        <docDataHash>base64Binary</docDataHash>
        <docDataHashAlg>string</docDataHashAlg>
        <currSignHashAlg>string</currSignHashAlg>
        <globalStatus>string</globalStatus>
        <validationProperties>
          <ValidationTime>dateTime</ValidationTime>
          <CustomValidationTime>boolean</CustomValidationTime>
          <IgnoreNoPOE>boolean</IgnoreNoPOE>
          <UseClaimedTimeIfNoTS>boolean</UseClaimedTimeIfNoTS>
          <DontUseGracePeriodForQCerts>boolean</DontUseGracePeriodForQCerts>
        </validationProperties>
        <sigInfos>
          <SigInfo>
            <id>unsignedInt</id>
            <sid>string</sid>
            <DecisiveMoment>dateTime</DecisiveMoment>
            <DecisiveMomentSource>string</DecisiveMomentSource>
            <sigTimestamps xsi:nil="true" />
            <sigType>string</sigType>
            <xmlSignedReferences xsi:nil="true" />
            <pdfByteRange xsi:nil="true" />
            <hasFurtherChanges>boolean</hasFurtherChanges>
            <Reason>string</Reason>
            <Location>string</Location>
            <Contact>string</Contact>
          </SigInfo>
          <SigInfo>
            <id>unsignedInt</id>
            <sid>string</sid>
            <DecisiveMoment>dateTime</DecisiveMoment>
            <DecisiveMomentSource>string</DecisiveMomentSource>
            <sigTimestamps xsi:nil="true" />
            <sigType>string</sigType>
            <xmlSignedReferences xsi:nil="true" />
            <pdfByteRange xsi:nil="true" />
            <hasFurtherChanges>boolean</hasFurtherChanges>
            <Reason>string</Reason>
            <Location>string</Location>
            <Contact>string</Contact>
          </SigInfo>
        </sigInfos>
      </DocInfo>
      <StatusMessage>string</StatusMessage>
    </Preserve_registerResponse>
  </soap:Body>
</soap:Envelope>
```

6.1.1.4 Výstupní parametry metody

6.1.1.4.1 <Preserve_registerResult>

Návratová hodnota	Popis
Int	Výsledek metody Preserve_register (uchování dokumentu). 0 = v pořádku, jinak Návratové kódy všech metod a chyba popsaná ve StatusMessage.

6.1.1.4.2 <OutputData>

Návratová hodnota	Popis
Base64Binary	Data uchovaného dokumentu s elektronickými podpisy kódovaná v Base64

6.1.1.4.3 <PreservationInfo>

6.1.1.4.3.1 <CreationDateTime>

Návratová hodnota	Popis
dateTime	Datum a čas, kdy došlo k vytvoření reportu o uchování dokumentu s elektronickými podpisy

6.1.1.4.3.2 <docID>

Návratová hodnota	Popis
String	Jednoznačné identifikační číslo uchovaného dokumentu s elektronickými podpisy. Bylo automaticky vygenerováno při procesu uchování ve službě SecuSign. Pod tímto číslem je možné v metodě *Preserve_getInfo* zjistit informace o uchovaném dokumentu Max. 128 znaků.

6.1.1.4.3.3 <fileName>

Návratová hodnota	Popis
String	Název uchovaného souboru s elektronickými podpisy. Max. 260 znaků.

6.1.1.4.3.4 <fileSize>

Návratová hodnota	Popis
Long	Velikost uchovaného souboru s elektronickými podpisy

6.1.1.4.3.5 <sortInfo>

Návratová hodnota	Popis
String	Zatřiďovací informace – např. název složky, nebo struktura vnořených složek, ve kterých je dokument u uživatele evidován. Max. 100 znaků.

6.1.1.4.3.6 <lastUpdate>

Návratová hodnota	Popis
dateTime	Datum a čas posledního prodloužení platnosti a ověřitelnosti dokumentu s elektronickými podpisy

6.1.1.4.3.7 <expiration>

Návratová hodnota	Popis
dateTime	Datum a čas vypršení ověřitelnosti platnosti celého dokumentu. Po tomto datu nebude možné ověřit platnost certifikátů podpisů / pečetí / razítek a zajistit další ověřitelnost a platnost uchovaného dokumentu.

6.1.1.4.3.8 <docDataHash>

Návratová hodnota	Popis
Base64Binary	Hash analyzovaného dokumentu kódovaný v Base64. Algoritmus výpočtu hashe je v následujícím elementu docDataHashAlg.

6.1.1.4.3.9 <docDataHashAlg>

Návratová hodnota	Popis
String	Algoritmus výpočtu hashe analyzovaného dokumentu. Ve tvaru například: 2.16.840.1.101.3.4.2.1

6.1.1.4.3.10 <currSignHashAlg>

Návratová hodnota	Popis
string	Algoritmus výpočtu hashe posledního podpisu. Příklad: 2.16.840.1.101.3.4.2.1

6.1.1.4.3.11 <sigValidityCondition>

Návratová hodnota	Popis
string	Zvolené podmínky platnosti podpisu v čase uchování. Hodnoty: ALL – všechny podpisy jsou platné AT_LEAST_ONE – alespoň jeden podpis je platný LAST – poslední podpis je platný

6.1.1.4.3.12 <sigsPreservationStatus>

6.1.1.4.3.12.1 <PreservationInfo> opakující se element podle počtu podpisů v dokumentu

6.1.1.4.3.12.2 <sid>

Návratová hodnota	Popis
string	Identifikátor uchovaného podpisu, který k danému dokumentu eviduje služba SecuSign

6.1.1.4.3.12.3 <sigStatus>

6.1.1.4.3.12.4 <indication>

Návratová hodnota	Popis
string	Stav ověření podpisu – indikace. Může nabývat hodnot: VALID – platný (TOTAL_PASSED dle normy ETSI[2]) INVALID – neplatný (TOTAL_FAILED dle normy ETSI[2]) INDETERMINATE – neurčitý UNKNOWN - neznámý

6.1.1.4.3.12.5 <subindication>

Návratová hodnota	Popis
string	Podstav ověření podpisu - subindikace. Nabývá hodnot (odpovídajících normě ETSI[2]): VALID – Elektronický certifikát nebyl v okamžiku podepsání revokovaný nebo expirovaný a podpis je možné prohlásit za platný. INVALID_REVOKED - Podpisový certifikát byl odvolán ještě před okamžikem pořízení podpisu. Podpis je neplatný. INVALID_HASH_FAILURE - Elektronický podpis je porušený a od podepsání dokumentu zřejmě došlo ke změně podepsané části jeho obsahu. Kontrolní součet uvedený v podpisu nesouhlasí s kontrolním součtem podepsané části! Podpis je neplatný. INVALID_SIG_CRYPTO_FAILURE - Nepodařilo se ověřit příslušnost veřejného klíče k podpisu. Podpis je neplatný. INVALID_FORMAT_FAILURE - Podepsaná data nebyla rozpoznána, formát podpisu je porušený. Podpis je neplatný. INDETERMINATE_NO_CERTIFICATE_CHAIN_FOUND - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Nepodařilo se získat všechny potřebné informace pro kontrolu důvěryhodnosti a odvolání certifikátu. INDETERMINATE_NO_POE - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Nepodařilo se získat všechny potřebné informace pro kontrolu důvěryhodnosti a odvolání certifikátu. INDETERMINATE_TRY_LATER - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Kontrolu odvolání certifikátu je možné provést na základě seznamu odvolaných certifikátů (CRL) vydaném po INDETERMINATE_SIGNED_DATA_NOT_FOUND - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout, protože nejsou k dispozici data, jejichž podpis je ověřován. INDETERMINATE_UNKNOWN_SIGNING_TIME - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Nepodařilo se získat všechny potřebné informace pro kontrolu důvěryhodnosti a odvolání certifikátu. INDETERMINATE_UNTRUST_SIGNING_TIME - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Není k dispozici důvěryhodný údaj z časového razítka o času podepsání. INDETERMINATE_GENERAL_ERROR - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Obecná chyba aplikace, kontaktujte správce. INDETERMINATE_REVOKED_NO_POE - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Podpisový certifikát byl odvolán v době ověření, ale je nejistý čas podepsání. INDETERMINATE_REVOKED_CA_NO_POE - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Nejméně jeden řetěz certifikátu byl nalezen, ale certifikát zprostředkující CA je revokován. INDETERMINATE_OUT_OF_BOUNDS_NO_POE - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Podpisový certifikát vypršel nebo ještě nenastala jeho platnost v době ověření a algoritmus ověřování podpisu nemůže zjistit, že čas podepsání leží uvnitř intervalu platnosti podpisového certifikátu.

	INDETERMINATE_EXPIRED - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Podpisový certifikát vypršel. Podpis byl vytvořen po datu expirace (notAfter) podpisového certifikátu. INDETERMINATE_NOT_YET_VALID - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Podpisový certifikát nebyl ještě platný v době ověřování. Čas podepsání leží před datumem vydání (notBefore) podpisového certifikátu. INDETERMINATE_POLICY_PROCESSING_ERROR - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Soubor dané formální politiky z nějakého důvodu nemohl být zpracován (např. není přístupný, není zpracovatelný, nesouhlasí kontrolní algoritmus, atd.) INDETERMINATE_TIMESTAMP_ORDER_FAILURE - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Některá omezení v pořadí podpisu časových razítek a/nebo podepsaných datových objektů časových razítek nejsou respektována. INDETERMINATE_SIG_CONSTRAINTS_FAILURE - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Nejsou splněna omezení podpisu (chybějící podpisové atributy, nesouhlasná politika el. podpisu, apod.). INDETERMINATE_CHAIN_CONSTRAINTS_FAILURE - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Obecná chyba při sestavování certifikační cesty. INDETERMINATE_CRYPTO_CONSTRAINTS_FAILURE - Alespoň jeden z algoritmů, které byly použity v materiálu (např. hodnota podpisu, certifikát, ...) zapojeném v ověřování podpisu, nebo velikost klíče použita s tímto algoritmem, je pod požadovanou úroveň kryptografického zabezpečení, a tento materiál byl produkován po čase, kdy byl tento algoritmus/klíč považován za bezpečný (je-li znám takový čas), a materiál není chráněn dostatečně silným časovým razítkem aplikovaným před dobou ve které byl algoritmus považován za bezpečný (je-li znám takový čas).

6.1.1.4.3.12.6 </sigStatus>

6.1.1.4.3.12.7 <extendedValidationEndDate>

Návratová hodnota	Popis
dateTime	Datum a čas do kdy byla prodloužena ověřitelnost podpisu

6.1.1.4.3.12.8 <signingCertSubject>

Návratová hodnota	Popis
string	Identifikace podpisového certifikátu, který byl ošetřen

6.1.1.4.3.12.9 <bISDocTimeStamp>

Návratová hodnota	Popis
boolean	Určuje, zda podpis je samostatným časovým razítkem

6.1.1.4.3.12.10 <procesStatus>

Návratová hodnota	Popis
string	Stav ošetření podpisu při uchování. Hodnoty: None – Neproběhlo ošetření podpisu Full – Proběhlo plné ošetření podpisu Partial - Podpis byl ošetřen částečně (neobsahuje všechna validační data) Unknown – Neznámý stav

6.1.1.4.3.12.11 </PreservationInfo>

6.1.1.4.3.13 </sigsPreservationStatus>

6.1.1.4.3.14 <preservationHistory>

6.1.1.4.3.14.1 <PreservationRecord>

6.1.1.4.3.14.2 <id>

Návratová hodnota	Popis
int	Identifikátor provedené operace

6.1.1.4.3.14.3 <operationTime>

Návratová hodnota	Popis
dateTime	Datum a čas provedení operace

6.1.1.4.3.14.4 <operationType>

Návratová hodnota	Popis
PreserveOperation	Typ provedené operace. Hodnoty: REGISTER – uchování dokumentu s elektronickými podpisy UPDATE – prodloužení platnosti a ověřitelnosti elektronických podpisů v dokumentu UNREGISTER – odebrání dokumentu z uchování ve službě SecuSign UNKNOWN – neznámý typ operace

6.1.1.4.3.14.5 <operationStatus>

Návratová hodnota	Popis
int	Stav provedení operace. 0 = v pořádku.

6.1.1.4.3.14.6 <operationStatusInfo>

Návratová hodnota	Popis
string	Textová zpráva odpovídající stavu provedení operace

6.1.1.4.3.14.7 <fileName>

Návratová hodnota	Popis
string	Název souboru, ze kterého byl podpis uchován. Max. 260 znaků.

6.1.1.4.3.14.8 <fileSize>

Návratová hodnota	Popis
string	Velikost souboru, ze kterého byl podpis uchován

6.1.1.4.3.14.9 <hashIn>

Návratová hodnota	Popis
string	Hash souboru, který měl dokument na vstupu

6.1.1.4.3.14.10 <hashOut>

Návratová hodnota	Popis
string	Hash souboru, který měl dokument na výstupu

6.1.1.4.3.14.11 <userComment>

Návratová hodnota	Popis
string	Vlastní komentář nebo popis dokumentu uživatelem

6.1.1.4.3.14.12 </PreservationRecord>

6.1.1.4.3.15 </preservationHistory>

6.1.1.4.3.16 <docType>

Návratová hodnota	Popis
UNKNOWN	Neznámý typ dokumentu
CMSPKCS7	Dokument podepsaný interním CMS/PKCS7 podpisem
CMSPKCS7Ext	Dokument podepsaný externím CMS/PKCS7 podpisem
PDF	Podepsaný PDF dokument
XML	Podepsaná XML data
XML602FORM	Podepsané datové zprávy z Informačního systému datových schránek a FO/ZFO formuláře aplikace Software602 Form Filler
XMLISDOC	Podepsaná XML ISDOC data
ASiC_S_CAdES	ASiC-Simple s CAdES podpisem
ASiC_S_XAdES	ASiC-Simple s XAdES podpisem
ASiC_S_Tst	ASiC-Simple s Timestamp
ASiC_E_CAdES_Tst	ASiC-Extended s CAdES podpisem nebo s Timestamp
ASiC_E_XAdES	ASiC-Extended s XAdES podpisem
MS_WORD	Podepsaný dokument aplikace MS Word

MS_EXCEL	Podepsaný dokument aplikace MS Excel
MS_PWR_PNT	Podepsaný dokument aplikace MS Powerpoint
ODF	Podepsaný OpenDocumentFormat (OpenOffice)

6.1.1.4.4 </PreservationInfo>

6.1.1.4.5 <DocInfo> - struktura elementu se vrací pouze v případě, kdy nelze provést registraci vstupního dokumentu

6.1.1.4.5.1 <CreationDateTime>

Návratová hodnota	Popis
dateTime	Datum a čas, kdy došlo k vytvoření reportu o uchování

6.1.1.4.5.2 <FileName>

Návratová hodnota	Popis
string	Název vstupního souboru (včetně přípony), ze kterého byly ověřeny podpisy. Max. 260 znaků.

6.1.1.4.5.3 <FileSize>

Návratová hodnota	Popis
Long	Velikost vstupního souboru (v bajtech)

6.1.1.4.5.4 <PDFVersion>

Návratová hodnota	Popis
string	Verze PDF dokumentu. Např. 1.4, 1.5, 1.7

6.1.1.4.5.5 <PDFNumOfPages>

Návratová hodnota	Popis
Int	Počet stránek v PDF dokumentu

6.1.1.4.5.6 <docType>

Návratová hodnota	Popis
UNKNOWN	Neznámý typ dokumentu
CMSPKCS7	Dokument podepsaný interním CMS/PKCS7 podpisem
CMSPKCS7Ext	Dokument podepsaný externím CMS/PKCS7 podpisem
PDF	Podepsaný PDF dokument
XML	Podepsaná XML data
XML602FORM	Podepsané datové zprávy z Informačního systému datových schránek a FO/ZFO formuláře aplikace Software602 Form Filler

XMLISDOC	Podepsaná XML ISDOC data
ASiC_S_CAdES	ASiC-Simple s CAdES podpisem
ASiC_S_XAdES	ASiC-Simple s XAdES podpisem
ASiC_S_Tst	ASiC-Simple s Timestamp
ASiC_E_CAdES_Tst	ASiC-Extended s CAdES podpisem nebo s Timestamp
ASiC_E_XAdES	ASiC-Extended s XAdES podpisem
MS_WORD	Podepsaný dokument aplikace MS Word
MS_EXCEL	Podepsaný dokument aplikace MS Excel
MS_PWR_PNT	Podepsaný dokument aplikace MS Powerpoint
ODF	Podepsaný OpenDocumentFormat (OpenOffice)

6.1.1.4.5.7 <expiration>

Návratová hodnota	Popis
DateTime	Datum a čas vypršení ověřitelnosti celého dokumentu. Po tomto datu nebude možné ověřit platnost podpisových certifikátů a zajistit další ověřitelnost, uchování a platnost dokumentu.

6.1.1.4.5.8 <docDataHash>

Návratová hodnota	Popis
Base64Binary	Hash analyzovaného dokumentu v kódování Base64. Algoritmus výpočtu hashe je v následujícím elementu docDataHashAlg.

6.1.1.4.5.9 <docDataHashAlg>

Návratová hodnota	Popis
String	Algoritmus výpočtu hashe analyzovaného dokumentu. Ve tvaru například: 2.16.840.1.101.3.4.2.1.

6.1.1.4.5.10 <currSignHashAlg>

Návratová hodnota	Popis
String	Algoritmus výpočtu hashe posledního podpisu. Příklad: 2.16.840.1.101.3.4.2.1

6.1.1.4.5.11 <globalStatus>

Návratová hodnota	Popis
String	Sumarizuje stav dokumentu na základě všech podpisů a časových razítek. Může nabývat hodnot: OK = 0 (Všechny podpisy a dokumentová časová razítka jsou platná; TOTAL_PASSED dle normy ETSI[2]) WARNING = 1 (Nelze určit platnost některých podpisových certifikátů nebo dokumentových časových razítek; INDETERMINATE dle normy ETSI[2]))

	ERROR = 2 (Některé podpisy nebo dokumentová časová razítka jsou neplatná, např. odvolaný certifikát, poškozený hash dokumentu, změny po podepsání atd.; TOTAL_FAILED dle normy ETSI[2])) NO_SIGNATURES = 3 (Dokument neobsahuje žádné podpisy ani dokumentová časová razítka)

6.1.1.4.6 <sigInfos>

6.1.1.4.6.1 <SigInfo>

Informace o podpisu (opakující se element v případě více podpisů).

6.1.1.4.6.1.1 <status>

Návratová hodnota	Popis
String	Výsledný stav ověření podpisu podle první verze ETSI normy[1] týkající se ověřování PAdES, CAdES, XAdES a ASiC.

6.1.1.4.6.1.2 <statusEN>

Návratová hodnota	Popis
String	Výsledný stav ověření podpisu podle aktuální verze ETSI normy[2] týkající se ověřování PAdES, CAdES, XAdES a ASiC, viz hodnoty Indication a subIndication v Preserve_register/update/getInfo

6.1.1.4.6.1.3 <message>

Návratová hodnota	Popis
string	Podrobnosti ověření stavu podpisu/pečeti/razítka, pokud jsou u daného stavu k dispozici.

6.1.1.4.6.1.4 <certType>

Návratová hodnota	Popis
string	Typ certifikátu podpisu/pečeti/razítka. Může nabývat hodnot: COMMERCIAL = Komerční certifikát pro autentizaci QUALIFIED = Kvalifikovaný certifikát pro elektronický podpis/pečeť vydaný kvalifikovaným poskytovatelem služeb vydávání certifikátů TRUSTED = Certifikát pro elektronický podpis/pečeť vydaný kvalifikovaným poskytovatelem služeb vydávání certifikátů INTERNAL = Privátní certifikát UNKNOWN = Neznámý OST = Důvěryhodný certifikát operačního systému

6.1.1.4.6.1.5 <adesType>

Návratová hodnota	Popis
string	Typ podpisového certifikátu dle standardu AdES (Advanced Electronic Signature)

6.1.1.4.6.1.6 <eidasType>

Návratová hodnota	Popis
string	Typ podpisového certifikátu dle nařízení eIDAS. Může nabývat hodnot: ADVANCED_SIGNATURE = Zaručený elektronický podpis ACREDITED_SIGNATURE = Uznávaný elektronický podpis (Zaručený elektronický podpis založený na kvalifikovaném certifikátu) QUALIFIED_SIGNATURE = Uznávaný elektronický podpis (Kvalifikovaný elektronický podpis založený na kvalifikovaném certifikátu a vytvořený na kvalifikovaném prostředku) ADVANCED_SEAL = Zaručená elektronická pečeť TRUSTED_SEAL = Zaručená elektronická pečeť, založená na certifikátu pro elektronické pečeti od kvalifikovaného poskytovatele služeb vytvářejících důvěru ACREDITED_SEAL = Uznávaná elektronická pečeť (Zaručená elektronická pečeť založená na kvalifikovaném certifikátu pro elektronické pečeti) QUALIFIED_SEAL = Kvalifikovaná eletronická pečeť založená na kvalifikovaném certifikátu od kvalifikovaného poskytovatele služeb vytvářejících důvěru TIMESTAMP = Elektronické časové razítko QUALIFIED_TIMESTAMP = Kvalifikované elektronické časové razítko

6.1.1.4.6.1.7 <baselineType>

Návratová hodnota	Popis
string	Typ podpisového certifikátu dle Baseline profilu. Může nabývat hodnot: BaselineType_LEGACY=Neodpovídá žádnému Baseline profilu CADES_B = CAdES B-B (Baseline B) CADES_T = CAdES B-T (Baseline T) CADES_LT = CAdES B-LT (Baseline LT) CADES_LTA = CAdES B-LTA (Baseline LTA) PADES_B = PAdES B-B (Baseline B) PADES_T = PAdES B-T (Baseline T) PADES_LT = PAdES B-LT (Baseline LT) PADES_LTA = PAdES B-LTA (Baseline LTA) XADES_B = XAdES B-B (Baseline B) XADES_T = XAdES B-T (Baseline T) XADES_LT = XAdES B-LT (Baseline LT) XADES_LTA = XAdES B-LTA (Baseline LTA) ASIC_B = ASiC B-B (Baseline B) ASIC_T = ASiC B-T (Baseline T) ASIC_LT = ASiC B-LT (Baseline LT) ASIC_LTA = ASiC B-LTA (Baseline LTA)

6.1.1.4.6.1.8 <signCert>

6.1.1.4.6.1.9 <Name>

Návratová hodnota	Popis
string	Jméno podepisujího tak, jak je uvedeno v certifikátu

6.1.1.4.6.1.10 <Subject>

Návratová hodnota	Popis
string	Informace z certifikátového atributu Subjekt, např.: CN = Common Name (Běžné jméno) GN = Given Name (Křestní jméno) SN = Surname (Příjmení) SERIALNUMBER = Sériové číslo C = Country (Země) L = Locality (Lokalita) E = Email O = Organization (Organizace) OU =Organizational unit (Organizační jednotka) Pseudonyme = pseudonym

6.1.1.4.6.1.11 <IssuerName>

Návratová hodnota	Popis
string	Jméno vystavitele certifikátu z CN v atributu Issuer

6.1.1.4.6.1.12 <Issuer>

Návratová hodnota	Popis
string	Kompletní informace o vystaviteli certifikátu z atributu Issuer

6.1.1.4.6.1.13 <Serial>

Návratová hodnota	Popis
string	Sériové číslo certifikátu

6.1.1.4.6.1.14 <NotBefore>

Návratová hodnota	Popis
string	Platnost certifikátu od

6.1.1.4.6.1.15 <NotAfter>

Návratová hodnota	Popis
string	Platnost certifikátu do

6.1.1.4.6.1.16 <Hash>

Návratová hodnota	Popis
string	Hash veřejného klíče certifikátu algoritmu SHA256

6.1.1.4.6.1.17 <Data>

Návratová hodnota	Popis
string	Data veřejného klíče certifikátu

6.1.1.4.6.1.18 </signCert>

6.1.1.4.6.1.19 <qcStatements>

6.1.1.4.6.1.20 <string>

Návratová hodnota	Popis
string	Prohlášení vystavitele kvalifikovaného certifikátu ve formě OID.

6.1.1.4.6.1.21 </qcStatements>

6.1.1.4.6.1.22 <qcType>

Návratová hodnota	Popis
string	Typ certifikátu podpisu/pečeti/razítka dle eIDAS, pouze u CertType QUALIFIED a LEGACY.

6.1.1.4.6.1.23 <signCertIsPseudonyme>

Návratová hodnota	Popis
boolean	Určuje, zda je certifikát (podpisu/pečeti/razítka) vystaven na pseudonym

6.1.1.4.6.1.24 <time>

Návratová hodnota	Popis
dateTime	Důvěryhodný časový údaj podpisu/pečeti/razítka

6.1.1.4.6.1.25 <timeFromComputerClock>

Návratová hodnota	Popis
dateTime	Časový údaj podpisu/pečeti/razítka z hodin počítače autora

6.1.1.4.6.1.26 <validTo>

Návratová hodnota	Popis
dateTime	Platnost podpis/pečeti/razítka do

6.1.1.4.6.2 <certPath>

6.1.1.4.6.2.1 <CertInfo>

Návratová hodnota	Popis
dateTime	Platnost podpis/pečeti/razítka do

6.1.1.4.6.2.2 Name>

Návratová hodnota	Popis
string	Jméno podepisujího tak, jak je uvedeno v certifikátu

6.1.1.4.6.2.3 <Subject>

Návratová hodnota	Popis
string	Informace z atributu certifikátu Subjekt, např. CN=Common Name (Běžné jméno) GN=Given Name (Křestní jméno) SN=Surname (Příjmení) SERIALNUMBER=seriové číslo certifikátu C=Country (Země) L=Locality (Lokalita) E=Email O= Organization (Organizace) OU=Organizational unit (Organizační jednotka) Pseudonym=pseudonym

6.1.1.4.6.2.4 <IssuerName>

Návratová hodnota	Popis
string	Jméno vystavitele certifikátu z CN= v atributu Issuer

6.1.1.4.6.2.5 <Issuer>

Návratová hodnota	Popis
string	Kompletní informace o vystaviteli certifikátu z atributu Issuer

6.1.1.4.6.2.6 <Serial>

Návratová hodnota	Popis
string	Sériové číslo certifikátu

6.1.1.4.6.2.7 <NotBefore>

Návratová hodnota	Popis
string	Platnost certifikátu od

6.1.1.4.6.2.8 <NotAfter>

Návratová hodnota	Popis
string	Platnost certifikátu do

6.1.1.4.6.2.9 <Hash>

Návratová hodnota	Popis
string	Hash veřejného klíče certifikátu algoritmu SHA256

6.1.1.4.6.2.10 <ServiceStatusUri>

Návratová hodnota	Popis
String	Obsahuje celou Uri stanovující servisní stav certifikátu na TSL, např. http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

6.1.1.4.6.2.11 <ServiceTypeUri>

Návratová hodnota	Popis
String	Obsahuje celou Uri stanovující servisní typ certifikátu na TSL, např. http://uri.etsi.org/TrstSvc/Svctype/CA/QC

6.1.1.4.6.2.12 <IsTrustAnchor>

Návratová hodnota	Popis
Boolean	Definuje, zda je certifikát uveden na TSL

6.1.1.4.6.2.13 <Data>

Návratová hodnota	Popis
string	Data veřejného klíče certifikátu

6.1.1.4.6.3 </certPath>

6.1.1.4.6.4 <crlPath>

6.1.1.4.6.4.1 <RevocationData>

6.1.1.4.6.4.2 <Type>

Návratová hodnota	Popis
string	Typ revokačních dat. Může být: CRL, OCSP

6.1.1.4.6.4.3 <Issuer>

Návratová hodnota	Popis
string	Vystavitel revokačních dat (pouze u CRL)

6.1.1.4.6.4.4 <Serial>

Návratová hodnota	Popis
string	Sériové číslo revokačních dat (pouze u CRL)

6.1.1.4.6.4.5 <ThisUpdate>

Návratová hodnota	Popis
dateTime	Datum a čas poslední aktualizace revokačních dat.

6.1.1.4.6.4.6 <NextUpdate>

Návratová hodnota	Popis
dateTime	Datum a čas následující aktualizace revokačních dat.

6.1.1.4.6.4.7 <Hash>

Návratová hodnota	Popis
string	Hash revokačních dat.

6.1.1.4.6.4.8 <Data>

Návratová hodnota	Popis
string	Revokační data CRL v base64 na základě kterých se ověřovala platnost podpisu/pečeti/razítka

6.1.1.4.6.4.9 <Source>

Návratová hodnota	Popis
string	Zdroj revokačních dat, nabývá hodnot: SECUSIGN - v případě revokačních dat stažených ze serveru Secusign ONLINE - v případě revokačních dat stažených z jejich online zdroje CUSTOM - v případě revokačních dat poskytnutých uživatelem PADES_DSS_VRI - v případě revokačních dat uložených v PDF dokumetu XADES_UNSIGNED_SIGNATURE_PROPERTIES - v případě revokačních dat uložených v nepodepsané části XAdES podpisu CADES_SIGNED_DATA - v případě revokačních dat uložených v podepsané části CAdES podpisu CADES_UNSIGNED_ATTRIBUTES - v případě revokačních dat uložených v nepodepsané části CAdES podpisu UNKNOWN - neznámý zdroj revokačních dat nebo není vyplněno CERTIFICATE_FROM_SIGNATURE - certifikát pocházející z dokumentu/podpisu TS_CERTIFICATE_FROM_SIGNATURE - certifikát TS pocházející z dokumentu/podpisu DOC_INFO - certifikáty pocházející z DocInfo -> DocInfoTslProvider

6.1.1.4.6.4.10 <DistributionPointChecked>

Návratová hodnota	Popis
boolean	Informace, zda byl kontrolován distribuční bod CRL. Není vždy potřebné.

6.1.1.4.6.4.11 <DistributionPoint>

Návratová hodnota	Popis
string	URL distribučního bodu.

6.1.1.4.6.4.12 <DistributionPointCheckDate>

Návratová hodnota	Popis
dateTime	Datum a čas kontroly distribučního bodu.

6.1.1.4.6.4.13 <DistributionPointThisUpdate>

Návratová hodnota	Popis
dateTime	Informace z distribučního bodu CRL o datumu a času vydání této aktualizace. Pokud CRL pro časové razítko byl vydán před rozhodným okamžikem, hledá se novější na DistributionPoint a pokud není k dispozici novější, nebyl v DistributionCheckDate certifikát časového razítka revokován.

6.1.1.4.6.4.14 <DistributionPointHash>

Návratová hodnota	Popis
string	Hash distribučního bodu CRL.

6.1.1.4.6.4.15 </RevocationData>

6.1.1.4.6.5 </crlPath>

6.1.1.4.6.6 <lastHashAlgOid>

Návratová hodnota	Popis
dateTime	Jedná se o poslední použitý OID digest algoritmus v SignerInfo (CMS, PDF). Příklad pro SHA256 algoritmus: 2.16.840.1.101.3.4.2.1

6.1.1.4.6.7 <id>

Návratová hodnota	Popis
unsignedInt	Pořadové číslo podpisu tak, jak byl přidán do dokumentu. Počítáno od nuly.

6.1.1.4.6.8 <sid>

Návratová hodnota	Popis
string	Unikátní identifikátor podpisu.

6.1.1.4.6.9 <DecisiveMoment>

Návratová hodnota	Popis
dateTime	Rozhodný okamžik je čas, ke kterému rozhodujeme o dané entitě (podpisu/razítku). Jedná se vlastně o Proof of Existence, ke kterému entitu ověřujeme. Pokud není k dispozici datum a čas časového razítka použije se ValidationTime (případně aktuální datum).

6.1.1.4.6.10 <DecisiveMomentSource>

Návratová hodnota	Popis

string	Informace o původu času rozhodného okamžiku pro vyhodnocení podpisu. Hodnoty: VALIDATION_DATE - ověřovalo se k datu validace, CUSTOM_VALIDATION_DATE - ověřovalo se k datu validace zadaného uživatelem, TIMESTAMP - ověřovalo se k datu z razítka, CLAIMED_TIME - ověřovalo se k datu z tzv. claimedTime tedy hodnoty pocházející z hodin počítače autora podpisu

6.1.1.4.6.11 <sigTimestamps> nepovinný element, je závislý na existenci časového razítka u podpisu

Návratová hodnota	Popis
XML struktura	Informace o časovém razítku přidaném jako atribut k digitálnímu podpisu. Stejná XML struktura informací jako u nadřazeného podpisu. Tedy obsahuje element *SigInfo*, viz výše, včetně všech jeho potomků. Informace v potomcích se váží k certifikátu časového razítka.

6.1.1.4.6.12 <sigType>

Návratová hodnota	Popis
enum	Typ podpisu. Může nabývat hodnot: UNKNOWN - neznámý STANDARD – standardní XML602FORM_TECHNICAL – formulářový Software602

6.1.1.4.6.13 <xmlSignedReferences> nepovinný element, je závislý na formátu vstupního souboru (jen pro XML/ZFO)

Návratová hodnota	Popis
XML struktura	Data podpisu

6.1.1.4.6.14 <pdfByteRange> nepovinný element, je závislý na formátu vstupního souboru (jen pro PDF)

Návratová hodnota	Popis
XML struktura	Bytový rozsah PDF podpisů

6.1.1.4.6.15 <hasFurtherChanges>

Návratová hodnota	Popis
Boolean	Údaj, zda byly v dokumentu provedeny změny po podpisu. Hodnoty: false, true

6.1.1.4.6.16 <Reason>

Návratová hodnota	Popis
String	Důvod podepsání dokumentu.

6.1.1.4.6.17 <Location>

Návratová hodnota	Popis
String	Místo podepsání dokumentu.

6.1.1.4.6.18 <Contact>

Návratová hodnota	Popis
String	Kontaktní informace k podepsání dokumentu.

6.1.1.4.7 </DocInfo>

6.1.1.4.8 <StatusMessage>

Návratová hodnota	Popis
String	Textová zpráva odpovídající celkovému výsledku uchování elektronických podpisů ve službě SecuSign. Hodnota je naplněna pouze v případě problematického výsledku.

6.1.2 Metoda Preserve_update

Umožňuje prodloužit platnost uchovaných podpisů v dokumentu přidáním dalšího kvalifikovaného časového razítka a revokačních dat - informací souvisejících s ověřením podpisu jako jsou odpovědi OCSP/CRL na všechny certifikáty v řetězci, tj. od podpisového certifikátu ke kořenovému certifikátu vystavitele (certifikační autority), díky čemuž se zajistí jejich další ověřitelnost.

Popis služby včetně WSDL schématu a příklad požadavku a odpovědi pro SOAP 1.1 a SOAP 1.2 je umístěn na https://localhost/secusign/default.asmx?op=Preserve_update *

* localhost je název používaný pro lokální počítač; namísto něj zvolte jméno/IP adresu SDK serveru (dle nastavení v IIS)

6.1.2.1 Požadavek v rozhraní SOAP 1.1

```
POST /secusign/default.asmx HTTP/1.1
Host: localhost
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://software602.com/secusign/Preserve_update"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <Preserve_update xmlns="http://software602.com/secusign/">
      <DocID>string</DocID>
      <FileName>string</FileName>
      <FileData>base64Binary</FileData>
      <FileType>UNKNOWN or CMSPKCS7 or CMSPKCS7Ext or PDF or XML or XML602FORM or
XMLISDOC or ASiC_S_CAdES or ASiC_S_XAdES or ASiC_S_Tst or ASiC_E_CAdES_Tst or
ASiC_E_XAdES or MS_WORD or MS_EXCEL or MS_PWR_PNT or ODF</FileType>
      <ExternalSignatureFileName>string</ExternalSignatureFileName>
      <ExternalSignature>base64Binary</ExternalSignature>
      <SortInfo>string</SortInfo>
      <UserComment>string</UserComment>
      <Params>string</Params>
    </Preserve_update>
```

```
  </soap:Body>
</soap:Envelope>
```

6.1.2.2 Vstupní parametry metody

6.1.2.2.1 <DocID>

[povinný element]

Vstup	Popis
string	Jednoznačné identifikační číslo uchovaných elektronických podpisů v dokumentu. Bylo automaticky vygenerováno při procesu uchování ve službě SecuSign. Lze jej najít v uživatelském rozhraní účtu. Max. 128 znaků.

6.1.2.2.2 <FileName>

[povinný element]

Vstup	Popis
String	Název vstupního souboru (včetně přípony) pro uchování elektronických podpisů. Příklad: Dokument.pdf Max. 260 znaků.

6.1.2.2.3 <FileData>

[povinný element]

Vstup	Popis
Base64Binary	Data vstupního souboru kódovaná v base64

6.1.2.2.4 <FileType>

[povinný element]

Vstup	Popis
UNKNOWN	Neznámý typ dokumentu
CMSPKCS7	Dokument podepsaný interním CMS/PKCS7 podpisem
CMSPKCS7Ext	Dokument podepsaný externím CMS/PKCS7 podpisem
PDF	Podepsaný PDF dokument
XML	Podepsaná XML data
XML602FORM	Podepsané datové zprávy z Informačního systému datových schránek a FO/ZFO formuláře aplikace Software602 Form Filler
XMLISDOC	Podepsaná XML ISDOC data
ASiC_S_CAdES	ASiC-Simple s CAdES podpisem
ASiC_S_XAdES	ASiC-Simple s XAdES podpisem
ASiC_S_Tst	ASiC-Simple s Timestamp
ASiC_E_CAdES_Tst	ASiC-Extended s CAdES podpisem nebo s Timestamp
ASiC_E_XAdES	ASiC-Extended s XAdES podpisem
MS_WORD	Dokument aplikace MS Word

MS_EXCEL	Dokument aplikace MS Excel
MS_PWR_PNT	Dokument aplikace MS Powerpoint
ODF	Podepsaný OpenDocumentFormat (OpenOffice)

6.1.2.2.5 <ExternalSignatureFileName>

[nepovinný element]

Vstup	Popis
string	Název souboru externího podpisu. Pouze v případě, že k dokumentu byl takový podpis vytvořen.

6.1.2.2.6 <ExternalSignature>

[nepovinný element]

Vstup	Popis
Base64Binary	Data externího podpisu kódovaná v base64. Pouze v případě, že k dokumentu byl takový podpis vytvořen.

6.1.2.2.7 <SortInfo>

[nepovinný element]

Vstup	Popis
String	Zatřiďovací informace – např. název složky, nebo struktura vnořených složek, ve kterých je dokument u uživatele evidován. Max. 100 znaků.

6.1.2.2.8 <UserComment>

[nepovinný element]

Vstup	Popis
String	Vlastní komentář nebo popis uživatele k uchovanému dokumentu

6.1.2.2.9 <Params>

[nepovinný element]

Vstup	Popis
String	Volitelné, obsahuje další parametry. Zatím se nevyužívá.

6.1.2.3 Struktura odpovědi na požadavek

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <Preserve_updateResponse xmlns="http://software602.com/secusign/">
      <Preserve_updateResult>int</Preserve_updateResult>
      <OutputData>base64Binary</OutputData>
      <PreservationInfo>
```

```
        <CreationDateTime>dateTime</CreationDateTime>
        <docId>string</docId>
        <fileName>string</fileName>
        <fileSize>long</fileSize>
        <sortInfo>string</sortInfo>
        <lastUpdate>dateTime</lastUpdate>
        <expiration>dateTime</expiration>
        <docDataHash>base64Binary</docDataHash>
        <docDataHashAlg>string</docDataHashAlg>
        <currSignHashAlg>string</currSignHashAlg>
        <sigValidityCondition>ALL or AT_LEAST_ONE or LAST</sigValidityCondition>
        <sigsPreservationStatus>
          <PreservationInfo>
            <sid>string</sid>
            <sigStatus xsi:nil="true" />
            <extendedValidationEndDate>dateTime</extendedValidationEndDate>
            <signingCertSubject>string</signingCertSubject>
            <bIsDocTimeStamp>boolean</bIsDocTimeStamp>
            <procesStatus>string</procesStatus>
          </PreservationInfo>
          <PreservationInfo>
            <sid>string</sid>
            <sigStatus xsi:nil="true" />
            <extendedValidationEndDate>dateTime</extendedValidationEndDate>
            <signingCertSubject>string</signingCertSubject>
            <bIsDocTimeStamp>boolean</bIsDocTimeStamp>
            <procesStatus>string</procesStatus>
          </PreservationInfo>
        </sigsPreservationStatus>
        <preservationHistory>
          <PreservationRecord>
            <id>int</id>
            <operationTime>dateTime</operationTime>
            <operationType>REGISTER or UPDATE or UNREGISTER or UNKNOWN</operationType>
            <operationStatus>int</operationStatus>
            <operationStatusInfo>string</operationStatusInfo>
            <fileName>string</fileName>
            <fileSize>long</fileSize>
            <hashIn>string</hashIn>
            <hashOut>string</hashOut>
            <userComment>string</userComment>
          </PreservationRecord>
          <PreservationRecord>
            <id>int</id>
            <operationTime>dateTime</operationTime>
            <operationType>REGISTER or UPDATE or UNREGISTER or UNKNOWN</operationType>
            <operationStatus>int</operationStatus>
            <operationStatusInfo>string</operationStatusInfo>
            <fileName>string</fileName>
            <fileSize>long</fileSize>
            <hashIn>string</hashIn>
            <hashOut>string</hashOut>
            <userComment>string</userComment>
          </PreservationRecord>
        </preservationHistory>
        <docType>string</docType>
      </PreservationInfo>
      <StatusMessage>string</StatusMessage>
    </Preserve_updateResponse>
  </soap:Body>
</soap:Envelope>
```

6.1.2.4 Výstupní parametry metody

6.1.2.4.1 <Preserve_updateResult>

Návratová hodnota	Popis
Int	Výsledek metody Preserve_update (ošetření dokumentu s elektronickými podpisy). 0 = v pořádku, jinak Návratové kódy všech metod a chyba popsaná ve StatusMessage.

6.1.2.4.2 <OutputData>

Návratová hodnota	Popis
Base64Binary	Data uchovaného dokumentu s ošetřenými elektronickými podpisy kódována v base64

6.1.2.4.3 <Info>

6.1.2.4.3.1 <CreationDateTime>

Návratová hodnota	Popis
dateTime	Datum a čas, kdy došlo k vytvoření reportu o uchování dokumentu s elektronickými podpisy

6.1.2.4.3.2 <docID>

Návratová hodnota	Popis
String	Jednoznačné identifikační číslo uchovaného dokumentu s ošetřenými elektronickými podpisy. Bylo automaticky vygenerováno při procesu uchování ve službě SecuSign. Pod tímto číslem je možné v metodě *Preserve_getInfo* zjistit informace o uchovaném dokumentu Max. 128 znaků.

6.1.2.4.3.3 <fileName>

Návratová hodnota	Popis
String	Název uchovaného souboru s elektronickými podpisy. Max. 260 znaků.

6.1.2.4.3.4 <fileSize>

Návratová hodnota	Popis
Long	Velikost uchovaného souboru s elektronickými podpisy

6.1.2.4.3.5 <sortInfo>

Návratová hodnota	Popis
String	Zatřiďovací informace – např. název složky, nebo struktura vnořených složek, ve kterých je dokument u uživatele evidován. Max. 100 znaků.

6.1.2.4.3.6 <lastUpdate>

Návratová hodnota	Popis

dateTime	Datum a čas posledního prodloužení platnosti a ověřitelnosti dokumentu s elektronickými podpisy

6.1.2.4.3.7 <expiration>

Návratová hodnota	Popis
dateTime	Datum a čas vypršení ověřitelnosti platnosti celého dokumentu. Po tomto datu nebude možné ověřit platnost certifikátů podpisů / pečetí / razítek a zajistit další ověřitelnost a platnost uchovaného dokumentu.

6.1.2.4.3.8 <docDataHash>

Návratová hodnota	Popis
Base64Binary	Hash analyzovaného dokumentu kódovaný v Base64. Algoritmus výpočtu hashe je v následujícím elementu docDataHashAlg.

6.1.2.4.3.9 <docDataHashAlg>

Návratová hodnota	Popis
String	Algoritmus výpočtu hashe analyzovaného dokumentu. Ve tvaru například: 2.16.840.1.101.3.4.2.1

6.1.2.4.3.10 <currSignHashAlg>

Návratová hodnota	Popis
String	Algoritmus výpočtu hashe posledního podpisu. Příklad: 2.16.840.1.101.3.4.2.1

6.1.2.4.3.11 <sigValidityCondition>

Návratová hodnota	Popis
String	Podmínky platnosti podpisu pro další uchování. Hodnoty: ALL – všechny podpisy jsou platné AT_LEAST_ONE – alespoň jeden podpis je platný LAST – poslední podpis je platný

6.1.2.4.3.12 <sigsPreservationStatus>

6.1.2.4.3.12.1 <PreservationInfo> - opakující se element podle počtu podpisů v dokumentu

6.1.2.4.3.12.2 <sid>

Návratová hodnota	Popis
String	Identifikátor podpis, který k danému uchovanému dokumentu eviduje služba SecuSign

6.1.2.4.3.12.3 <sigStatus>

6.1.2.4.3.12.4 <indication>

Návratová hodnota	Popis

String	Stav ověření podpisu – indikace. Může nabývat hodnot: VALID – platný (TOTAL_PASSED dle normy ETSI[2]) INVALID – neplatný (TOTAL_FAILED dle normy ETSI[2]) INDETERMINATE – neurčitý UNKNOWN - neznámý

6.1.2.4.3.12.5 <subindication>

Návratová hodnota	Popis
string	Podstav ověření podpisu - subindikace. Nabývá hodnot (odpovídajících normě ETSI[2]): VALID – Elektronický certifikát nebyl v okamžiku podepsání revokovaný nebo expirovaný a podpis je možné prohlásit za platný. INVALID_REVOKED - Podpisový certifikát byl odvolán ještě před okamžikem pořízení podpisu. Podpis je neplatný. INVALID_HASH_FAILURE - Elektronický podpis je porušený a od podepsání dokumentu zřejmě došlo ke změně podepsané části jeho obsahu. Kontrolní součet uvedený v podpisu nesouhlasí s kontrolním součtem podepsané části! Podpis je neplatný. INVALID_SIG_CRYPTO_FAILURE - Nepodařilo se ověřit příslušnost veřejného klíče k podpisu. Podpis je neplatný. INVALID_FORMAT_FAILURE - Podepsaná data nebyla rozpoznána, formát podpisu je porušený. Podpis je neplatný. INDETERMINATE_NO_CERTIFICATE_CHAIN_FOUND - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Nepodařilo se získat všechny potřebné informace pro kontrolu důvěryhodnosti a odvolání certifikátu. INDETERMINATE_NO_POE - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Nepodařilo se získat všechny potřebné informace pro kontrolu důvěryhodnosti a odvolání certifikátu. INDETERMINATE_TRY_LATER - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Kontrolu odvolání certifikátu je možné provést na základě seznamu odvolaných certifikátů (CRL) vydaném po INDETERMINATE_SIGNED_DATA_NOT_FOUND - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout, protože nejsou k dispozici data, jejichž podpis je ověřován. INDETERMINATE_UNKNOWN_SIGNING_TIME - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Nepodařilo se získat všechny potřebné informace pro kontrolu důvěryhodnosti a odvolání certifikátu. INDETERMINATE_UNTRUST_SIGNING_TIME - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Není k dispozici důvěryhodný údaj z časového razítka o času podepsání. INDETERMINATE_GENERAL_ERROR - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Obecná chyba aplikace, kontaktujte správce. INDETERMINATE_REVOKED_NO_POE - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Podpisový certifikát byl odvolán v době ověření, ale je nejistý čas podepsání.

	INDETERMINATE_REVOKED_CA_NO_POE - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Nejméně jeden řetěz certifikátu byl nalezen, ale certifikát zprostředkující CA je revokován. INDETERMINATE_OUT_OF_BOUNDS_NO_POE - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Podpisový certifikát vypršel nebo ještě nenastala jeho platnost v době ověření a algoritmus ověřování podpisu nemůže zjistit, že čas podepsání leží uvnitř intervalu platnosti podpisového certifikátu. INDETERMINATE_EXPIRED - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Podpisový certifikát vypršel. Podpis byl vytvořen po datu expirace (notAfter) podpisového certifikátu. INDETERMINATE_NOT_YET_VALID - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Podpisový certifikát nebyl ještě platný v době ověřování. Čas podepsání leží před datumem vydání (notBefore) podpisového certifikátu. INDETERMINATE_POLICY_PROCESSING_ERROR - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Soubor dané formální politiky z nějakého důvodu nemohl být zpracován (např. není přístupný, není zpracovatelný, nesouhlasí kontrolní algoritmus, atd.) INDETERMINATE_TIMESTAMP_ORDER_FAILURE - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Některá omezení v pořadí podpisu časových razítek a/nebo podepsaných datových objektů časových razítek nejsou respektována. INDETERMINATE_SIG_CONSTRAINTS_FAILURE - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Nejsou splněna omezení podpisu (chybějící podpisové atributy, nesouhlasná politika el. podpisu, apod.). INDETERMINATE_CHAIN_CONSTRAINTS_FAILURE - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Obecná chyba při sestavování certifikační cesty. INDETERMINATE_CRYPTO_CONSTRAINTS_FAILURE - Alespoň jeden z algoritmů, které byly použity v materiálu (např. hodnota podpisu, certifikát, ...) zapojeném v ověřování podpisu, nebo velikost klíče použita s tímto algoritmem, je pod požadovanou úroveň kryptografického zabezpečení, a tento materiál byl produkován po čase, kdy byl tento algoritmus/klíč považován za bezpečný (je-li znám takový čas), a materiál není chráněn dostatečně silným časovým razítkem aplikovaným před dobou ve které byl algoritmus považován za bezpečný (je-li znám takový čas).

6.1.2.4.3.12.6 </sigStatus>

6.1.2.4.3.12.7 <extendedValidationEndDate>

Návratová hodnota	Popis
dateTime	Datum a čas do kdy byla prodloužena ověřitelnost podpisu

6.1.2.4.3.12.8 <signingCertSubject>

Návratová hodnota	Popis
string	Identifikace podpisového certifikátu, který byl ošetřen

6.1.2.4.3.12.9 <bISDocTimeStamp>

Návratová hodnota	Popis
boolean	Určuje, zda podpis je samostatným časovým razítkem

6.1.2.4.3.12.10 <procesStatus>

Návratová hodnota	Popis
string	Stav ošetření podpisu při uchování. Hodnoty: None – Neproběhlo ošetření podpisu Full – Plně proběhlo ošetření podpisu Partial - Podpis byl ošetřen částečně (neobsahuje všechna validační data) Unknown – Neznámý stav

6.1.2.4.3.12.11 </PreservationInfo>

6.1.2.4.3.13 </sigsPreservationStatus>

6.1.2.4.3.14 <preservationHistory>

6.1.2.4.3.14.1 <PreservationRecord>

6.1.2.4.3.14.2 <id>

Návratová hodnota	Popis
int	Identifikátor provedené operace

6.1.2.4.3.14.3 <operationTime>

Návratová hodnota	Popis
dateTime	Datum a čas provedení operace

6.1.2.4.3.14.4 <operationType>

Návratová hodnota	Popis
PreserveOperation	Typ provedené operace. Hodnoty: REGISTER – uchování dokumentu s elektronickými podpisy UPDATE – prodloužení platnosti a ověřitelnosti elektronických podpisů v dokumentu UNREGISTER – odebrání dokumentu z uchování ve službě SecuSign UNKNOWN – neznámý typ operace

6.1.2.4.3.14.5 <operationStatus>

Návratová hodnota	Popis
Int	Stav provedení operace. 0 = v pořádku.

6.1.2.4.3.14.6 <operationStatusInfo>

Návratová hodnota	Popis
string	Textová zpráva odpovídající stavu provedení operace

6.1.2.4.3.14.7 <fileName>

Návratová hodnota	Popis
string	Název souboru, ze kterého byl podpis uchován. Max. 260 znaků.

6.1.2.4.3.14.8 <fileSize>

Návratová hodnota	Popis
long	Velikost souboru, ze kterého byl podpis uchován

6.1.2.4.3.14.9 <hashIn>

Návratová hodnota	Popis
string	Hash souboru, který měl dokument na vstupu

6.1.2.4.3.14.10 <hashOut>

Návratová hodnota	Popis
string	Hash souboru, který měl dokument na výstupu

6.1.2.4.3.14.11 <userComment>

Návratová hodnota	Popis
string	Vlastní komentář nebo popis dokumentu uživatelem

6.1.2.4.3.14.12 </PreservationRecord>

6.1.2.4.3.15 </preservationHistory>

6.1.2.4.3.16 <docType>

Návratová hodnota	Popis
UNKNOWN	Neznámý typ dokumentu
CMSPKCS7	Dokument podepsaný interním CMS/PKCS7 podpisem
CMSPKCS7Ext	Dokument podepsaný externím CMS/PKCS7 podpisem
PDF	Podepsaný PDF dokument
XML	Podepsaná XML data
XML602FORM	Podepsané datové zprávy z Informačního systému datových schránek a FO/ZFO formuláře aplikace Software602 Form Filler
XMLISDOC	Podepsaná XML ISDOC data
ASiC_S_CAdES	ASiC-Simple s CAdES podpisem

ASiC_S_XAdES	ASiC-Simple s XAdES podpisem
ASiC_S_Tst	ASiC-Simple s Timestamp
ASiC_E_CAdES_Tst	ASiC-Extended s CAdES podpisem nebo s Timestamp
ASiC_E_XAdES	ASiC-Extended s XAdES podpisem
MS_WORD	Podepsaný dokument aplikace MS Word
MS_EXCEL	Podepsaný dokument aplikace MS Excel
MS_PWR_PNT	Podepsaný dokument aplikace MS Powerpoint
ODF	Podepsaný OpenDocumentFormat (OpenOffice)

6.1.2.4.4 </PreservationInfo>

6.1.2.4.5 <StatusMessage>

Návratová hodnota	Popis
String	Textová zpráva odpovídající celkovému výsledku uchování elektronických podpisů ve službě SecuSign. Hodnota je naplněna pouze v případě problematického výsledku.

6.1.3 Metoda Preserve_unregister

Umožňuje odregistrování dokumentu a uchovaných elektronických podpisů z dalšího uchovávání v kvalifikované službě SecuSign.

Popis služby včetně WSDL schématu a příklad požadavku a odpovědi pro SOAP 1.1 a SOAP 1.2 je umístěn na https://localhost/secusign/default.asmx?op=Preserve_unregister *

* localhost je název používaný pro lokální počítač; namísto něj zvolte jméno/IP adresu SDK serveru (dle nastavení v IIS)

6.1.3.1 Požadavek v rozhraní SOAP 1.1

```
POST /secusign/default.asmx HTTP/1.1
Host: localhost
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://software602.com/secusign/Preserve_unregister"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <Preserve_unregister xmlns="http://software602.com/secusign/">
      <DocID>string</DocID>
      <Params>string</Params>
    </Preserve_unregister>
  </soap:Body>
</soap:Envelope>
```

6.1.3.2 Vstupní parametry metody

6.1.3.2.1 <DocID>

[povinný element]

Vstup	Popis
String	Jednoznačné identifikační číslo dokumentu s uchovanými elektronickými podpisy. Bylo automaticky vygenerováno při procesu uchování ve službě SecuSign. Lze jej najít v uživatelském rozhraní účtu. Max. 128 znaků.

6.1.3.2.2 <Params>

[nepovinný element]

Vstup	Popis
String	Volitelné, obsahuje další parametry. Zatím se nevyužívá.

6.1.3.3 Struktura odpovědi na požadavek

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <Preserve_unregisterResponse xmlns="http://software602.com/secusign/">
      <Preserve_unregisterResult>int</Preserve_unregisterResult>
      <StatusMessage>string</StatusMessage>
    </Preserve_unregisterResponse>
  </soap:Body>
</soap:Envelope>
```

6.1.3.4 Výstupní parametry metody

6.1.3.4.1 <Preserve_unregisterResult>

Návratová hodnota	Popis
int	Výsledek metody Preserve_unregister (odregistrování dokumentu s el. podpisy). 0 = v pořádku, jinak Návratové kódy všech metod a chyba popsaná ve StatusMessage.

6.1.3.4.2 <StatusMessage>

Návratová hodnota	Popis
String	Textová zpráva odpovídající celkovému výsledku odregistrování dokumentu s elektronickými podpisy ve službě SecuSign. Hodnota je naplněna pouze v případě problematického výsledku.

6.1.4 Metoda Preserve_getInfo

Umožňuje zjistit informace o dokumentu a uchovaných elektronických podpisech v kvalifikované službě SecuSign. Tyto informace je možné získat v PDF, XML a HTML doložce.

Popis služby včetně WSDL schématu a příklad požadavku a odpovědi pro SOAP 1.1 a SOAP 1.2 je umístěn na https://localhost/secusign/default.asmx?op=Preserve_getInfo *

* localhost je název používaný pro lokální počítač; namísto něj zvolte jméno/IP adresu SDK serveru (dle nastavení v IIS)

6.1.4.1 Požadavek v rozhraní SOAP 1.1

```
POST /secusign/default.asmx HTTP/1.1
Host: localhost
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://software602.com/secusign/Preserve_getInfo"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <Preserve_getInfo xmlns="http://software602.com/secusign/">
      <DocID>string</DocID>
      <FileData>base64Binary</FileData>
      <ExternalSignature>base64Binary</ExternalSignature>
      <Params>string</Params>
      <Properties>
        <ReportLanguage>string</ReportLanguage>
        <GetReport>boolean</GetReport>
        <GetXMLReport>boolean</GetXMLReport>
        <GetHTMLReport>boolean</GetHTMLReport>
        <GetPDFReport>boolean</GetPDFReport>
      </Properties>
    </Preserve_getInfo>
  </soap:Body>
</soap:Envelope>
```

6.1.4.2 Vstupní parametry metody

6.1.4.2.1 <DocID>

[povinný element]

Vstup	Popis
string	Jednoznačné identifikační číslo uchovaných elektronických podpisů v dokumentu. Bylo automaticky vygenerováno při procesu uchování ve službě SecuSign. Lze jej najít v uživatelském rozhraní účtu. Max. 128 znaků.

6.1.4.2.2 <FileData>

[nepovinný element]

Vstup	Popis
Base64Binary	Data vstupního souboru kódovaná v base64

6.1.4.2.3 <ExternalSignature>

[nepovinný element]

Vstup	Popis

Base64Binary	Data externího podpisu kódovaná v base64.

6.1.4.2.4 <Params>

[nepovinný element]

Vstup	Popis
String	Volitelné, obsahuje další parametry. Zatím se nevyužívá.

6.1.4.2.5 <Properties>

[nepovinný element]

6.1.4.2.5.1 <ReportLanguage>

[nepovinný element]

Vstup	Popis
string	Lokalizace textových informací ve výstupní doložce. Hodnoty: cz, en Výchozí hodnota: `cz`

6.1.4.2.5.2 <GetReport>

[nepovinný element]

Vstup	Popis
boolean	Logická hodnota určující, zda se mají informace vygenerovat přímo v odpovědi. Výchozí hodnota: `true`

6.1.4.2.5.3 <GetXMLReport>

[nepovinný element]

Vstup	Popis
boolean	Logická hodnota určující, zda se mají informace vygenerovat do XML doložky. Výchozí hodnota: `false`

6.1.4.2.5.4 <GetHTMLReport>

[nepovinný element]

Vstup	Popis
boolean	Logická hodnota určující, zda se mají informace vygenerovat do HTML doložky. Výchozí hodnota: `false`

6.1.4.2.5.5 <GetPDFReport>

[nepovinný element]

Vstup	Popis
boolean	Logická hodnota určující, zda se mají informace vygenerovat do PDF doložky. Výchozí hodnota: `false`

6.1.4.3 Struktura odpovědi na požadavek

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <Preserve_getInfoResponse xmlns="http://software602.com/secusign/">
      <Preserve_getInfoResult>int</Preserve_getInfoResult>
      <Report>
        <CreationDateTime>dateTime</CreationDateTime>
        <docId>string</docId>
        <fileName>string</fileName>
        <fileSize>long</fileSize>
        <sortInfo>string</sortInfo>
        <lastUpdate>dateTime</lastUpdate>
        <expiration>dateTime</expiration>
        <docDataHash>base64Binary</docDataHash>
        <docDataHashAlg>string</docDataHashAlg>
        <currSignHashAlg>string</currSignHashAlg>
        <sigValidityCondition>ALL or AT_LEAST_ONE or LAST</sigValidityCondition>
        <sigsPreservationStatus>
          <PreservationInfo>
            <sid>string</sid>
            <sigStatus xsi:nil="true" />
            <extendedValidationEndDate>dateTime</extendedValidationEndDate>
            <signingCertSubject>string</signingCertSubject>
            <bIsDocTimeStamp>boolean</bIsDocTimeStamp>
            <procesStatus>string</procesStatus>
          </PreservationInfo>
          <PreservationInfo>
            <sid>string</sid>
            <sigStatus xsi:nil="true" />
            <extendedValidationEndDate>dateTime</extendedValidationEndDate>
            <signingCertSubject>string</signingCertSubject>
            <bIsDocTimeStamp>boolean</bIsDocTimeStamp>
            <procesStatus>string</procesStatus>
          </PreservationInfo>
        </sigsPreservationStatus>
        <preservationHistory>
          <PreservationRecord>
            <id>int</id>
            <operationTime>dateTime</operationTime>
            <operationType>REGISTER or UPDATE or UNREGISTER or UNKNOWN</operationType>
            <operationStatus>int</operationStatus>
            <operationStatusInfo>string</operationStatusInfo>
            <fileName>string</fileName>
            <fileSize>long</fileSize>
            <hashIn>string</hashIn>
            <hashOut>string</hashOut>
            <userComment>string</userComment>
          </PreservationRecord>
          <PreservationRecord>
            <id>int</id>
            <operationTime>dateTime</operationTime>
            <operationType>REGISTER or UPDATE or UNREGISTER or UNKNOWN</operationType>
            <operationStatus>int</operationStatus>
            <operationStatusInfo>string</operationStatusInfo>
            <fileName>string</fileName>
            <fileSize>long</fileSize>
            <hashIn>string</hashIn>
            <hashOut>string</hashOut>
```

```
            <userComment>string</userComment>
          </PreservationRecord>
        </preservationHistory>
        <docType>string</docType>
      </Report>
      <XMLReport>base64Binary</XMLReport>
      <HTMLReport>base64Binary</HTMLReport>
      <PDFReport>base64Binary</PDFReport>
      <StatusMessage>string</StatusMessage>
    </Preserve_getInfoResponse>
  </soap:Body>
</soap:Envelope>
```

6.1.4.4 Výstupní parametry metody

6.1.4.4.1 <Preserve_getInfoResult>

Návratová hodnota	Popis
int	Výsledek metody Preserve_getInfoResult. 0 = v pořádku, jinak Návratové kódy všech metod a chyba popsaná ve StatusMessage.

6.1.4.4.2 <Report>

6.1.4.4.2.1 <CreationDateTime>

Návratová hodnota	Popis
dateTime	Datum a čas, kdy došlo k vytvoření reportu se zjištěnými informacemi o uchovaném dokumentu s elektronickými podpisy

6.1.4.4.2.2 <docID>

Návratová hodnota	Popis
string	Jednoznačné identifikační číslo uchovaného dokumentu s elektronickými podpisy. Bylo automaticky vygenerováno při procesu uchování ve službě SecuSign. Pod tímto číslem je možné v metodě *Preserve_getInfo* zjistit informace o uchovaném dokumentu Max. 128 znaků.

6.1.4.4.2.3 <fileName>

Návratová hodnota	Popis
string	Název uchovaného souboru s elektronickými podpisy. Max. 260 znaků.

6.1.4.4.2.4 <fileSize>

Návratová hodnota	Popis
long	Velikost uchovaného souboru s elektronickými podpisy

6.1.4.4.2.5 <sortInfo>

Návratová hodnota	Popis
string	Zatřiďovací informace – např. název složky, nebo struktura vnořených složek, ve kterých je dokument u uživatele evidován. Max. 100 znaků.

6.1.4.4.2.6 <lastUpdate>

Návratová hodnota	Popis
dateTime	Datum a čas posledního prodloužení platnosti a ověřitelnosti dokumentu s elektronickými podpisy

6.1.4.4.2.7 <expiration>

Návratová hodnota	Popis
dateTime	Datum a čas vypršení ověřitelnosti platnosti celého dokumentu. Po tomto datu nebude možné ověřit platnost certifikátů podpisů / pečetí / razítek a zajistit další ověřitelnost a platnost uchovaného dokumentu.

6.1.4.4.2.8 <docDataHash>

Návratová hodnota	Popis
Base64Binary	Hash analyzovaného dokumentu kódovaný v Base64. Algoritmus výpočtu hashe je v následujícím elementu docDataHashAlg.

6.1.4.4.2.9 <docDataHashAlg>

Návratová hodnota	Popis
string	Algoritmus výpočtu hashe analyzovaného dokumentu. Ve tvaru například: 2.16.840.1.101.3.4.2.1

6.1.4.4.2.10 <currSignHashAlg>

Návratová hodnota	Popis
string	Algoritmus výpočtu hashe posledního podpisu. Příklad: 2.16.840.1.101.3.4.2.1

6.1.4.4.2.11 <sigValidityCondition>

Návratová hodnota	Popis
string	Zvolené podmínky platnosti podpisu při uchování. Hodnoty: ALL – všechny podpisy jsou platné AT_LEAST_ONE – alespoň jeden podpis je platný LAST – poslední podpis je platný

6.1.4.4.2.12 <sigsPreservationStatus>

6.1.4.4.2.12.1 <PreservationInfo> opakující se element podle počtu podpisů v dokumentu

6.1.4.4.2.12.2 <sid>

Návratová hodnota	Popis
string	Identifikátor podpis, který k danému uchovanému dokumentu eviduje služba SecuSign

6.1.4.4.2.12.3 <sigStatus>

6.1.4.4.2.12.4 <indication>

Návratová hodnota	Popis
string	Stav ověření podpisu – indikace. Může nabývat hodnot: VALID – platný (TOTAL_PASSED dle normy ETSI[2]) INVALID – neplatný (TOTAL_FAILED dle normy ETSI[2]) INDETERMINATE – neurčitý UNKNOWN - neznámý

6.1.4.4.2.12.5 <subindication>

Návratová hodnota	Popis
string	Podstav ověření podpisu - subindikace. Nabývá hodnot (odpovídajících normě ETSI[2]): VALID – Elektronický certifikát nebyl v okamžiku podepsání revokovaný nebo expirovaný a podpis je možné prohlásit za platný. INVALID_REVOKED - Podpisový certifikát byl odvolán ještě před okamžikem pořízení podpisu. Podpis je neplatný. INVALID_HASH_FAILURE - Elektronický podpis je porušený a od podepsání dokumentu zřejmě došlo ke změně podepsané části jeho obsahu. Kontrolní součet uvedený v podpisu nesouhlasí s kontrolním součtem podepsané části! Podpis je neplatný. INVALID_SIG_CRYPTO_FAILURE - Nepodařilo se ověřit příslušnost veřejného klíče k podpisu. Podpis je neplatný. INVALID_FORMAT_FAILURE - Podepsaná data nebyla rozpoznána, formát podpisu je porušený. Podpis je neplatný. INDETERMINATE_NO_CERTIFICATE_CHAIN_FOUND - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Nepodařilo se získat všechny potřebné informace pro kontrolu důvěryhodnosti a odvolání certifikátu. INDETERMINATE_NO_POE - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Nepodařilo se získat všechny potřebné informace pro kontrolu důvěryhodnosti a odvolání certifikátu. INDETERMINATE_TRY_LATER - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Kontrolu odvolání certifikátu je možné provést na základě seznamu odvolaných certifikátů (CRL) vydaném po INDETERMINATE_SIGNED_DATA_NOT_FOUND - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout, protože nejsou k dispozici data, jejichž podpis je ověřován. INDETERMINATE_UNKNOWN_SIGNING_TIME - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Nepodařilo se získat všechny potřebné informace pro kontrolu důvěryhodnosti a odvolání certifikátu. INDETERMINATE_UNTRUST_SIGNING_TIME - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Není k dispozici důvěryhodný údaj z časového razítka o času podepsání. INDETERMINATE_GENERAL_ERROR - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Obecná chyba aplikace, kontaktujte správce.

	INDETERMINATE_REVOKED_NO_POE - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Podpisový certifikát byl odvolán v době ověření, ale je nejistý čas podepsání. INDETERMINATE_REVOKED_CA_NO_POE - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Nejméně jeden řetěz certifikátu byl nalezen, ale certifikát zprostředkující CA je revokován. INDETERMINATE_OUT_OF_BOUNDS_NO_POE - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Podpisový certifikát vypršel nebo ještě nenastala jeho platnost v době ověření a algoritmus ověřování podpisu nemůže zjistit, že čas podepsání leží uvnitř intervalu platnosti podpisového certifikátu. INDETERMINATE_EXPIRED - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Podpisový certifikát vypršel. Podpis byl vytvořen po datu expirace (notAfter) podpisového certifikátu. INDETERMINATE_NOT_YET_VALID - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Podpisový certifikát nebyl ještě platný v době ověřování. Čas podepsání leží před datumem vydání (notBefore) podpisového certifikátu. INDETERMINATE_POLICY_PROCESSING_ERROR - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Soubor dané formální politiky z nějakého důvodu nemohl být zpracován (např. není přístupný, není zpracovatelný, nesouhlasí kontrolní algoritmus, atd.) INDETERMINATE_TIMESTAMP_ORDER_FAILURE - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Některá omezení v pořadí podpisu časových razítek a/nebo podepsaných datových objektů časových razítek nejsou respektována. INDETERMINATE_SIG_CONSTRAINTS_FAILURE - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Nejsou splněna omezení podpisu (chybějící podpisové atributy, nesouhlasná politika el. podpisu, apod.). INDETERMINATE_CHAIN_CONSTRAINTS_FAILURE - O platnosti podpisu není možné v tuto chvíli prokazatelně rozhodnout. Obecná chyba při sestavování certifikační cesty. INDETERMINATE_CRYPTO_CONSTRAINTS_FAILURE - Alespoň jeden z algoritmů, které byly použity v materiálu (např. hodnota podpisu, certifikát, ...) zapojeném v ověřování podpisu, nebo velikost klíče použita s tímto algoritmem, je pod požadovanou úroveň kryptografického zabezpečení, a tento materiál byl produkován po čase, kdy byl tento algoritmus/klíč považován za bezpečný (je-li znám takový čas), a materiál není chráněn dostatečně silným časovým razítkem aplikovaným před dobou ve které byl algoritmus považován za bezpečný (je-li znám takový čas).

6.1.4.4.2.12.6 </sigStatus>

6.1.4.4.2.12.7 <extendedValidationEndDate>

Návratová hodnota	Popis
dateTime	Datum a čas do kdy byla prodloužena ověřitelnost podpisu

6.1.4.4.2.12.8 <signingCertSubject>

Návratová hodnota	Popis
string	Identifikace podpisového certifikátu, který byl ošetřen

6.1.4.4.2.12.9 <bISDocTimeStamp>

Návratová hodnota	Popis
boolean	Určuje, zda podpis je samostatným časovým razítkem

6.1.4.4.2.12.10 <procesStatus>

Návratová hodnota	Popis
string	Stav ošetření podpisu během uchování. Hodnoty: None – Neproběhlo ošetření podpisu Full – Plně proběhlo ošetření podpisu Partial - Podpis byl ošetřen částečně (neobsahuje všechna validační data) Unknown – Neznámý stav

6.1.4.4.2.12.11 </PreservationInfo>

6.1.4.4.2.13 </sigsPreservationStatus>

6.1.4.4.2.14 <preservationHistory>

6.1.4.4.2.14.1 <PreservationRecord>

6.1.4.4.2.14.2 <id>

Návratová hodnota	Popis
int	Identifikátor provedené operace

6.1.4.4.2.14.3 <operationTime>

Návratová hodnota	Popis
dateTime	Datum a čas provedení operace

6.1.4.4.2.14.4 <operationType>

Návratová hodnota	Popis
PreserveOperation	Typ provedené operace. Hodnoty: REGISTER – uchování dokumentu s elektronickými podpisy UPDATE – prodloužení platnosti a ověřitelnosti elektronických podpisů v dokumentu UNREGISTER – odebrání dokumentu z uchovávání ve službě SecuSign UNKNOWN – neznámý typ operace

6.1.4.4.2.14.5 <operationStatus>

Návratová hodnota	Popis
int	Stav provedení operace. 0 = v pořádku.

6.1.4.4.2.14.6 <operationStatusInfo>

Návratová hodnota	Popis
string	Textová zpráva odpovídající stavu provedení operace

6.1.4.4.2.14.7 <fileName>

Návratová hodnota	Popis
string	Název souboru, ze kterého byl podpis uchován. Max. 260 znaků.

6.1.4.4.2.14.8 <fileSize>

Návratová hodnota	Popis
long	Velikost souboru, ze kterého byl podpis uchován

6.1.4.4.2.14.9 <hashIn>

Návratová hodnota	Popis
string	Hash souboru, který měl dokument na vstupu

6.1.4.4.2.14.10 <hashOut>

Návratová hodnota	Popis
string	Hash souboru, který měl dokument na výstupu

6.1.4.4.2.14.11 <userComment>

Návratová hodnota	Popis
string	Vlastní komentář nebo popis dokumentu uživatelem

6.1.4.4.2.14.12 </PreservationRecord>

6.1.4.4.2.15 </preservationHistory>

6.1.4.4.2.16 <docType>

Návratová hodnota	Popis
UNKNOWN	Neznámý typ dokumentu
CMSPKCS7	Dokument podepsaný interním CMS/PKCS7 podpisem
CMSPKCS7Ext	Dokument podepsaný externím CMS/PKCS7 podpisem
PDF	Podepsaný PDF dokument
XML	Podepsaná XML data

XML602FORM	Podepsané datové zprávy z Informačního systému datových schránek a FO/ZFO formuláře aplikace Software602 Form Filler
XMLISDOC	Podepsaná XML ISDOC data
ASiC_S_CAdES	ASiC-Simple s CAdES podpisem
ASiC_S_XAdES	ASiC-Simple s XAdES podpisem
ASiC_S_Tst	ASiC-Simple s Timestamp
ASiC_E_CAdES_Tst	ASiC-Extended s CAdES podpisem nebo s Timestamp
ASiC_E_XAdES	ASiC-Extended s XAdES podpisem
MS_WORD	Podepsaný dokument aplikace MS Word
MS_EXCEL	Podepsaný dokument aplikace MS Excel
MS_PWR_PNT	Podepsaný dokument aplikace MS Powerpoint
ODF	Podepsaný OpenDocumentFormat (OpenOffice)

6.1.4.4.3 </Report>

6.1.4.4.4 <XMLReport>

Návratová hodnota	Popis
Base64Binary	Data XML doložky se zjištěnými informacemi o uchovaném dokumentu kódována v Base64

6.1.4.4.5 <HTMLReport>

Návratová hodnota	Popis
Base64Binary	Data HTML doložky se zjištěnými informacemi o uchovaném dokumentu kódována v Base64

6.1.4.4.6 <PDFReport>

Návratová hodnota	Popis
Base64Binary	Data PDF doložky se zjištěnými informacemi o uchovaném dokumentu kódována v Base64

6.1.4.4.7 <StatusMessage>

Návratová hodnota	Popis
String	Textová zpráva odpovídající celkovému výsledku zjištěných informací o uchovaném dokumentu s elektronickým podpisem ve službě SecuSign. Hodnota je naplněna pouze v případě problematického výsledku.

6.1.5 Metoda Preserve_getForUpdate

Umožňuje zjistit informace o uchovaných dokumentech, které je třeba před vypršením platnosti elektronického podpisu, elektronické pečeti a/nebo časového razítka prodloužit.

Popis služby včetně WSDL schématu a příklad požadavku a odpovědi pro SOAP 1.1 a SOAP 1.2 je umístěn na https://localhost/secusign/default.asmx?op=Preserve_getForUpdate *

* localhost je název používaný pro lokální počítač; namísto něj zvolte jméno/IP adresu SDK serveru (dle nastavení v IIS)

6.1.5.1 Požadavek v rozhraní SOAP 1.1

```
POST /secusign/default.asmx HTTP/1.1
Host: localhost
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://software602.com/secusign/Preserve_getForUpdate"
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <Preserve_getForUpdate xmlns="http://software602.com/secusign/">
      <ExpirationLimit>dateTime</ExpirationLimit>
      <SortInfoMask>string</SortInfoMask>
      <FileType>UNKNOWN or CMSPKCS7 or CMSPKCS7Ext or PDF or XML or XML602FORM or
XMLISDOC or ASiC_S_CAdES or ASiC_S_XAdES or ASiC_S_Tst or ASiC_E_CAdES_Tst or
ASiC_E_XAdES or MS_WORD or MS_EXCEL or MS_PWR_PNT or ODF</FileType>
      <MaxResCount>int</MaxResCount>
      <Offset>integer</Offset>
      <Params>string</Params>
    </Preserve_getForUpdate>
  </soap:Body>
</soap:Envelope>
```

6.1.5.2 Vstupní parametry metody

6.1.5.2.1 <ExpirationLimit>

[povinný element]

Vstup	Popis
dateTime	Datum a čas, ke kterému se vyhledají uchované elektronické podpisy v dokumentech, které je nutné prodloužit

6.1.5.2.2 <SortInfoMask>

[nepovinný element]

Vstup	Popis
string	Definuje název zatřiďovací složky, nebo strukturu vnořených složek (Např. /FA/2017/02) ze které vrátí informace o uchovaných elektronických podpisech v dokumentech. Max. 100 znaků.

6.1.5.2.3 <FileType>

[povinný element]

Vstup	Popis
UNKNOWN	Neznámý typ dokumentu

CMSPKCS7	Dokument podepsaný interním CMS/PKCS7 podpisem
CMSPKCS7Ext	Dokument podepsaný externím CMS/PKCS7 podpisem
PDF	Podepsaný PDF dokument
XML	Podepsaná XML data
XML602FORM	Podepsané datové zprávy z Informačního systému datových schránek a FO/ZFO formuláře aplikace Software602 Form Filler
XMLISDOC	Podepsaná XML ISDOC data
ASiC_S_CAdES	ASiC-Simple s CAdES podpisem
ASiC_S_XAdES	ASiC-Simple s XAdES podpisem
ASiC_S_Tst	ASiC-Simple s Timestamp
ASiC_E_CAdES_Tst	ASiC-Extended s CAdES podpisem nebo s Timestamp
ASiC_E_XAdES	ASiC-Extended s XAdES podpisem
MS_WORD	Dokument aplikace MS Word
MS_EXCEL	Dokument aplikace MS Excel
MS_PWR_PNT	Dokument aplikace MS Powerpoint
ODF	Podepsaný OpenDocumentFormat (OpenOffice)

6.1.5.2.4 <MaxResCount>

[povinný element]

Vstup	Popis
Int	Maximální počet výsledků, které se mají vrátit.

6.1.5.2.5 <Offset>

[povinný element]

Vstup	Popis
Int	Stránkování vrácených DocIDs. Číslem se nastaví počet IDs, od kterých se má pokračovat ve vrácení dalších výsledků.

6.1.5.2.6 <Params>

[nepovinný element]

Vstup	Popis
String	Volitelné, obsahuje další parametry. Zatím se nevyužívá.

6.1.5.3 Struktura odpovědi na požadavek

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
```

```
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <Preserve_getForUpdateResponse xmlns="http://software602.com/secusign/">
      <Preserve_getForUpdateResult>int</Preserve_getForUpdateResult>
      <DocIDs>
        <string>string</string>
        <string>string</string>
      </DocIDs>
      <StatusMessage>string</StatusMessage>
    </Preserve_getForUpdateResponse>
  </soap:Body>
</soap:Envelope>
```

6.1.5.4 Výstupní parametry metody

6.1.5.4.1 <Preserve_getForUpdateResult>

Návratová hodnota	Popis
int	Výsledek metody Preserve_getForUpdateResult. 0 = v pořádku, jinak Návratové kódy všech metod a chyba popsaná ve StatusMessage.

6.1.5.4.2 <DocIDs>

6.1.5.4.2.1 <String> - opakující se element v případě vice dokumentů

Návratová hodnota	Popis
String	Seznam identifikátorů dokumentů s uchovanými podpisy, které k poskytnutému ExpirationLimit služba eviduje. Každý string má max. 128 znaků.

6.1.5.4.3 </DocIDs>

6.1.5.4.4 <StatusMessage>

Návratová hodnota	Popis
String	Textová zpráva odpovídající celkovému výsledku zjištění informací o uchovaných dokumentech s elektronickými podpisy, které je nutné ve službě SecuSign prodloužit. Hodnota je naplněna pouze v případě problematického výsledku.

6.2 Praktické zkušenosti

6.2.1 Preserve_register

Uchování kvalifikovaných elektronických podpisů/pečetí s kvalifikovaným časovým razítkem v dokumentu (v metodě Preserve_register) doporučujeme provádět s určitým časovým odstupem – minimálně 5 minut, ideálně 24 hodin - od podepsání/pečetění dokumentu (v metodě Seal) a to z důvodu potřebného připojení odpovídajících revokačních informací o podpisech/pečetích/razítkách z OCSP/CRL. V případě CRL může být vyžadováno oněch 24 hodin.

7 Služba pečetění a podepisování

Metoda webové služby **Seal** umožňuje:

1. Elektronicky opečetit vstupní soubor (data) certifikátem pro (kvalifikovanou) elektronickou pečeť, který je:
   - nahrán přes uživatelské rozhraní 602 ID účtu do bezpečného úložiště služby SecuSign – Azure KeyVault,
   - vygenerován v kvalifikovaném prostředku (HSM) pro službu Vzdáleného pečetění,
   - vygenerován na lokálním kvalifikovaném prostředku (HSM) zákazníka,
   - nainstalován v systémovém úložišti certifikátů, nebo umístěný v PFX souboru, na SDK serveru.
2. Elektronicky podepsat vstupní soubor (data) certifikátem pro (kvalifikovaný) elektronický podpis, který je:
   - vygenerován v kvalifikovaném prostředku (HSM) pro službu Vzdáleného podepisování

Metoda webové služby **SealEx** navíc umožňuje:

3. Elektronicky podepsat/opečetit vstupní soubor (data) s vizualizací a/nebo důvodem/místem podepsání/opečetění.

Výstupem obou metod je elektronicky opečetěný, nebo elektronicky podepsaný, dokument, případně externí podpis/pečeť k datům, s kvalifikovaným časovým razítkem.

Kvalifikované časové razítko je odebíráno pomocí autentizačního certifikátu, nebo basic autentizací (jméno/heslo), z URI poskytovatele časových razítek, které je definováno v konfiguraci SecuSign SDK. Výchozí konfigurace SDK získává kvalifikované časové razítko od QTSP PostSignum.

7.1 Název metody: Seal

Popis služby včetně WSDL schématu a příklad požadavku a odpovědi pro SOAP 1.1 a SOAP 1.2 je umístěn na https://localhost/secusign/default.asmx?op=Seal *

* localhost je název používaný pro lokální počítač; namísto něj zvolte jméno/IP adresu SDK serveru (dle nastavení v IIS)

7.1.1 Požadavek v rozhraní SOAP 1.1

```
POST /secusign/default.asmx HTTP/1.1
Host: localhost
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://software602.com/secusign/Seal"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <Seal xmlns="http://software602.com/secusign/">
      <FileName>string</FileName>
      <Input>base64Binary</Input>
      <FileType>UNKNOWN or CMSPKCS7 or CMSPKCS7Ext or PDF or XML or XML602FORM or
XMLISDOC or ASiC_S_CAdES or ASiC_S_XAdES or ASiC_S_Tst or ASiC_E_CAdES_Tst or
ASiC_E_XAdES or MS_WORD or MS_EXCEL or MS_PWR_PNT or ODF</FileType>
      <CertificateID>string</CertificateID>
```

```
      <PrivateKeyPIN>string</PrivateKeyPIN>
      <SignatureType>DEFAULT or ENVELOPED or DETACHED or ENCAPSULATE or
DETACHED_FROM_HASH</SignatureType>
      <Params>string</Params>
    </Seal>
  </soap:Body>
</soap:Envelope>
```

7.1.2 Vstupní parametry metody

7.1.2.1 <FileName>

[povinný element]

Vstup	Popis
string	Název vstupního souboru (včetně přípony), který bude opatřen kvalifikovanou elektronickou pečetí. Příklad: Dokument.pdf Max. 260 znaků.

7.1.2.2 <Input>

[povinný element]

Vstup	Popis
Base64Binary	Data vstupního souboru kódovaná v base64

7.1.2.3 <FileType>

[povinný element]

Typ podepisovaného dokumentu nebo dat	
Vstup	**Popis**
UNKNOWN	Neznámý typ dokumentu
CMSPKCS7	Dokument podepsaný interním CMS/PKCS7 podpisem
CMSPKCS7Ext	Dokument podepsaný externím CMS/PKCS7 podpisem
PDF	PDF dokument
XML	XML data
XML602FORM	Datové zprávy z Informačního systému datových schránek a FO/ZFO formuláře aplikace Software602 Form Filler
XMLISDOC	XML ISDOC data
ASiC_S_CAdES	ASiC-Simple s CAdES podpisem
ASiC_S_XAdES	ASiC-Simple s XAdES podpisem
ASiC_S_Tst	ASiC-Simple s Timestamp
ASiC_E_CAdES_Tst	ASiC-Extended s CAdES podpisem nebo s Timestamp
ASiC_E_XAdES	ASiC-Extended s XAdES podpisem
MS_WORD	Dokument aplikace MS Word
MS_EXCEL	Dokument aplikace MS Excel

MS_PWR_PNT	Dokument aplikace MS Powerpoint
ODF	OpenDocumentFormat (OpenOffice)

7.1.2.4 <CertificateID>

[nepovinný element]

Vstup	Popis
String	Identifikace certifikátu pro vytvoření zaručené/kvalifikované elektronické pečeti nebo zaručeného/kvalifikovaného elektronického podpisu. V případě in-house rozhraní SecuSign SDK je možné použít formáty: ■ HStore:[alias] ▪ alias certifikátu pro podepsání/pečetění z HSM modulu služby Vzdáleného podepisování/pečetění. ▪ pokud je v konfiguraci webové služby nastaven konfigurační klíč Seal_DefaultToQStore, prefix HStore se neuvádí ■ PKCS11:[alias] ▪ alias certifikátu pro podepsání/pečetění z HSM modulu klienta nebo ze systémového úložiště Windows. ■ QStore:[alias] ▪ Pečetí se certifikátem nahraným na účtu klienta v Azure KeyVault. ■ urn:hex:[hexadecimalne_kodovany_sha1_hash_certu] ▪ podepsání/pečetění certifikátem ze systémového úložiště Windows pod Current User. Nutné spouštět aplikační pool pod konkrétním uživatelem. ■ urn:sha:[Base64_kodovany_sha1_hash_certu] ▪ podepsání/pečetění certifikátem ze systémového úložiště Windows pod Current User. Nutné spouštět aplikační pool pod konkrétním uživatelem. ■ [cesta k PFX] ▪ podepsání konkrétním PFX, který je lokálně přístupný pro webovou službu/aplikaci v souboru. ■ prázdný řetězec ▪ použije se nastavení SigningCertPath v konfiguraci webové služby SecuSign SDK. ▪ pokud je v konfiguraci webové služby nastaven konfigurační klíč Seal_DefaultToQStore, pak se použije výchozí certifikát ze služby Vzdáleného pečetění V případě webových služeb SecuSign v Azure je možné použít např. hodnotu z CN nebo SERIALNUMBER – obě informace je možné zjistit v administraci služby SecuSign > Seal po přihlášení do uživatelského rozhraní 602 ID účtu. Výchozí hodnota: prázdný řetězec

7.1.2.5 <PrivateKeyPIN>

[nepovinný element]

Vstup	Popis
string	PIN, který byl zvolen žadatelem jako přístupové heslo k privátní části certifikátu Hodnota je povinná v případě `QStore, PKCS11` a souboru PFX. V případě použití `HStore` aliasu záleží, zda se používá pro podepisování nebo pečetění. Pro podepisování s nastaveným potvrzením pomocí PIN je nutné `PrivateKeyPIN` uvést. Pro podepisování s nastaveným potvrzením pomocí 602KEY se `PrivateKeyPIN` neuvádí. Pro pečetění není nutné `PrivateKeyPIN` uvádět, protože přístup k certifikátu je definován na základě autentizačního (licenčního) certifikátu volající aplikace, pokud není zvoleno jinak.

7.1.2.6 <SignatureType>

[povinný element]

Vstup	Popis
enum	Typ elektronického podpisu. Hodnoty: ■ DEFAULT ■ ENVELOPED ■ DETACHED ■ ENCAPSULATE ■ DETACHED_FROM_HASH Pro CAdES mají hodnoty DEFAULT a ENCAPSULATE stejný význam - podepisovaná data jsou vložena k podpisu. Hodnota DETACHED znamená, že podpis je oddělen do jiného souboru. Hodnota DETACHED_FROM_HASH je stejná jako DETACHED jen s tím rozdílem, že při vytváření je na vstupu pouze hash podepisovaných dat. Pro XAdES mají jednotlivé hodnoty význam: DEFAULT - podepisovaná data jsou vložena do struktury podpisu ENVELOPED - podpis je uvnitř podepisovaných dat DETACHED - podpis je oddělen od dat do samostatného souboru Výchozí hodnota: DEFAULT

7.1.2.7 <Params>

[nepovinný element]

Vstup	Popis
String	Volitelné, obsahuje další parametry pro splnění projektových požadavků, např.: ■ add_timestamp=false – nepřipojení časového razítko k podpisu/pečeti ■ id_user=string – identifikace uživatele podpisového certifikátu

7.1.3 Struktura odpovědi na požadavek

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <SealResponse xmlns="http://software602.com/secusign/">
      <SealResult>int</SealResult>
      <Output>base64Binary</Output>
      <StatusMessage>string</StatusMessage>
    </SealResponse>
  </soap:Body>
</soap:Envelope>
```

7.1.4 Výstupní parametry metody

7.1.4.1 <SealResult>

Návratová hodnota	Popis
Int	Výsledek metody Seal (pečetění/podepsání dokumentu). 0 = v pořádku, jinak Návratové kódy všech metod a chyba popsaná ve StatusMessage.

7.1.4.2 <Output>

Návratová hodnota	Popis
base64Binary	Výstupní data podepsaného/opečetěného dokumentu, nebo externího podpisu/pečeti (v případě FileType=CMSPKCS7Ext), kódovaná v Base64

7.1.4.3 <StatusMessage>

Návratová hodnota	Popis
string	Textová zpráva odpovídající celkovému výsledku podepsání/pečetění dokumentu. Hodnota je naplněna pouze v případě problematického výsledku.

7.2 Název metody: SealEx

Metoda SealEx je k dispozici pro vizualizaci vkládaného elektronického podpisu/pečeti do PDF dokumentu - to znamená např., že elektronický podpis/pečeť bude v souboru viditelný prostřednictvím podpisového pole (s obrázkem) a uživatel skrze kliknutí na obrázek bude moci v prohlížeči PDF souborů jednoduše zjistit informace o vloženém elektronickém podpisu/pečeti. Dále také umožňuje nastavení důvodu a místa podepsání/opečetění.

Popis služby včetně WSDL schématu a příklad požadavku a odpovědi pro SOAP 1.1 a SOAP 1.2 je umístěn na https://localhost/secusign/default.asmx?op=SealEx *

* localhost je název používaný pro lokální počítač; namísto něj zvolte jméno/IP adresu SDK serveru (dle nastavení v IIS)

7.2.1 Požadavek v rozhraní SOAP 1.1

```
POST /secusign/default.asmx HTTP/1.1
Host: localhost
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://software602.com/secusign/Seal"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <SealEx xmlns="http://software602.com/secusign/">
      <FileName>string</FileName>
      <Input>base64Binary</Input>
      <FileType>UNKNOWN or CMSPKCS7 or CMSPKCS7Ext or PDF or XML or XML602FORM or
XMLISDOC or ASiC_S_CAdES or ASiC_S_XAdES or ASiC_S_Tst or ASiC_E_CAdES_Tst or
ASiC_E_XAdES or MS_WORD or MS_EXCEL or MS_PWR_PNT or ODF or EML or MSG or
CERTIFICATE</FileType>
      <CertificateID>string</CertificateID>
      <PrivateKeyPIN>string</PrivateKeyPIN>
      <SignatureType>DEFAULT or ENVELOPED or DETACHED or ENCAPSULATE or
DETACHED_FROM_HASH</SignatureType>
      <Params>string</Params>
      <ParamsEx>
        <Param>
          <Name>string</Name>
          <Value>string</Value>
        </Param>
        <Param>
          <Name>string</Name>
          <Value>string</Value>
        </Param>
      </ParamsEx>
    </SealEx>
  </soap:Body>
</soap:Envelope>
```

7.2.2 Vstupní parametry metody

V základu jsou shodné s metodou Seal, navíc je možné na vstupu metody SealEx definovat:

7.2.2.1 <ParamsEx>

[povinný element]

7.2.2.1.1 <Param>

[povinný element]

- *Pole Param obsahující vždy dvojici parametrů s jejich názvem a hodnotou*
- *Dvojice Param jsou volitelné a jsou uvedeny pod sebou tak, jak k sobě náleží*

7.2.2.1.1.1 <Name>

[volitelný element]

Vstup	Popis
string	Název vstupního parametru. Může nabývat hodnot: Flags – Vlastnosti vizualizace podpisu/pečeti PosX – Pozice pole podpisu/pečeti na X souřadnici

	PosY – Pozice pole podpisu/pečeti na Y souřadnici SizeX – Velikost pole podpisu/pečeti na X souřadnici SizeY – Velikost pole podpisu/pečeti na Y souřadnici Page – Stránka, na kterou se má podpis vložit Text – Text pro vložený podpis/pečeti TextHeader – Tučný nadpis vložený nad Text Image – Data obrázku pro vizualizaci podpisu/pečeti Reason – Důvod podepsání/pečetění dokumentu Location – Informace o místě podepsání/pečetí dokumentu Contact – Kontaktní informace podepisující/pečetící osoby

7.2.2.1.1.2 <Value>

[volitelný element]

Vstup	Popis
string	Hodnota vstupního parametru náležící k danému názvu parametru. Value pro Flags je kombinací (součtem) následujících příznaků: ■ 0 (0x0000) – nevizuální podpis (default) ■ 1 (0x0001) – podpisové pole s obrázkem (PDF_SIGN_SHOW_IMAGE) ■ 2 (0x0002) – podpisové pole s textem (PDF_SIGN_SHOW_TEXT) Value pro Page může být libovolné číslo stránky dokumentu: ■ 1 – první stránka (výchozí) ■ záporné číslo znamená číslo stránky od konce dokumentu Value pro Image musí obsahovat base64 kódovaná data obrázku: ■ Base64:<Base64BinaryData> Pokud se má Value pro Text odřádkovat, je možné použít znaky \n Pokud se má Value pro Text escapovat, je možné použít znak \

7.2.3 Struktura odpovědi na požadavek

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <SealExResponse xmlns="http://software602.com/secusign/">
      <SealExResult>int</SealExResult>
      <Output>base64Binary</Output>
      <StatusMessage>string</StatusMessage>
    </SealExResponse>
  </soap:Body>
</soap:Envelope>
```

7.2.4 Výstupní parametry metody

7.2.4.1 <SealExResult>

Návratová hodnota	Popis
Int	Výsledek metody SealEx (pečetění/podepsání dokumentu). 0 = v pořádku, jinak Návratové kódy všech metod a chyba popsaná ve StatusMessage.

7.2.4.2 <Output>

Návratová hodnota	Popis
base64Binary	Výstupní data podepsaného/opečetěného dokumentu, nebo externího podpisu/pečeti (v případě FileType=CMSPKCS7Ext), kódovaná v Base64

7.2.4.3 <StatusMessage>

Návratová hodnota	Popis
string	Textová zpráva odpovídající celkovému výsledku podepsání/pečetění dokumentu. Hodnota je naplněna pouze v případě problematického výsledku.

7.2.5 Příklad volání SealEx

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:sec="http://software602.com/secusign/">
   <soapenv:Header/>
   <soapenv:Body>
      <sec:SealEx>
         <sec:FileName>Mini.pdf</sec:FileName>
         <sec:Input>Base64BinaryData</sec:Input>
         <sec:FileType>PDF</sec:FileType>
         <sec:CertificateID>HStore:01ab23cd-45ef-78ab-cd01-2345ef678fed</sec:CertificateID>
         <!--Optional:-->
         <sec:PrivateKeyPIN/>
         <sec:SignatureType>DEFAULT</sec:SignatureType>
         <!--Optional:-->
         <sec:Params/>
         <!--Optional:-->
         <sec:ParamsEx>
            <!--Zero or more repetitions:-->
            <sec:Param>
              <sec:Name>Flags</sec:Name>
               <sec:Value>3</sec:Value>
            </sec:Param>
            <sec:Param>
              <sec:Name>PosX</sec:Name>
               <sec:Value>50</sec:Value>
            </sec:Param>
            <sec:Param>
              <sec:Name>PosY</sec:Name>
               <sec:Value>-50</sec:Value>
            </sec:Param>
            <sec:Param>
              <sec:Name>SizeX</sec:Name>
               <sec:Value>150</sec:Value>
            </sec:Param>
            <sec:Param>
              <sec:Name>SizeY</sec:Name>
               <sec:Value>50</sec:Value>
```

```
            </sec:Param>
            <sec:Param>
              <sec:Name>Text</sec:Name>
               <sec:Value>Tohle je text podpisu</sec:Value>
            </sec:Param>
            <sec:Param>
              <sec:Name>Image</sec:Name>
               <sec:Value>Base64:Base64BinaryData</sec:Value>
            </sec:Param>
            <sec:Param>
              <sec:Name>Reason</sec:Name>
               <sec:Value>Jsem autorem tohoto dokumentu.</sec:Value>
            </sec:Param>
            <sec:Param>
              <sec:Name>Location</sec:Name>
               <sec:Value>Hornokrčská 15, Praha 4, 140 00, CZ</sec:Value>
            </sec:Param>
            <sec:Param>
              <sec:Name>Contact</sec:Name>
               <sec:Value>Kontaktujte nás na info@602.cz</sec:Value>
            </sec:Param>
          </sec:ParamsEx>
      </sec:SealEx>
   </soapenv:Body>
</soapenv:Envelope>
```

8 Služba razítkování

Služba umožňuje opatřit vstupní dokument (data) kvalifikovaným časovým razítkem. Časovým razítkem lze opatřit pouze ty dokumenty (data), které obsahují elektronický podpis/pečeť. U souborů typu PDF je možné kvalifikovaným časovým razítkem opatřit i nepodepsané dokumenty.

Kvalifikované časové razítko je odebíráno pomocí autentizačního certifikátu, nebo basic autentizací (jméno/heslo), z URI poskytovatele časových razítek, které je definováno v konfiguraci SecuSign SDK. Výchozí konfigurace SecuSign SDK získává kvalifikované časové razítko QTSP PostSignum z uživatelského 602 ID účtu, u kterého je nastaven licenční certifikát SecuSign SDK.

8.1 Název metody: Timestamp

Popis služby včetně WSDL schématu a příklad požadavku a odpovědi pro SOAP 1.1 a SOAP 1.2 je umístěn na https://localhost/secusign/default.asmx?op=Timestamp *

* localhost je název používaný pro lokální počítač; namísto něj zvolte jméno/IP adresu SDK serveru (dle nastavení v IIS)

8.1.1 Požadavek v rozhraní SOAP 1.1

```
POST /secusign/default.asmx HTTP/1.1
Host: localhost
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://software602.com/secusign/Timestamp"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <Timestamp xmlns="http://software602.com/secusign/">
      <FileName>string</FileName>
      <Input>base64Binary</Input>
      <ExternalSignature>base64Binary</ExternalSignature>
      <FileType>UNKNOWN or CMSPKCS7 or CMSPKCS7Ext or PDF or XML or XML602FORM or
XMLISDOC or ASiC_S_CAdES or ASiC_S_XAdES or ASiC_S_Tst or ASiC_E_CAdES_Tst or
ASiC_E_XAdES or MS_WORD or MS_EXCEL or MS_PWR_PNT or ODF</FileType>
      <ForRegistration>boolean</ForRegistration>
      <Params>string</Params>
    </Timestamp>
  </soap:Body>
</soap:Envelope>
```

8.1.2 Vstupní parametry metody

8.1.2.1 <FileName>

[povinný element]

Vstup	Popis
string	Název vstupního souboru (včetně přípony), který bude opatřen kvalifikovaným časovým razítkem. Příklad: Dokument.pdf Max. 260 znaků.

8.1.2.2 <Input>

[povinný element]

Vstup	Popis
Base64Binary	Data vstupního souboru kódovaná v base64

8.1.2.3 <ExternalSignature>

[nepovinný element]

Vstup	Popis
Base64Binary	Data externího podpisu kódovaná v base64, pokud je chtěno připojit razítko k externímu podpisu

8.1.2.4 <FileType>

[povinný element]

Typ podepisovaného dokumentu nebo dat	
Vstup	**Popis**
UNKNOWN	Neznámý typ dokumentu
CMSPKCS7	Dokument podepsaný interním CMS/PKCS7 podpisem
CMSPKCS7Ext	Dokument podepsaný externím CMS/PKCS7 podpisem
PDF	PDF dokument
XML	Podepsaná XML data
XML602FORM	Podepsané datové zprávy z Informačního systému datových schránek a FO/ZFO formuláře aplikace Software602 Form Filler
XMLISDOC	Podepsaná XML ISDOC data
ASiC_S_CAdES	ASiC-Simple s CAdES podpisem
ASiC_S_XAdES	ASiC-Simple s XAdES podpisem
ASiC_S_Tst	ASiC-Simple s Timestamp
ASiC_E_CAdES_Tst	ASiC-Extended s CAdES podpisem nebo s Timestamp
ASiC_E_XAdES	ASiC-Extended s XAdES podpisem
MS_WORD	Podepsaný dokument aplikace MS Word
MS_EXCEL	Podepsaný dokument aplikace MS Excel
MS_PWR_PNT	Podepsaný dokument aplikace MS Powerpoint
ODF	Podepsaný OpenDocumentFormat (OpenOffice)

8.1.2.5 <ForRegistration>

[povinný element]

Vstup	Popis
String	Parametr pro získání odpovídajícího razítka. Možné hodnoty: False – standardní kvalifikované časové razítko

	True – přípravné kvalifikované časové razítko (pro následnou registraci k uchování dokumentu) Výchozí hodnota: `false`

8.1.2.6 <Params>

[nepovinný element]

Vstup	Popis
String	Volitelné, obsahuje další parametry. Zatím se nevyužívá.

8.1.3 Struktura odpovědi na požadavek

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <TimestampResponse xmlns="http://software602.com/secusign/">
      <TimestampResult>int</TimestampResult>
      <Output>base64Binary</Output>
      <StatusMessage>string</StatusMessage>
    </TimestampResponse>
  </soap:Body>
</soap:Envelope>
```

8.1.4 Výstupní parametry metody

8.1.4.1 <TimestampResult>

Návratová hodnota	Popis
int	Výsledek metody Timestamp (orazítkování dokumentu). 0 = v pořádku, jinak Návratové kódy všech metod a chyba popsaná ve StatusMessage.

8.1.4.2 <Output>

Návratová hodnota	Popis
base64Binary	Výstupní data orazítkovaného dokumentu kódovaná v Base64

8.1.4.3 <StatusMessage>

Návratová hodnota	Popis
String	Textová zpráva odpovídající celkovému výsledku orazítkování dokumentu. Hodnota je naplněna pouze v případě problematického výsledku.

9 Získání seznamu certifikátů

Metoda webové služby ListCerts umožňuje volajícímu systému/aplikaci získat seznam certifikátů ověřeného uživatele.

Metoda webové služby ListCerts2 umožňuje volajícímu systému/aplikaci k seznamu certifikátů ověřeného uživatele získat navíc informaci o typu zabezpečení certifikátu.

**Dostupnost metod ve webové definici je závislá na verzi webové služby SecuSign SDK (viz konfigurační příručka)*

9.1 Název metody: ListCerts

Popis služby včetně WSDL schématu a příklad požadavku a odpovědi pro SOAP 1.1 a SOAP 1.2 je umístěn na https://localhost/secusign/default.asmx?op=ListCerts *

* localhost je název používaný pro lokální počítač; namísto něj zvolte jméno/IP adresu SDK serveru (dle nastavení v IIS)

9.1.1 Požadavek v rozhraní SOAP 1.1

```
POST /secusign/default.asmx HTTP/1.1
Host: localhost
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://software602.com/secusign/ListCerts"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <ListCerts xmlns="http://software602.com/secusign/">
      <Params>string</Params>
      <IncludeNotEnabled>integer</IncludeNotEnabled>
    </ListCerts>
  </soap:Body>
</soap:Envelope>
```

9.1.2 Vstupní parametry metody

9.1.2.1 <Params>

[nepovinný element]

Vstup	Popis
string	Pokud nebyl uživatel autentizován k webové službě svým účtem (např. 602 ID), pak je možné specifikovat uživatele pomocí Identifikátoru uživatele (id_user) a Identifikátoru organizace (id_org). Zápis v podobě: Id_user=Name; id_org=IdentOrgGUID Standardně se počítá s autentizací a identifikací 602 ID účtu uživatele.

9.1.2.2 <IncludeNotEnabled>

[nepovinný element]

Vstup	Popis

Int	Vrátí i certifikáty, které jsou ve stavu DISABLED nebo REVOKED

9.1.3 Struktura odpovědi na požadavek

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <ListCertsResponse xmlns="http://software602.com/secusign/">
      <ListCertsResult>int</ListCertsResult>
      <CertList>
        <PKCS11CertInfo>
          <Alias>string</Alias>
          <X509CertData>base64Binary</X509CertData>
          <Status>string</Status>
        </PKCS11CertInfo>
        <PKCS11CertInfo>
          <Alias>string</Alias>
          <X509CertData>base64Binary</X509CertData>
          <Status>string</Status>
        </PKCS11CertInfo>
      </CertList>
      <StatusMessage>string</StatusMessage>
    </ListCertsResponse>
  </soap:Body>
</soap:Envelope>
```

9.1.4 Výstupní parametry metody

9.1.4.1 <ListCertsResult>

Návratová hodnota	Popis
Int	Výsledek metody ListCerts (získání seznamu certifikátů). 0 = v pořádku, jinak Návratové kódy všech metod a chyba popsaná ve StatusMessage.

9.1.4.2 <CertList>

Pole se seznamem certifikátů

9.1.4.3 <PKCS11CertInfo>

Informace o certifikátu

9.1.4.4 <Alias>

Návratová hodnota	Popis
String	Alias nebo li CertificateID uživatelského certifikátu v GUID formátu

9.1.4.5 <X509CertData>

Návratová hodnota	Popis
`Base64Binary`	Base64 Data certifikátu ve formátu X509

9.1.4.6 <Status>

Návratová hodnota	Popis
`String`	Stav uživatelského certifikátu. Hodnoty: ENABLED – povolený, lze použít. DISABLED – zakázaný, nelze použít. REVOKED – odvolaný, nelze použít. EXPIRED – vypršelý, nelze použít.

9.1.4.7 <StatusMessage>

Návratová hodnota	Popis
`String`	Textová zpráva odpovídající celkovému získání seznamu certifikátů. Hodnota je naplněna pouze v případě problematického výsledku.

9.2 Název metody: ListCerts2

Popis služby včetně WSDL schématu a příklad požadavku a odpovědi pro SOAP 1.1 a SOAP 1.2 je umístěn na https://localhost/secusign/default.asmx?op=ListCerts2 *

* localhost je název používaný pro lokální počítač; namísto něj zvolte jméno/IP adresu SDK serveru (dle nastavení v IIS)

9.2.1 Požadavek v rozhraní SOAP 1.1

```
POST /secusign/default.asmx HTTP/1.1
Host: localhost
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://software602.com/secusign/ListCerts2"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <ListCerts2 xmlns="http://software602.com/secusign/">
      <Params>string</Params>
      <IncludeNotEnabled>int</IncludeNotEnabled>
    </ListCerts2>
  </soap:Body>
</soap:Envelope>
```

9.2.2 Vstupní parametry metody

Stejné jako u metody ListCerts

9.2.3 Struktura odpovědi na požadavek

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <ListCerts2Response xmlns="http://software602.com/secusign/">
      <ListCerts2Result>int</ListCerts2Result>
      <CertList>
        <PKCS11CertInfo2>
          <Alias>string</Alias>
          <X509CertData>base64Binary</X509CertData>
          <Status>string</Status>
          <AuthMode>string</AuthMode>
        </PKCS11CertInfo2>
        <PKCS11CertInfo2>
          <Alias>string</Alias>
          <X509CertData>base64Binary</X509CertData>
          <Status>string</Status>
          <AuthMode>string</AuthMode>
        </PKCS11CertInfo2>
      </CertList>
      <StatusMessage>string</StatusMessage>
    </ListCerts2Response>
  </soap:Body>
</soap:Envelope>
```

9.2.4 Výstupní parametry metody

Stejné jako u metody ListCerts s tím rozdílem, že se vrací ListCerts2Result a PKCS11CertInfo2, a v rámci PKCS11CertInfo2 je navíc element:

9.2.4.1 <AuthMode>

Návratová hodnota	Popis
String	Zabezpečení přístupu k uživatelskému certifikátu. Hodnoty: PIN – uživatelským heslem (zvoleným při generování žádosti nebo poslední změně) 602KEY – druhým faktorem přes mobilní aplikaci 602®Key (zvoleným při nastavení ve správcovské aplikaci – typicky Sofa) V případě, že je u certifikátu nastaveno zabezpečení 602KEY, pak při podepsání certifikátem s tímto zabezpečením je zapotřebí ve volající aplikaci zobrazit dialog, který informuje uživatele o nutnosti potvrzení v mobilní aplikaci 602®Key, a s vhodným timeout (např. 1 minuta) vyčkat na odpověď služby. Pro potvrzování pomocí 602KEY je potřebné mít nastavenou vhodnou adresu webové služby HSM WS, viz Konfigurační příručka.

10 Získání pečeti / podpisu k hash

Metoda webové služby **SignHash** umožňuje vytvořit podpis/pečeť k hash libovolného dokumentu nebo datům.

Výpočet hash provádí volající aplikace, která je zodpovědná za správnost výpočtu hashe. Pro správné vytvoření podpisu/pečeti k danému hash je nutné, aby odpovídal také hashovací algoritmus.

Vrácený podpis/pečeť k hash je třeba odpovídajícím způsobem vložit do dat dokumentu (dle specifikací ETSI) nebo uchovat u daného souboru (v případě externího CMS podpisu).

**Dostupnost metody ve webové definici je závislá na verzi webové služby SecuSign SDK (viz konfigurační příručka)*

10.1 Název metody: SignHash

Popis služby včetně WSDL schématu a příklad požadavku a odpovědi pro SOAP 1.1 a SOAP 1.2 je umístěn na https://localhost/secusign/default.asmx?op=SignHash *

* localhost je název používaný pro lokální počítač; namísto něj zvolte jméno/IP adresu SDK serveru (dle nastavení v IIS)

10.1.1 Požadavek v rozhraní SOAP 1.1

```
POST /secusign/default.asmx HTTP/1.1
Host: localhost
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://software602.com/secusign/SignHash"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <SignHash xmlns="http://software602.com/secusign/">
      <Hash>base64Binary</Hash>
      <HashAlgOID>string</HashAlgOID>
      <CertificateID>string</CertificateID>
      <PrivateKeyPIN>string</PrivateKeyPIN>
      <SignatureFormat>integer</SignatureFormat>
      <Params>string</Params>
    </SignHash>
  </soap:Body>
</soap:Envelope>
```

10.1.2 Vstupní parametry metody

10.1.2.1 <Hash>

[povinný element]

Vstup	Popis
Base64Binary	Vypočtený Hash dokumentu nebo dat kódovaný v Base64 Pro výpočet kódovaného Base64 sha256 hash lze využít např. openssl ■ openssl sha256 -binary test.pdf >hash.bin ■ certutil -encode hash.bin hash.b64

	nebo třeba externí online aplikace: ■ https://md5file.com/calculator ■ https://base64.guru/converter/encode/hex

10.1.2.2 <HashAlgOID>

[povinný element]

Vstup	Popis
String	OID hashovacího algoritmu použitého pro výpočet. Například pro hashovací algoritmus SHA256 to je OID: 2.16.840.1.101.3.4.2.1

10.1.2.3 <CertificateID>

[nepovinný element]

Vstup	Popis

String	Identifikace certifikátu pro vytvoření zaručené/kvalifikované elektronické pečeti nebo zaručeného/kvalifikovaného elektronického podpisu.
	
	V případě in-house rozhraní SecuSign SDK je možné použít formáty:
	■ HStore:[alias]
	  ■ alias certifikátu pro podepsání/pečetění z HSM modulu služby Vzdáleného podepisování/pečetění.
	  ■ pokud je v konfiguraci webové služby nastaven konfigurační klíč Seal_DefaultToQStore, prefix HStore se neuvádí
	■ PKCS11:[alias]
	  ■ alias certifikátu pro podepsání/pečetění z HSM modulu klienta nebo ze systémového úložiště Windows.
	■ QStore:[alias]
	  ■ Pečetí se certifikátem nahraným na účtu klienta v Azure KeyVault.
	■ urn:hex:[hexadecimalne_kodovany_sha1_hash_certu]
	  ■ podepsání/pečetění certifikátem ze systémového úložiště Windows pod Current User. Nutné spouštět aplikační pool pod konkrétním uživatelem.
	■ urn:sha:[Base64_kodovany_sha1_hash_certu]
	  ■ podepsání/pečetění certifikátem ze systémového úložiště Windows pod Current User. Nutné spouštět aplikační pool pod konkrétním uživatelem.
	■ [cesta k PFX]
	  ■ podepsání konkrétním PFX, který je lokálně přístupný pro webovou službu/aplikaci v souboru.
	■ prázdný řetězec
	  ■ použije se nastavení SigningCertPath v konfiguraci webové služby SecuSign SDK.
	  ■ pokud je v konfiguraci webové služby nastaven konfigurační klíč Seal_DefaultToQStore, pak se použije výchozí certifikát ze služby Vzdáleného pečetění

	V případě webových služeb SecuSign v Azure je možné použít např. hodnotu z CN nebo SERIALNUMBER – obě informace je možné zjistit v administraci služby SecuSign > Seal po přihlášení do uživatelského rozhraní 602 ID účtu. Výchozí hodnota: prázdný řetězec

10.1.2.4 <PrivateKeyPIN>

[nepovinný element]

Vstup	Popis
string	PIN, který byl zvolen žadatelem jako přístupové heslo k privátní části certifikátu Hodnota je povinná v případě `QStore, PKCS11` a souboru PFX. V případě použití `HStore` aliasu záleží, zda se používá pro podepisování nebo pečetění. Pro podepisování s nastaveným potvrzením pomocí PIN je nutné `PrivateKeyPIN` uvést. Pro podepisování s nastaveným potvrzením pomocí 602KEY se `PrivateKeyPIN` neuvádí. Pro pečetění není nutné `PrivateKeyPIN` uvádět, protože přístup k certifikátu je definován na základě autentizačního (licenčního) certifikátu volající aplikace, pokud není zvoleno jinak.

10.1.2.5 <SignatureFormat>

[nepovinný element]

Vstup	Popis
Int	Typ podpisu/pečeti. Hodnoty: 0 = CMS (CAdES detached)[default], 1 = PKCS1 signature, 2 = PKCS1 signature, ale parametr Hash obsahuje přímo DigestInfo (struktura obsahující hash dokumentu a OID použitého hash algoritmu)

10.1.2.6 <Params>

[nepovinný element]

Vstup	Popis
String	Nepovinné, aktuálně se nevyužívá

10.1.3 Struktura odpovědi na požadavek

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <SignHashResponse xmlns="http://software602.com/secusign/">
      <SignHashResult>int</SignHashResult>
```

```
      <Output>base64Binary</Output>
      <SigningCert>base64Binary</SigningCert>
      <StatusMessage>string</StatusMessage>
    </SignHashResponse>
  </soap:Body>
</soap:Envelope>
```

10.1.4 Výstupní parametry metody

10.1.4.1 <SignHashResult>

Návratová hodnota	Popis
Int	Výsledek metody SignHash (získání podpis/pečeti k hash). 0 = v pořádku, jinak Návratové kódy všech metod a chyba popsaná ve StatusMessage.

10.1.4.2 <Output>

Návratová hodnota	Popis
Base64Binary	Podepsaná data ve formátu CMS nebo PKCS1 kódovaná v Base64.

10.1.4.3 <SigningCert>

Návratová hodnota	Popis
Base64Binary	Data X.509 certifikátu použitého pro podpis/pečeť kódovaná v Base64. Ze získaných dat lze po dekódování zjistit např. vystavitel certifikátu, pro koho byl certifikát vystaven, platnost certifikátu od-do, kryptografický otisk (hash) a další informace.

10.1.4.4 <StatusMessage>

Návratová hodnota	Popis
String	Textová zpráva odpovídající celkovému výsledku získání pečeti/podpisu k hash. Hodnota je naplněna pouze v případě problematického výsledku.

11 Získání dat certifikátu pro vložení pečeti/podpisu

Metoda webové služby **GetCertificate** slouží volajícím aplikacím pro získání dat certifikátu a přípravu datového prostoru k vložení získaného podpisu/pečeti, např. do dat PDF nebo XML souboru.

**Dostupnost metody ve webové definici je závislá na verzi webové služby SecuSign SDK (viz konfigurační příručka)*

11.1 Název metody: GetCertificate

Popis služby včetně WSDL schématu a příklad požadavku a odpovědi pro SOAP 1.1 a SOAP 1.2 je umístěn na https://localhost/secusign/default.asmx?op=GetCertificate *

* localhost je název používaný pro lokální počítač; namísto něj zvolte jméno/IP adresu SDK serveru (dle nastavení v IIS)

11.1.1 Požadavek v rozhraní SOAP 1.1

```
POST /secusign/default.asmx HTTP/1.1
Host: localhost
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://software602.com/secusign/GetCertificate"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <GetCertificate xmlns="http://software602.com/secusign/">
      <CertificateID>string</CertificateID>
      <Params>string</Params>
    </GetCertificate>
  </soap:Body>
</soap:Envelope>
```

11.1.2 Vstupní parametry metody

11.1.2.1 <CertificateID>

[povinný element]

Vstup	Popis
String	Identifikace certifikátu pro získání dat a přípravu k vložení zaručené/kvalifikované elektronické pečeti nebo zaručeného/kvalifikovaného elektronického podpisu. V případě in-house rozhraní SecuSign SDK je možné použít formáty: ■ HStore:[alias] ■ alias certifikátu pro podepsání/pečetění z HSM modulu služby Vzdáleného podepisování/pečetění. ■ pokud je v konfiguraci webové služby nastaven konfigurační klíč Seal_DefaultToQStore, prefix HStore se neuvádí

	■ prázdný řetězec ■ pokud je v konfiguraci webové služby nastaven konfigurační klíč Seal_DefaultToQStore, pak se použije výchozí certifikát ze služby Vzdáleného pečetění Výchozí hodnota: `prázdný řetězec`

11.1.2.2 <Params>

[nepovinný element]

Vstup	Popis
String	Nepovinné, aktuálně se nevyužívá

11.1.3 Struktura odpovědi na požadavek

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <GetCertificateResponse xmlns="http://software602.com/secusign/">
      <GetCertificateResult>int</GetCertificateResult>
      <X509Certificate>base64Binary</X509Certificate>
      <StatusMessage>string</StatusMessage>
    </GetCertificateResponse>
  </soap:Body>
</soap:Envelope>
```

11.1.4 Výstupní parametry metody

11.1.4.1 <GetCertificateResult>

Návratová hodnota	Popis
Int	Výsledek metody GetCertificate (získání dat certifikátu). 0 = v pořádku, jinak Návratové kódy všech metod a chyba popsaná ve StatusMessage.

11.1.4.2 <X509Certificate>

Návratová hodnota	Popis
Base64Binary	Base64 Data certifikátu ve formátu X509

11.1.4.3 <StatusMessage>

Návratová hodnota	Popis

`String`	Textová zpráva odpovídající celkovému výsledku získání dat certifikátu. Hodnota je naplněna pouze v případě problematického výsledku.

12 Ověřování platnosti certifikátů

Metoda ValidateCertificate webové služby SecuSign umožňuje ověřit platnost certifikátů ve formátu X.509, jejichž vystavitel je dostupný ve vzdáleném úložišti (databázi) backendového serveru SecuSign nebo v interním úložišti (složce) SecuSign SDK serveru zákazníka.

Od června 2020 je možné ověřit, zda daný certifikát je kvalifikovaný a vydaný poskytovateli platebních služeb splňujících Reference[14].

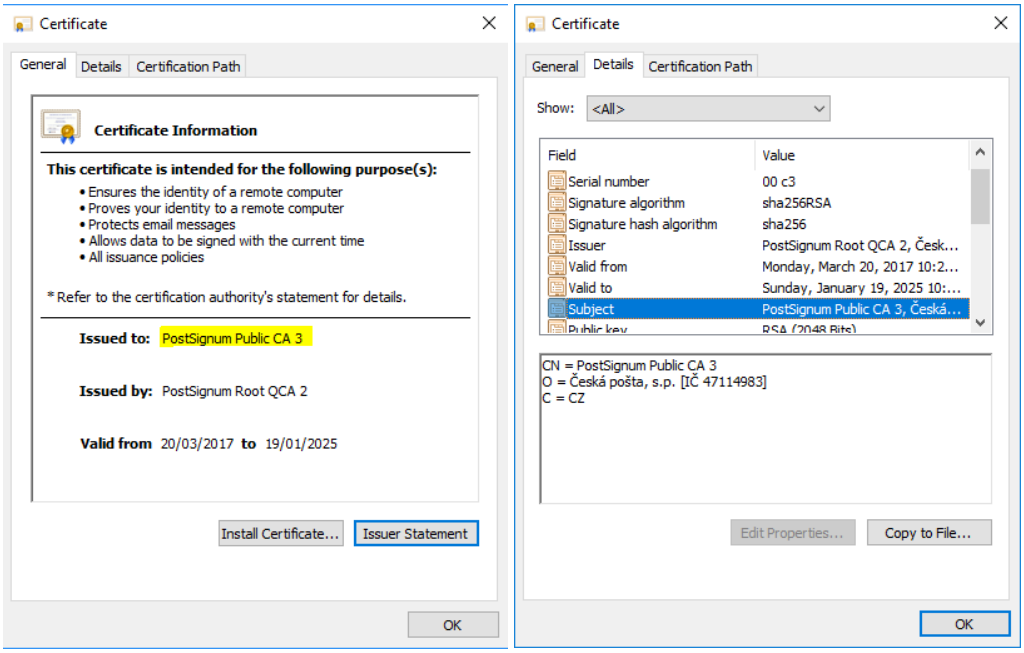
Ověřuje se správnost formátu, zda je certifikát platný, kvalifikovaný, případně vypršelý nebo revokovaný. V případě PSD2 certifikátu je navíc provedena kontrola na určení certifikátu, obsažené atributy a platnost licence pro jednotlivé činnosti.
Vrací se informace o typu a platnosti certifikátu, subjektu (komu byl vydán), vystaviteli, sériovém číslu, důvěryhodné kotvě, revokační informace a další. V případě PSD2 certifikátu se navíc vrací název a identifikátor národní kompetentní autority, identifikátor poskytovatele platebních služeb a povolených rolí (činností), a záznam z daného registru obsahující detailnější informace o poskytovateli platebních služeb a platnosti jednotlivých činností (licencí).

Implementováno: od verze 2.0.759.0628
Aktualizováno: ve verzi 2.1.7268.1218
Aktualizováno (PSD2): ve verzi 2.1.7474.0624
Implementace ověřování certifikátů PSD2 je dle ETSI normy viz Reference[14]

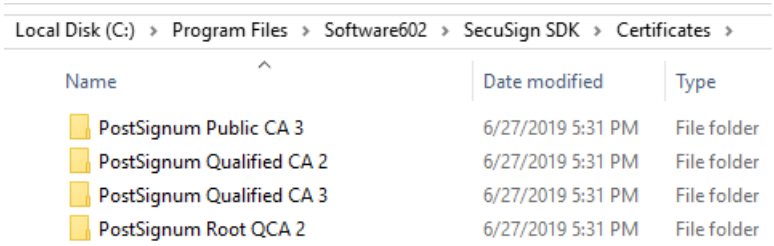
12.1 Konfigurace

Pro funkčnost ověřování certifikátů z interního umístění (složky) serveru je třeba provést konfiguraci webové služby. Postup:

- Do elementu <*appSettings*> konfiguračního souboru webové služby *InstallDir\WebService\Web.config* přidat nový klíč *SecusignConfigPath* s cestou ke konfiguračnímu souboru s*ecusign.properties*:
  - <add key="SecusignConfigPath" value="C:\Program Files\Software602\SecuSign SDK\AdES\secusign.properties" />
    - Lze zvolit jakoukoliv vlastní cestu, kde má webová služba právo čtení
- V konfiguračním souboru *secusign.properties* je třeba nastavit cestu k adresáři s certifikáty, které tvoří certifikační cestu pro ověření certifikátu. Příklad:
  - Lokální složka serveru:
    - CERTIFICATE_READER_DIRECTORY = c:\\SecuSign\\Certificates
  - SMB disk:
    - CERTIFICATE_READER_DIRECTORY = \\\\IP_ADRESA\\SecuSign\\Certificates\\
- Služba čeká, že v nastaveném CERTIFICATE_READER_DIRECTORY umístění budou jednotlivé certifikáty uloženy ve svých podadresářích.
  - Název podadresáře se musí shodovat s názvem certifikátu, pro koho byl vystaven.
  - Název certifikátu lze zjistit z vlastností certifikátu, kde je v položce *Subject* uveden jako hodnota "CN = <*hodnota*>“, příklad:



Příklad adresářové struktury Certificates:



Upozornění:

- V případě, že jsou v názvu certifikátu lomítka (/), tak název adresáře musí být bez nich.
  - Příklad: Název certifikátu = I.CA Qualified 2 CA/RSA 02/2016; Název adresáře = I.CA Qualified 2 CARSA 022016
- V případě rekonfigurace *secusign.properties* je třeba restartovat aplikační pool webové služby SecuSign.
- Funkčnost je možné testovat na prostředí (Web.config klíč Environment) QSTEST.

12.2 Název metody: ValidateCertificate

Popis služby včetně WSDL schématu a příklad požadavku a odpovědi pro SOAP 1.1 a SOAP 1.2 je umístěn na https://localhost/secusign/default.asmx?op=ValidateCertificate *

* localhost je název používaný pro lokální počítač; namísto něj zvolte jméno/IP adresu SDK serveru (dle nastavení v IIS)

12.2.1 Požadavek v rozhraní SOAP 1.1

```
POST /secusign/default.asmx HTTP/1.1
Host: localhost
Content-Type: text/xml; charset=utf-8
Content-Length: length
```

```
SOAPAction: "http://software602.com/secusign/ValidateCertificate"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <ValidateCertificate xmlns="http://software602.com/secusign/">
      <FileName>string</FileName>
      <FileData>base64Binary</FileData>
      <FileType>CERTIFICATE</FileType>
      <Properties>
        <ValidationTime>dateTime</ValidationTime>
        <Psd2Scope>string</Psd2Scope>
        <Psd2Country>string</Psd2Country>
      </Properties>
      <Params>string</Params>
    </ValidateCertificate>
  </soap:Body>
```

12.2.2 Vstupní parametry metody

12.2.2.1 <FileName>

[povinný element]

Vstup	Popis
String	Název vstupního souboru (včetně přípony), který se má ověřit. Příklad: Certificate.cer Max. 260 znaků.

12.2.2.2 <FileData>

[povinný element]

Vstup	Popis
Base64Binary	Data vstupního souboru s certifikátem kódovaná v Base64

12.2.2.3 <FileType>

[povinný element]

Vstup	Popis
CERTIFICATE	Typ vstupních dat souboru. CERTIFICATE = X.509 certifikát

12.2.2.4 <Properties>

[nepovinný element]

12.2.2.4.1 <ValidationTime>

[nepovinný element]

Vstup	Popis
dateTime	Definuje rozhodný okamžik, ke kterému se má ověřovat platnost certifikátu. Příklad hodnoty: `2018-11-09T07:35:00+02:00` *(vč. časové zóny)*

	Pokud údaj `ValidationTime` není zadán, nastaví se rozhodný okamžik na aktuální. Výchozí hodnota: *Now* (aktuální čas ze SecuSign serveru)

12.2.2.4.2 <Psd2Scope>

[nepovinný element]

Vstup	Popis
string	Činnost, pro kterou musí být licence platná. Tímto parametrem se limitují vrácené činnosti pro daný záznam v registru. Možné hodnoty: PSP_AS - vedení účtu PSP_PI - iniciování platby PSP_AI - informování o účtu PSP_IC - vydávání karetních platebních prostředků Pokud není parametr zadán, vrací se všechny platné záznamy nehledě na činnost. Parametr je case insensitive. Výchozí hodnota: všechny

12.2.2.4.3 <Psd2Country>

[nepovinný element]

Vstup	Popis
string	Země, ve které musí být licence platná. Tímto parametrem se limitují vrácené činnosti pro daný záznam. Možné hodnoty: cz – Česká republika sk – Slovenská republika Pokud není parametr zadán, použije se výchozí hodnota 'cz' pro Českou republiku. Parametr je case insensitive. Výchozí hodnota: cz

12.2.2.5 </Properties>

12.2.2.6 <Params>

[nepovinný element]

Vstup	Popis
String	Pro ověřování certifikátů se nepoužívá

12.2.3 Struktura odpovědi na požadavek

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <ValidateCertificateResponse xmlns="http://software602.com/secusign/">
      <ValidateCertificateResult>int</ValidateCertificateResult>
      <certificateValidationInfo>
            <psd2Verification>
               <validityCheck>boolean</validityCheck>
               <validityCheckMessage>string</validityCheckMessage>
               <qualifiedCheck>boolean</qualifiedCheck>
               <qualifiedCheckMessage>string</qualifiedCheckMessage>
               <qualifiedCertTypeCheck>boolean</qualifiedCertTypeCheck>

<qualifiedCertTypeCheckMessage>string</qualifiedCertTypeCheckMessage>
               <psd2QcStatementCheck>boolean</psd2QcStatementCheck>
               <psd2QcStatementCheckMessage>string</psd2QcStatementCheckMessage>
               <organizationIdentifierCheck>boolean</organizationIdentifierCheck>

<organizationIdentifierCheckMessage>string</organizationIdentifierCheckMessage>
               <registryCheck>boolean</registryCheck>
               <registryCheckMessage>string</registryCheckMessage>
               <psd2Status>string</psd2Status>
            </psd2Verification>
            <Guid>string</Guid>
            <filename>string</filename>
            <statusIndication>string</statusIndication>
            <statusSubindication>string</statusSubindication>
            <certType>string</certType>
            <qualifiedCertType>string</qualifiedCertType>
            <validationMaterial>
               <validationDate>dateTime</validationDate>
               <certificatePath>
                  <certificate xsi:nil="true" />
                     <uid>4a93397eb251 .. d8c4d5301</uid>
                     <issuerUid>d35e250cb0 .. 12b54e3b1f02</issuerUid>
                     <revocationUid>8e5fa57178b5c1b .. 18720beb1310</revocationUid>
                     <isEndCertificate>true</isEndCertificate>
                     <isTrustedAnchor>false</isTrustedAnchor>
                     <notBefore>2019-05-24T11:32:41+02:00</notBefore>
                     <notAfter>2020-05-23T11:32:41+02:00</notAfter>
                     <subject>C=CZ,2.5.4.97=NTRCZ-63078236,O=Software602 a.s. [IČ
63078236],OU=254,CN=Jmeno
Prijmeni,SURNAME=Prijmeni,GIVENNAME=Jmeno,SERIALNUMBER=P564111</subject>
                     <issuer>C=CZ,O=Česká pošta\, s.p. [IČ 47114983],CN=PostSignum
Qualified CA 3</issuer>
                     <serialNumber>511111</serialNumber>
                     <qcStatements>
                        <qcStatement name="qc-compliance">0.4.0.1862.1.1</qcStatement>
                        <qcStatement name="qc-sscd">0.4.0.1862.1.4</qcStatement>
                        <qcStatement name="qc-pds">0.4.0.1862.1.5</qcStatement>
                        <qcStatement name="qc-type">0.4.0.1862.1.6</qcStatement>
                     </qcStatements>
                     <qcTypes>
                        <qcType name="esign">0.4.0.1862.1.6.1</qcType>
                     </qcTypes>
                     <certType>QUALIFIED</certType>
```

```
                     <qualifiedCertType>ESIGN</qualifiedCertType>
                     <ordinalNumber>0</ordinalNumber>
                     <isSelfSigned>false</isSelfSigned>
                     <source>SECUSIGN</source>
                     <psd2Data>
                        <record>
                           <registryType>eba</registryType>
                           <code>IE_CBI!C190092</code>
                           <pspId>C190092</pspId>
                           <name>CRIF RealTime Ireland Limited</name>
                           <address>Adelphi plaza, George's Street Upper, Dún
Laoghaire</address>
                           <city>Dublin</city>
                           <country>IE</country>
                           <licences>
                              <licence>
                                 <country>CZ</country>
                                 <type>PSD_AISP</type>
                                 <scope>PSP_AI</scope>
                                 <validFrom>2019-05-30T02:00:00+02:00</validFrom>
                                 <validTo>0001-01-01T00:00:00</validTo>
                              </licence>
                           </licences>
                        </record>
                        <psd2>
                           <NCAName>Central Bank of Ireland</NCAName>
                           <NCAId>IE-CBI</NCAId>
                           <rolesOfPsp>
                              <roleOfPsp name="PSP_AI">0.4.0.19495.1.3</roleOfPsp>
                           </rolesOfPsp>
                           <organizationIdentifier>PSDIE-CBI-
C190092</organizationIdentifier>
                           <pspIdentifier>C190092</pspIdentifier>
                        </psd2>
                     </psd2Data>
                  </certificate>
                  <certificate xsi:nil="true" />
                     <uid>d35e250cb02e27 .. 54e3b1f02</uid>
                     <issuerUid>ad016f958 .. edddc7d6578</issuerUid>
                     <revocationUid>e7b26c175d3dc6f6 .. e15d485ab5e</revocationUid>
                     <isEndCertificate>false</isEndCertificate>
                     <isTrustedAnchor>false</isTrustedAnchor>
                     <notBefore>2014-03-26T09:01:32+01:00</notBefore>
                     <notAfter>2024-03-26T08:00:36+01:00</notAfter>
                     <subject>C=CZ,O=Česká pošta\, s.p. [IČ 47114983],CN=PostSignum
Qualified CA 3</subject>
                     <issuer>C=CZ,O=Česká pošta\, s.p. [IČ 47114983],CN=PostSignum Root
QCA 2</issuer>
                     <serialNumber>164</serialNumber>
                     <qcStatements/>
                     <qcTypes/>

<serviceTypeUri>http://www.602.cz/TrstSvc/Svctype/QCA_ASC</serviceTypeUri>
                     <ordinalNumber>2</ordinalNumber>
                     <isSelfSigned>true</isSelfSigned>
                     <source>SECUSIGN</source>
                  </certificate>
                  <certificate xsi:nil="true" />
                     <uid>ad016f958050 .. edddc7d6578</uid>
                     <issuerUid>ad016f958050e0 .. dddc7d6578</issuerUid>
                     <isEndCertificate>false</isEndCertificate>
                     <isTrustedAnchor>true</isTrustedAnchor>
                     <notBefore>2010-01-19T09:04:31+01:00</notBefore>
                     <notAfter>2025-01-19T09:04:31+01:00</notAfter>
                     <subject>C=CZ,O=Česká pošta\, s.p. [IČ 47114983],CN=PostSignum Root
QCA 2</subject>
```

```
                     <issuer>C=CZ,O=Česká pošta\, s.p. [IČ 47114983],CN=PostSignum Root
QCA 2</issuer>
                     <serialNumber>100</serialNumber>
                     <qcStatements/>
                     <qcTypes/>

<serviceStatusUri>http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</serviceStatu
sUri>

<serviceTypeUri>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</serviceTypeUri>
                     <ordinalNumber>1</ordinalNumber>
                     <isSelfSigned>false</isSelfSigned>
                     <source>SECUSIGN</source>
                  </certificate>
               </certificatePath>
               <revocations xsi:nil="true" />
                  <revocation>
                     <uid>8e5fa57178 .. 8720beb1310</uid>
                     <type>OCSP</type>
                     <thisUpdate>2019-06-27T11:23:41+02:00</thisUpdate>
                     <nextUpdate xsi:nil="true"/>
                     <producedAt>2019-06-27T11:23:41+02:00</producedAt>
                  </revocation>
                  <revocation>
                     <uid>e7b26c175d3d .. 1e15d485ab5e</uid>
                     <type>CRL</type>
                     <thisUpdate>2018-10-25T09:56:02+02:00</thisUpdate>
                     <nextUpdate>2019-10-25T10:01:02+02:00</nextUpdate>
                     <producedAt xsi:nil="true"/>
                     <source>SECUSIGN</source>
                  </revocation>
                  <revocation>
                     <uid>ea6ce4a9bef17 .. 468f50440ff9</uid>
                     <type>OCSP</type>
                     <thisUpdate>2019-12-18T17:00:35+01:00</thisUpdate>
                     <nextUpdate xsi:nil="true"/>
                     <producedAt>2019-12-18T17:00:35+01:00</producedAt>
                     <source>SECUSIGN</source>
                  </revocation>
               </revocations>
            </validationMaterial>
         </certificateValidationInfo>
      <StatusMessage>string</StatusMessage>
    </ValidateCertificateResponse>
  </soap:Body>
</soap:Envelope>
```

12.2.4 Výstupní parametry metody

12.2.4.1 <ValidateCertificateResult>

Návratová hodnota	Popis
Int	Výsledek metody ValidateCertificateResult (ověření platnosti certifikátu). 0 = v pořádku, jinak Návratové kódy všech metod a chyba popsaná ve StatusMessage.

12.2.4.2 <psd2Verification>

Vrací se jen v případě ověřování PSD2 certifikátu.

12.2.4.2.1 <validityCheck>

Návratová hodnota	Popis
`Boolean`	Kontrola platnosti certifikátu. Certifikát musí být v době ověření platný.

12.2.4.2.2 <validityCheckMessage>

Návratová hodnota	Popis
`String`	Vrací textovou informaci v případě, že kontrola platnosti certifikátu selhala.

12.2.4.2.3 <qualifiedCheck>

Návratová hodnota	Popis
`Boolean`	Kontrola, že certifikát je kvalifikovaný.

12.2.4.2.4 <qualifiedCheckMessage>

Návratová hodnota	Popis
`String`	Vrací textovou informaci v případě, že kontrola kvalifikovanosti certifikátu selhala.

12.2.4.2.5 <qualifiedCertTypeCheck>

Návratová hodnota	Popis
`Boolean`	Kontrola, že certifikát je určený pro pečetění (SEAL) nebo webovou autentizaci (WEB).

12.2.4.2.6 <qualifiedCertTypeCheckMessage>

Návratová hodnota	Popis
`String`	Vrací textovou informaci v případě, že kontrola typu certifikátu selhala.

12.2.4.2.7 <psd2QcStatementCheck>

Návratová hodnota	Popis
`Boolean`	Kontrola, že certifikát obsahuje PSD2 QCStatement a ten obsahuje potřebné atributy.

12.2.4.2.8 <psd2QcStatementCheckMessage>

Návratová hodnota	Popis
`String`	Vrací textovou informaci v případě, že kontrola PSD2 QCStatement a potřebného atributu v certifikátu selhala.

12.2.4.2.9 <organizationIdentifierCheck>

Návratová hodnota	Popis
`Boolean`	Kontrola, že certifikát obsahuje atribut organizationIdentifier a ten je ve správném formátu.

12.2.4.2.10 <organizationIdentifierCheckMessage>

Návratová hodnota	Popis
`String`	Vrací textovou informaci v případě, že kontrola atributu organizationalIdentifier a správnosti formátu selhala.

12.2.4.2.11 <registryCheck>

Návratová hodnota	Popis
`Boolean`	Kontrola záznamu v registru. V registru byl nalezen platný záznam pro daného poskytovatele platebních služeb a tento tento záznam obsahuje platné licence pro dotazované činnosti. Ty musí být také uvedené v certifikátu

12.2.4.2.12 <registryCheckMessage>

Návratová hodnota	Popis
`String`	Vrací textovou informaci v případě, že kontrola záznamu v registru selhala.

12.2.4.2.13 <validLicensesCheck>

Návratová hodnota	Popis
`Boolean`	Kontrola platnosti dotazované licence. Tato kontrola říká, zda dané činnosti jsou pro danou zemi aktivní. V dotazu je možné zadat činnost, pro jakou se platnost kontroluje (Psd2Scope) a zemi, v jaké se platnost kontroluje (Psd2Country). Pokud není zadáno, kontrolují se všechny činnosti uvedené v certifikátu pro výchozí zemi (cz – Česká republika). Možné hodnoty: PSP_AS - Account servicing (vedení účtu) PSP_PI - Payment initiation (iniciování platby) PSP_AI - Account information (informování o účtu) PSP_IC - Issuing of card-based payment instruments (vydávání karetních platebních prostředků)

12.2.4.2.14 <validLicensesCheckMessage>

Návratová hodnota	Popis
`String`	Obsahuje případné doplňující informace o kontrole platnosti dotazované licence (v češtině).

12.2.4.2.15 <psd2Status>

Návratová hodnota	Popis
`String`	Ověření PSD2 statusu pro daný certifikát. Výsledek může nabývat následujících hodnot: QWAC - kvalifikovaný autentizační certifikát pro web, který splňuje PSD2 QsealC - kvalifikovaný pečetící certifikát pro web, který splňuje PSD2 FAIL - pokud některá z podmínek není splněna

12.2.4.3 </psd2Verification>

12.2.4.4 <Guid>

Návratová hodnota	Popis
String	Unikátní ID daného volání metody ověření certifikátu

12.2.4.5 <filename>

Návratová hodnota	Popis
String	Název souboru s ověřovaným certifikátem. Max. 260 znaků.

12.2.4.6 <statusIndication>

Návratová hodnota	Popis
String	Výsledný stav (indikace) ověření certifikátu. Může nabývat hodnot: VALID – certifikát je vyhodnocen jako platný INDETERMINATE – o stavu certifikátu není možné v tuto chvíli rozhodnout INVALID – certifikát je vyhodnocen jako neplatný

12.2.4.7 <statusSubindication>

Návratová hodnota	Popis
String	Doplňující stav (indikace) ověření certifikátu. Může nabývat hodnot: OK – certifikát je vyhodnocen jako platný EXPIRED – ověřovaný certifikát byl v době ověření expirovaný (neplatný) NO_CERTIFICATE_CHAIN_FOUND – nelze sestavit certifikační cestu vystavitele certifikátu REVOKED – certifikát byl odvolán FORMAT_FAILURE – chyba formátu vstupních dat certifikátu

12.2.4.8 <certType>

Návratová hodnota	Popis
String	Typ ověřovaného certifikátu. Může nabývat hodnot: QUALIFIED – kvalifikovaný certifikát COMMERCIAL – komerční certifikát INTERNAL_STORAGE – certifikát pocházející z interního úložiště (byla sestavena certifikační cesta z důvěryhodného úložiště, ale typ není možné určit) UNKNOWN – neznámý certifikát (nebyla sestavena cesta a není možné určit typ)

12.2.4.9 <qualifiedCertType>

Návratová hodnota	Popis
String	Typ kvalifikovaného certifikátu, vrací se jen v tomto případě. Může nabývat hodnot: ESIGN – certifikát pro elektronický podpis ESEAL – certifikát pro elektronickou pečeť WEB – certifikát pro autentizaci k webu/službám UNKNOWN – neznámý certifikát (není možné určit)

12.2.4.10 <validationMaterial>

12.2.4.10.1 <validationDate>

Návratová hodnota	Popis
dateTime	Datum, ke kterému probíhalo ověření platnosti certifikátu

12.2.4.10.2 <certificatePath>

Certifikační cesta od ověřovaného koncového certifikátu až ke kořenovému certifikátu

12.2.4.10.2.1 <certificate xsi:nil="true">

12.2.4.10.2.2 <uid>

Návratová hodnota	Popis
String	Unikátní identifikátor ověřovaného certifikátu. Jedná se o SHA 256 otisk daného certifikátu.

12.2.4.10.2.3 <issuerUid>

Návratová hodnota	Popis
String	Unikátní identifikátor certifikátu vystavitele daného certifikátu. Jedná se o SHA 256 otisk daného certifikátu.

12.2.4.10.2.4 <revocationUid>

Návratová hodnota	Popis
String	Unikátní identifikátor revokačních informací získaných k ověřovanému certifikátu. Jedná se o SHA 256 otisk daných revokačních dat.

12.2.4.10.2.5 <isEndCertificate>

Návratová hodnota	Popis
Boolean	Určuje, zda se jedná o koncový certifikát

12.2.4.10.2.6 <isTrustedAnchor>

Návratová hodnota	Popis

Boolean	Určuje, zda se jedná o důvěryhodnou kotvu (ke kořenovému certifikátu)

12.2.4.10.2.7 <notBefore>

Návratová hodnota	Popis
dateTime	Datum a čas začátku platnosti certifikátu

12.2.4.10.2.8 <notAfter>

Návratová hodnota	Popis
dateTime	Datum a čas konce platnosti certifikátu

12.2.4.10.2.9 <subject>

Návratová hodnota	Popis
String	Informace z certifikátového atributu Subjekt, např.: CN = Common Name (Běžné jméno) GN = Given Name (Křestní jméno) SN = Surname (Příjmení) SERIALNUMBER = Sériové číslo C = Country (Země) L = Locality (Lokalita) E = Email O = Organization (Organizace) OU = Organizational unit (Organizační jednotka) Pseudonyme = pseudonym

12.2.4.10.2.10 <issuer>

Návratová hodnota	Popis
String	Kompletní informace o vystaviteli certifikátu z atributu Issuer

12.2.4.10.2.11 <serialNumber>

Návratová hodnota	Popis
String	Sériové číslo ověřovaného certifikátu (v dekadickém tvaru)

12.2.4.10.2.12 <qcStatements>

12.2.4.10.2.12.1 <qcStatement>

Návratová hodnota	Popis
String	Prohlášení vystavitele kvalifikovaného certifikátu ve formě OID. Může nabývat hodnot, např.: 0.4.0.1862.1.1 = qc-compliance (Evropský kvalifikovaný certifikát)

	0.4.0.1862.1.4 = qc-sscd (Certifikát je uložen na kvalifikovaném prostředku (QSCD) dle eIDAS - Nařízení Evropského parlamentu a rady (EU) č. 910/2014) 0.4.0.1862.1.5 = qc-pds (Zpráva pro uživatele) 0.4.0.1862.1.6 = qc-type (Typ certifikátu)

</qcStatements>

12.2.4.10.2.13 <qcTypes>

12.2.4.10.2.13.1 <qcType>

Návratová hodnota	Popis
String	Typ certifikátu podpisu/pečeti/razítka dle eIDAS, pouze u certifikátů typu QUALIFIED a LEGACY. Může nabývat hodnot, např.: 0.4.0.1862.1.6.1 = Certifikát pro elektronický podpis dle eIDAS - Nařízení Evropského parlamentu a rady (EU) č. 910/2014 0.4.0.1862.1.6.2 = Certifikát pro elektronickou pečeť dle eIDAS - Nařízení Evropského parlamentu a rady (EU) č. 910/2014 0.4.0.1862.1.6.3 = Certifikát pro autentizaci internetových stránek dle eIDAS - Nařízení Evropského parlamentu a rady (EU) č. 910/2014

12.2.4.10.2.14 </qcTypes>

12.2.4.10.2.15 <certType>

Návratová hodnota	Popis
String	Typ ověřovaného certifikátu. Může nabývat hodnot: QUALIFIED – kvalifikovaný certifikát COMMERCIAL – komerční certifikát INTERNAL_STORAGE – certifikát pocházející z interního úložiště (byla sestavena certifikační cesta z důvěryhodného úložiště, ale typ není možné určit) UNKNOWN – neznámý certifikát (nebyla sestavena cesta a není možné určit typ)

12.2.4.10.2.16 <qualifiedCertType>

Návratová hodnota	Popis
String	Typ kvalifikovaného certifikátu, vrací se jen v tomto případě. Může nabývat hodnot: ESIGN – certifikát pro elektronický podpis ESEAL – certifikát pro elektronickou pečeť WEB – certifikát pro autentizaci k webu/službám UNKNOWN – neznámý certifikát (není možné určit)

12.2.4.10.2.17 <ServiceStatusUri>

Návratová hodnota	Popis
String	Obsahuje celou Uri stanovující servisní stav autority na TSL, např. http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted

12.2.4.10.2.18 <ServiceTypeUri>

Návratová hodnota	Popis
String	Obsahuje celou Uri stanovující servisní typ autority na TSL, např. http://uri.etsi.org/TrstSvc/Svctype/CA/QC

12.2.4.10.2.19 <ordinalNumber>

Návratová hodnota	Popis
String	Pořadí certifikátu v hierarchii kotvy ke kořenovému certifikátu vydávající certifikační autority. Může nabývat hodnot (0 od koncového až po N): 0 – koncový (end) 1 – mezilehlý (intermediate) 2 – může být mezilehlý nebo kořenový (intermediate nebo root) 3 …

12.2.4.10.2.20 <isSelfSigned>

Návratová hodnota	Popis
Boolean	Indikuje, zda je certifikát podepsán sebou samým. Nabývá hodnot false/true True se vrací např. v případě kořenového certifikátu.

12.2.4.10.2.21 <source>

Návratová hodnota	Popis
String	Indikuje zdroj důvěryhodného úložiště, vůči kterému se certifikát ověřoval. Může nabývat hodnot: SECUSIGN – backendové servery služby SecuSign INTERNAL_STORAGE – lokální úložiště certifikátů na SecuSign SDK serveru zákazníka

12.2.4.10.2.22 <psd2Data>

Vrací se jen v případě ověřování PSD2 certifikátu.

12.2.4.10.2.22.1 <record>

12.2.4.10.2.22.2 <registryType>

Návratová hodnota	Popis
String	Obsahuje informaci o tom, jaký registr byl použit pro vyhledání záznamu. Může nabývat hodnot: eba - evropský registr (spravuje European Banking Authority) cz - český registr (spravuje Česká národní banka) sk – slovenský registr (spravuje Národná banka Slovenska).

12.2.4.10.2.22.3 <code>

Návratová hodnota	Popis
String	Obsahuje identifikátor organizace v daném registru.

	Příklad: IE_CBI!C190092

12.2.4.10.2.22.4 <pspId>

Návratová hodnota	Popis
String	Obsahuje identifikátor poskytovatele platebních služeb, tedy stejnou informaci, jaká je i v certifikátu.

12.2.4.10.2.22.5 <name>

Návratová hodnota	Popis
String	Obsahuje název poskytovatele platebních služeb

12.2.4.10.2.22.6 <address>

Návratová hodnota	Popis
String	Obsahuje plnou adresu poskytovatele platebních služeb

12.2.4.10.2.22.7 <city>

Návratová hodnota	Popis
String	Obsahuje název město z adresy poskytovatele platebních služeb

12.2.4.10.2.22.8 <country>

Návratová hodnota	Popis
String	Obsahuje zkrácený kódový název státu, ze kterého poskytovatel platebních služeb pochází

12.2.4.10.2.22.9 <licences>

12.2.4.10.2.22.10 <licence>

Seznam licencí, které jsou u certifikátu a poskytovatele služeb vedeny jako platné v daném registru. Výstup se liší dle zvolených vstupních kriterií. Pokud je na vstupu konkrétní typ licence, vrací se platné licence daného typu a pro daný stát. Pokud na vstupu není typ licence specifikován, vrací se všechny platné licence pro daný stát.

12.2.4.10.2.22.11 <country>

Návratová hodnota	Popis
String	Obsahuje zkrácený kódový název státu, ve kterém má poskytovatel služeb platnou licenci.

12.2.4.10.2.22.12 <type>

Návratová hodnota	Popis
String	Obsahuje zkrácený typ instituce, jak je specifikována danou národní kompetentní autoritou.

12.2.4.10.2.22.13 <scope>

Návratová hodnota	Popis
String	Obsahuje zkrácený název činnosti (role) pro kterou je poskytovatel služeb licencován Možné hodnoty: PSP_AS - Account servicing (vedení účtu) PSP_PI - Payment initiation (iniciování platby) PSP_AI - Account information (informování o účtu) PSP_IC - Issuing of card-based payment instruments (vydávání karetních platebních prostředků)

12.2.4.10.2.22.14 <validFrom>

Návratová hodnota	Popis
dateTime	Obsahuje datum a čas platnosti licence od

12.2.4.10.2.22.15 <validTo>

Návratová hodnota	Popis
dateTime	Obsahuje datum a čas platnosti licence do

12.2.4.10.2.22.16 </licence>

12.2.4.10.2.22.17 </licences>

12.2.4.10.2.22.18 </record>

12.2.4.10.2.22.19 <psd2>

12.2.4.10.2.22.20 <NCAName>

Návratová hodnota	Popis
String	Celý název národní kompetentní autority, uvedený v anglickém jazyce. Příklad: Central Bank of Ireland

12.2.4.10.2.22.21 <NCAId>

Návratová hodnota	Popis
String	Zkrácený unikátní identifikátor národní kompetentní autority Příklad hodnoty: IE-CBI Formát hodnoty: <zkratka státu>-<zkratka názvu kompetentní autority>

12.2.4.10.2.22.22 <rolesOfPsp>

12.2.4.10.2.22.23 <roleOfPsp name="role name">

Návratová hodnota	Popis

String	Název role, jak je činnost dle normy v certifikátu nazvána. Opakuje se pro každou jednotlivou roli (činnost). Každá `roleOfPsp` obsahuje název a jako hodnotu OID dané role. Příklady hodnot: <roleOfPsp name="PSP_AS">0.4.0.19495.1.1</roleOfPsp> <roleOfPsp name="PSP_PI">0.4.0.19495.1.2</roleOfPsp> <roleOfPsp name="PSP_AI">0.4.0.19495.1.3</roleOfPsp> <roleOfPsp name="PSP_IC">0.4.0.19495.1.4</roleOfPsp>

12.2.4.10.2.22.24 </rolesOfPsp>

12.2.4.10.2.22.25 <organizationIdentifier>

Návratová hodnota	Popis
String	Slouží k identifikaci poskytovatele platebních služeb i národní kompetentní autority. Příklad hodnoty: PSDIE-CBI-C190092 Formát hodnoty se skládá z: tříznakový řetězec “PSD” dvouznakový kód země národní kompetentní autority podle ISO 3166-1 znak pomlčka “-” (0x2D (ASCII), U+002D (UTF-8)) 2-8 znaků identifikátor národní kompetentní autority (A-Z velká písmena, bez mezer či oddělovačů) znak pomlčka “-” (0x2D (ASCII), U+002D (UTF-8)) identifikátor poskytovatele platebních služeb (autorizační číslo specifikované národní kompetentní autoritou. Text je bez znakových omezení)

12.2.4.10.2.22.26 <pspIdentifier>

Návratová hodnota	Popis
String	Samotný identifikátor poskytovatele platebních služeb, podle kterého se organizace vyhledává v registru poskytovatelů platebních služeb. Příklad hodnoty: C190092

12.2.4.10.2.22.27 </psd2>

12.2.4.10.2.23 </psd2Data>

12.2.4.10.3 </certificate>

12.2.4.11 </certificatePath>

12.2.4.12 <revocations>

12.2.4.12.1 <revocation xsi:nil="true">

12.2.4.12.1.1 <uid>

Návratová hodnota	Popis
String	Unikátní identifikátor revokačních informací získaných k ověřovanému certifikátu. Jedná se o SHA 256 otisk daných revokačních dat.

12.2.4.12.1.2 <type>

Návratová hodnota	Popis
String	Typ získaných revokačních dat. Hodnoty: OCSP, CRL

12.2.4.12.1.3 <thisUpdate>

Návratová hodnota	Popis
dateTime	Začátek platnosti (datum a čas vydání) získaných revokačních dat

12.2.4.12.1.4 <nextUpdate>

Návratová hodnota	Popis
dateTime	Datum a čas vydání následujících revokačních dat

12.2.4.12.1.5 <producedAt>

Návratová hodnota	Popis
dateTime	Datum a čas, ve který OCSP respondér podepsal OCSP odpověď

12.2.4.12.1.6 <source>

Návratová hodnota	Popis
String	Indikuje zdroj důvěryhodného úložiště získaných ověřovacích dat. Může nabývat hodnot: SECUSIGN – backendové servery služby SecuSign INTERNAL_STORAGE – lokální úložiště certifikátů na SecuSign SDK serveru zákazníka

12.2.4.12.1.7 </revocations>

12.2.4.12.2 </validationMaterial>

12.2.4.13 </certificateValidationInfo>

12.2.4.14 <StatusMessage>

Návratová hodnota	Popis
String	V případě chyby obsahuje textovou informaci s podrobnostmi o výsledku, např.: Signing certificate expired on Sat May 16 14:02:30 CEST 2015 Certificate has been revoked on Fri Jun 29 13:19:27 CEST 2018 code 9999: cz.software602.sdar.common.SdarException: Cannot find issuer 'ACAeID3.1 - Issuing Certificate' in 'c:\CertificateStore\.. '

12.3 Interpretace výsledku ověření (u non PSD2 certu)

Cílem je určit následující typy certifikátů:

1. Certifikát pro elektronickou pečeť
2. Certifikát pro elektronický podpis uživatele
3. Certifikát pro autentizaci webových služeb (SSL)

Čemuž odpovídají tyto certifikáty:

- Kvalifikovaný certifikát pro elektronickou pečeť (1)
- Kvalifikovaný certifikát pro elektronický podpis (2)
- Komerční certifikát vydaný kvalifikovaným poskytovatelem služeb (3)
- Komerční certifikát ověřený proti lokálnímu truststore (3)

Ty lze z výsledku validace určit následovně:

- Kvalifikovaný certifikát pro elektronickou pečeť (1)
  - certType = QUALIFIED, qualifiedCertType = ESEAL
- Kvalifikovaný certifikát pro elektronický podpis (2)
  - certType = QUALIFIED, qualifiedCertType = ESIGN
- Komerční certifikát vydaný kvalifikovaným poskytovatelem služeb (3)
  - certType = COMMERCIAL
  - certType = QUALIFIED, qualifiedCertType = WEB
- Komerční certifikát ověřený proti lokálnímu truststore (3)
  - certType = INTERNAL_STORAGE

Samozřejmě musí platit, že daný certifikát je VALID.

13 Dešifrování dat pomocí certifikátu

Webová služba umožňuje dešifrovat data (např. z emailu) pomocí vybraného certifikátu z HSM služby Vzdáleného podepisování/pečetění. Tuto metodu využívá Klíčenka602, která je distribuována v rámci aplikace Signer.

13.1 Název metody: Decrypt

Popis služby včetně WSDL schématu a příklad požadavku a odpovědi pro SOAP 1.1 a SOAP 1.2 je umístěn na https://localhost/secusign/default.asmx?op=Decrypt *

* localhost je název používaný pro lokální počítač; namísto něj zvolte jméno/IP adresu SDK serveru (dle nastavení v IIS)

13.1.1 Požadavek v rozhraní SOAP 1.1

```
POST /secusign/default.asmx HTTP/1.1
Host: localhost
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://software602.com/secusign/Decrypt"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <Decrypt xmlns="http://software602.com/secusign/">
      <CertificateID>string</CertificateID>
      <CertificatePIN>string</CertificatePIN>
      <EncryptedData>base64Binary</EncryptedData>
      <Params>string</Params>
    </Decrypt>
  </soap:Body>
</soap:Envelope>
```

13.1.2 Vstupní parametry metody

13.1.2.1 <CertificateID>

[povinný element]

Vstup	Popis
String	Identifikace certifikátu pro dešifrování dat. V případě in-house rozhraní SecuSign SDK je možné použít formát: ■ HStore:[alias] ■ alias certifikátu z HSM modulu služby Vzdáleného podepisování/pečetění.

13.1.2.2 <CertificatePIN>

[povinný element]

Vstup	Popis
String	PIN, který byl zvolen žadatelem jako přístupové heslo k privátní části certifikátu V případě použití `HStore` aliasu je třeba uvést vždy.

13.1.2.3 <EncryptedData>

[povinný element]

Vstup	Popis

String	Base64 zakódovaná data, která byla šifrována pomocí zvoleného certifikátu.

13.1.3 Struktura odpovědi na požadavek

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <DecryptResponse xmlns="http://software602.com/secusign/">
      <DecryptResult>int</DecryptResult>
      <DecryptedData>base64Binary</DecryptedData>
      <StatusMessage>string</StatusMessage>
    </DecryptResponse>
  </soap:Body>
</soap:Envelope>
```

13.1.4 Výstupní parametry metody

13.1.4.1 <DecryptResult>

Návratová hodnota	Popis
int	Výsledek metody Decrypt (dešifrování dat pomocí certifikátu). 0 = v pořádku, jinak Návratové kódy všech metod a chyba popsaná ve StatusMessage.

13.1.4.2 <DecryptedData>

Návratová hodnota	Popis
Base64Binary	Base64 zakódovaná data, která byla dešifrována pomocí zvoleného certifikátu

13.1.4.3 <StatusMessage>

Návratová hodnota	Popis
String	Textová zpráva odpovídající celkovému výsledku získání pečeti/podpisu k hash. Hodnota je naplněna pouze v případě problematického výsledku.

14 Zjištění nainstalované verze SecuSign SDK

Webová služba umožňuje zjistit číselné označení aktuálně nainstalované verze SecuSign SDK a jeho komponent, ověřit funkčnost licenčního certifikátu a zjistit maximální velikost požadavku, který lze na webové službě přijmout (konfigurovatelné v IIS).

14.1 Název metody: GetVersionInfo

Popis služby včetně WSDL schématu a příklad požadavku a odpovědi pro SOAP 1.1 a SOAP 1.2 je umístěn na https://localhost/secusign/default.asmx?op=GetVersionInfo *

* localhost je název používaný pro lokální počítač; namísto něj zvolte jméno/IP adresu SDK serveru (dle nastavení v IIS)

14.1.1 Požadavek v rozhraní SOAP 1.1

```
POST /secusign/default.asmx HTTP/1.1
Host: localhost
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://software602.com/secusign/GetVersionInfo"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <GetVersionInfo xmlns="http://software602.com/secusign/" />
  </soap:Body>
</soap:Envelope>
```

14.1.2 Struktura odpovědi na požadavek

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <GetVersionInfoResponse xmlns="http://software602.com/longtermdocs/">
      <GetVersionInfoResult>string</GetVersionInfoResult>
    </GetVersionInfoResponse>
  </soap:Body>
</soap:Envelope>
```

14.1.3 Výstupní parametry metody

Návratová hodnota	Popis

	Výsledek metody obsahující označení a číslo verze SecuSign, výsledek kontroly licence a maximální velikost požadavku.
`String`	Pokud je v odpovědi chybová zpráva „Certificate file specified by LicCert configuration key/parameter not found !!!“, která informuje o nenalezení licenčního certifikátu v konfiguraci, je potřeba provést nastavení certifikátu dle Instalační příručky.

15 Návratové kódy všech metod

Funkce SecuSign SDK obsahují ve výsledku (Result) návratovou hodnotu v podobě *integer*, která odpovídá jednomu z těchto kódů:

Kód	Název	Popis
Webová služba SecuSign SDK		
0	OK	Success.
1	ERROR	Unknown error. Signing Certificate is expired: NotAfter: Day Month dd HH:mm:ss CEST YYYY There is no signature to timestamp in the document. Signature already contains signature timestamp.
2	METHOD_NOT_ALLOWED	User is not allowed to call this method (e.g. Premium plan or remote sealing required)
3	UNAUTHORIZED.	Error connecting to secusign backend server due to VerifyUser failed to verify basic authentication or licence certificate (used for login to backend service)
4	INTERRUPTED_UNEXPECTEDLY	The operation was unexpectedly interrupted (cause: the transaction log contains the beginning, but the end is missing)
5	INVALID_PARAMETER	Invalid input parameter settings (eg method Validate and output format is not set)
6	INVALID_INPUT	Empty or mismatched content of input file
7	ERROR_ACCESS_SEALING_CERT	Error accessing the sealing certificate
8	NOT_IMPLEMENTED	Function not implemented
9	EXCEPTION	Exception raised during File processing
10	LTV_ANALYZE_ERROR	Error in ltvAnalyze
11	LTV_REGISTER_ERROR	Error in ltvRegister
12	LTV_UPDATE_ERROR	Error in ltvUpdate
13	LTV_UNREGISTER_ERROR	Error in ltvUnregister
14	LTV_GETINFO_ERROR	Error in ltvGetInfo
15	LTV_GETFORUPDATE_ERROR.	Error in ltvGetForUpdate
16	LTV_SIGN_ERROR.	Error in ltvSign
17	LTV_TIMESTAMP_ERROR.	Error in ltvTimestamp
18	DOCUMENT_NOT_SIGNED.	Document does not contain required digital signature or timestamp
19	LTV_UPDATE_ID_NOT_FOUND.	Document with specified ID not found. Document must be registered before update.
20	LTV_UPDATE_HASH_MISMATCH.	Document hash does not correspond to specified ID

21	LTV_UPDATE_FAILED	Unable to extend signature validity. For PDF, 602XMLForm and IDSOC the last signature must be VALID. For other formats, all signatures must be VALID and no one from registered signatures can be missing.
22	LTV_INCONVENIENT_CONDITIONS	Document does not comply with conditions for LTV. All/last/at least one signature must be marked as VALID.
23	DOCUMENT_NOT_REGISTERED	The document with the specified DocID or hash was not registered (no matching record was found)
24	LICENCE_ERROR	Error verifying license / role
Služba Vzdáleného podepisování/pečetění		
0	OK	Success. Úspěšné vytvoření podpisu/pečeti.
16	LTV_SIGN_ERROR	Obecná chyba při podepsání/pečetění dokumentu v SDK, např. z důvodu problému při zápisu do transakčního logu nebo když licenční certifikát není registrován na daném prostředí
101	UNKNOWN	Obecná nebo neznámá chyba vrácená ze služby Vzdáleného podepisování/pečetění, např. z důvodu že pod specifikovaným CertificateID nebyl nalezen certifikát
102	USER_ACCESS_DENIED	Certifikát a klíč se našel, ale zadaný uživatel k němu nemá přístup
103	INVALID_PIN	Certifikát a klíč se našel, uživatel k němu má přístup, ale zadaný PIN neodpovídá
104	CONFIG_ERROR	Chybné nastavení konfigurace, např. není nastaven licenční certifikát pro dešifrování požadavku v metodě SignEx
105	INVALID_PARAMETER	Neplatný parametr metody
106	ACCESS_DENIED	Chyba autentizace klienta ke službě Vzdáleného podepisování, např. z důvodu neplatného přihlašovacího certifikátu nebo ID organizace, přístup zakázán, operace není povolena
107	SEND_CONFIRMATION_FAILED	Chyba při odesílání potvrzovacího emailu
108	CONFIRMATION_TIMEOUT	Došlo k vypršení požadavku při čekání na potvrzení podpisu
109	CERT_NOT_FOUND	Certifikát s daným ID nenalezen
110	CERT_DISABLED	Certifikát má Status DISABLED (byl deaktivován)
111	CERT_REVOKED	Certifikát má Status REVOKED (byl revokován)
112	PKEY_NOT_AVAILABLE	Nenalezen privátní klíč nutný pro podpis
113	SIGNING_FAILED	Selhalo podepsání v rámci SignHash
114	CREATE_CERT_FAILED	Chyba při vytváření certifikátu SignMaster CA
115	SET_CERT_PROP_FAILED	Chyba při nastavení vlastnosti certifikátu
116	IMPORT_FAILED	Chyba při importu X509/P12

117	EXPORT_FAILED	Chyba při exportu certifikátu (platí pro Sofa/FFS)
118	NOT_YET_IMPLEMENTED	Funkce zatím nebyla implementována
119	IMPORT_PASSWORD_INVALID	Při importu bylo chybně zvolené heslo PFX nebo byl vložen poškozený soubor
120	CERTIFICATE_EXPIRED	Zvolený certifikát vypršel. NotAfter=YYYY-MM-DDTHH:mm:ssZ.
Služba Vzdáleného podepisování/pečetění s 602Key		
121	CONFIRMATION_NOT_ACTIVATED	Uživatel nemá aktivované žádné zařízení pro dvoufaktorové potvrzování
123	CONFIRMATION_REJECTED	Uživatel zamítl operaci
124	CONFIRMATION_FAILED	Potvrzování operace selhalo (chyba spojení se vzdáleným serverem 602Key, případně chyba na vzdáleném serveru 602Key apod.)

Každá z funkcí má také v odpovědi *StatusMessage*, kde se vrací textový popis a podrobnosti o chybě.