DSV-SERVER V4.0
РУКОВОДСТВО ПРОГРАММИСТА

Версия документа v1.0

СОДЕРЖАНИЕ

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

- SOAP - Simple Object Access Protocol - простой протокол доступа к объектам. Протокол обмена структурированными сообщениями в распределенной вычислительной среде.
- OCSP - Протокол состояния сетевого сертификата - это интернет-протокол, используемый для получения статуса отзыва цифрового сертификата X.509.

2. ОПИСАНИЕ

DSV-SERVER предназначен для проверки ЭЦП, цепочки сертификатов, статусов сертификатов в документе PKCS#7 и для выполнения других дополнительных функций.

2.1. Технические требования

Для запуска DSV-SERVER потребуется:

- ОС Windows 7/10 (x64) или Linux x64 (предпочтительно)
- JRE 1.8
- CPU - зависит от частоты проверок в сек. (одна проверка ЭЦП может занять одно лог. CPU за 1 сек.)
- RAM - не менее 8Гб, так же зависит от частоты проверок.
- Интернет соединение - для проверки статуса сертификата по протоколу OCSP.

2.2. Состав файлов и их описание

Файл	**Описание**
`dsv-server.jar`	Основной запускаемый модуль
`lib/*.jar`	Необходимые библиотеки
`keys/truststore.jks`	Файл хранит доверенные корневые сертификаты. Должен быть недоступен для изменения неавторизованными лицами.
`run.sh`	Shell-скрипт для запуска DSV-SERVER в ОС Linux
`run.bat`	Shell-скрипт для запуска DSV-SERVER в ОС Windows

3. УСТАНОВКА И ЗАПУСК

Для установки, извлеките файлы из архива в директорию на сервере. Путь и название директорий не должно содержать спец. символов и пробелов.

Откройте консоль, перейдите в директорию где находится файл `dsv-server.jar` и выполните команды:

- На ОС Windows

```
set TSA_URL=http://e-imzo.uz/cams/tst
set TRUSTSTORE_FILE=keys/truststore.jks
set TRUSTSTORE_PASSWORD=12345678

java -Dfile.encoding=UTF-8 -jar dsv-server.jar -p 9090
```

- На ОС Linux

```
export TSA_URL=http://e-imzo.uz/cams/tst
export TRUSTSTORE_FILE=keys/truststore.jks
export TRUSTSTORE_PASSWORD=12345678

java -Dfile.encoding=UTF-8 -jar dsv-server.jar -p 9090
```

приложение будет слушать сокет 127.0.0.1:9090, на экране (лог) напечатает URL SOAP сервиса по которому сторонние приложения могут обмениваться данными.

```
...
May 04, 2016 10:54:55 AM uz.yt.eimzo.dsv.server.Application run
INFO: http://127.0.0.1:9090/dsvs/tsaproxy/v1?wsdl
May 04, 2016 10:54:55 AM uz.yt.eimzo.dsv.server.Application run
INFO: http://127.0.0.1:9090/dsvs/cryptoauth/v1?wsdl
May 04, 2016 10:54:55 AM uz.yt.eimzo.dsv.server.Application run
INFO: http://127.0.0.1:9090/dsvs/pkcs7/v1?wsdl
...
```

SOAP сервис `http://127.0.0.1:9090/dsvs/pkcs7/v1?wsdl` предназначен для выполнению операций с документом PKCS#7.
SOAP сервис `http://127.0.0.1:9090/dsvs/tsaproxy/v1?wsdl` предназначен для выполнению операций с Токеном штампа времени.

Для вывода информации по параметрам, выполните команду:

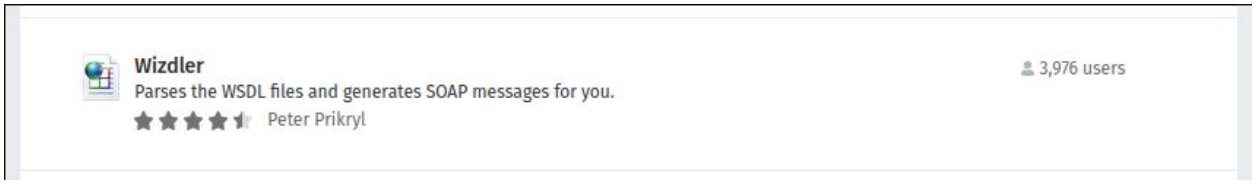
```
java -Dfile.encoding=UTF-8 -jar dsv-server.jar -h
```

Запуск в режиме автозагрузки DSV-SERVER должен быть настроен Администратором.

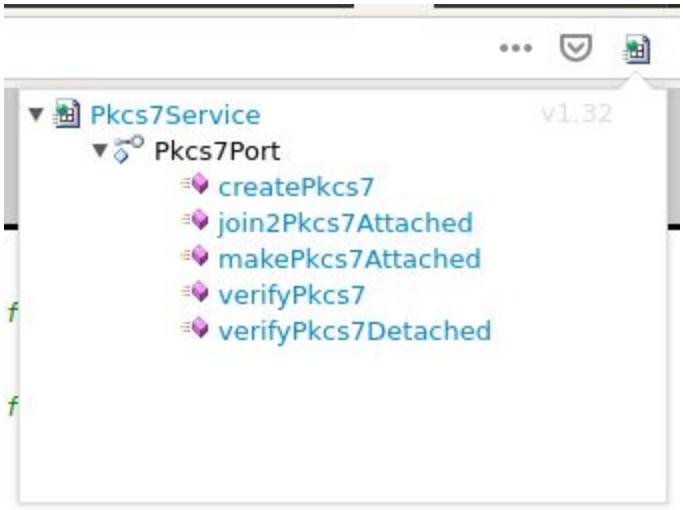
4. ПРОВЕРКА РАБОТЫ СЕРВИСА PKCS7

Для проверки работы сервиса `http://127.0.0.1:9090/dsvs/pkcs7/v1?wsdl` выполните следующие шаги:

1. Запустите DSV-SERVER
2. Откройте браузер Firefox и установите Add-on Wizdler



3. Откройте адрес `http://127.0.0.1:9090/dsvs/pkcs7/v1?wsdl` . В строке адреса появится иконка Wizdler. Нажмите и выберите функцию verifyPkcs7.




```
<Envelope xmlns="http://schemas.xmlsoap.org/soap/envelope/">
    <Body>
        <verifyPkcs7 xmlns="http://v1.pkcs7.plugin.server.dsv.eimzo.yt.uz/">
            <pkcs7B64 xmlns="">[string?]</pkcs7B64>
        </verifyPkcs7>
    </Body>
</Envelope>
```

4. Замените строку `[string?]` на строку текста PKCS#7 в кодировке Base64 (полученную из программы E-IMZO вызовом функции http://127.0.0.1:64646/apidoc.html#pkcs7.create_pkcs7 или на сайте http://dls.yt.uz/certkey-pfx-token-pkcs7.html). Нажмите на кнопку Go.

```
<Envelope xmlns="http://schemas.xmlsoap.org/soap/envelope/">
    <Body>
        <verifyPkcs7 xmlns="http://v1.pkcs7.plugin.server.dsv.eimzo.yt.uz/">
            <pkcs7B64 xmlns="">MIAGCSqGSIb3DQEHAqCAMIACAC5EVUsgWUFOR0.....PAMcewAAAAAAAA==</pkcs7B64>
        </verifyPkcs7>
    </Body>
</Envelope>
```

5. Сервис в ответ вернет JSON-документ с результатом проверки документа PKCS#7.


```
{
  "pkcs7Info":{
        "signers":[
        {
        "signerId":{
        "issuer":"CN=ПЕТРОВ ПЕТР ПЕТРОВИЧ,T=Директор,L=г.Ташкент ул.Абай 4,C=UZ",
        "subjectSerialNumber":"77777777"
        },
        "signingTime":"2016.11.08 07:03:17",
        "signature":"92e1e9a9d48d9bbfb07e28...7599849c6f316cfc799b",
        "digest":"922796f2dbefe6fd71056f527...58eb84ea4bccd34bcef1756f26",
        "certificate":[
        {
                "serialNumber":"77777777",
                "subjectName":"CN=ИВАНОВ
ИВАН,UID=555555555,1.2.860.3.16.1.2=33333333333333,1.2.860.3.16.1.1=333333333",
                "validFrom":"2016.09.29 11:07:41",
                "validTo":"2018.09.29 11:07:40",
                "issuerName":"CN=ПЕТРОВ ПЕТР ПЕТРОВИЧ,T=Директор,C=UZ",
                "publicKey":{
                "keyAlgName":"OZDST-1092-2009-2",
                "publicKey":"MGAwGQYJKoZcAw8BAQIBMAwGCiq...UYRHlgiPqhe0="
                },
                "signature":{
                "signAlgName":"OZDST-1106-2009-2-AwithOZDST-1092-2009-2",
                "signature":"98a8b6e74ce27ed83b7b0e...890de1b6666"
                }
        },
        {
                "serialNumber":"576a5ea5",
                "subjectName":"CN=ПЕТРОВ ПЕТР ПЕТРОВИЧ,L=г.Ташкент ул.Абай
4,E=info@e-imzo.uz,C=UZ",
                "validFrom":"2016.06.22 14:54:15",
                "validTo":"2021.06.22 14:54:15",
                "issuerName":"CN=ERI markazlarini ro'yxatdan o'tkazuvchi organi",
                "publicKey":{
                "keyAlgName":"OZDST-1092-2009-2",
                "publicKey":"MGAwGQYJKoZcAw8BAQIBMAwGCiq...BdEhSaqM3gI="
                },
                "signature":{
                "signAlgName":"OZDST-1106-2009-2-AwithOZDST-1092-2009-2",
                "signature":"1a2047a8abd96ffaf2e23242a21...29ccd535c"
                }
        }
        ],
        "OCSPResponse":"MIILo...j8to0",
        "statusUpdatedAt":"2019.03.19 11:45:43",
        "statusNextUpdateAt":"2019.03.19 11:46:43",
        "verified":true,
        "certificateVerified":true,
        "trustedCertificate":{
        "serialNumber":"575a613a",
        "subjectName":"CN=ERI markazlarini ro'yxatdan o'tkazuvchi organi",
        "validFrom":"2016.06.10 11:49:30",
        "validTo":"2036.06.10 11:49:30",
```

```
        "issuerName":"CN=ERI markazlarini ro'yxatdan o'tkazuvchi organi",
        "publicKey":{
                "keyAlgName":"OZDST-1092-2009-2",
                "publicKey":"MGAwGQYJKoZcAw8BAQIBMAwGCiq...wKeJ3lmYVT7I="
        },
        "signature":{
                "signAlgName":"OZDST-1106-2009-2-AwithOZDST-1092-2009-2",
                "signature":"5f5212c6e65993c963204b31ee...7df6c864d"
        }
        },
        "policyIdentifiers":[
        "1.2.860.3.2.2.1.2.4",
        "1.2.860.3.2.2.1.2.3",
        "1.2.860.3.2.2.1.2.1",
        "1.2.860.3.2.2.1.2.2"
        ],
        "certificateValidAtSigningTime":true,
        "revokedStatusInfo":{
        "revocationTime":"2021.02.26 16:29:46",
        "crlReason":"CRLReason: certificateHold"
        },
        "exception":"...."
        }
        ],
        "documentBase64":"PD94....Q+DQo="
  },
  "success":true,
  "reason":"some error..."
}
```


Поле	**Описание**
`success`	успешность операции (если `true` проверьте следующие поля, если `false` проверьте поле `reason`)
`pkcs7Info.documentBase64`	подписанный документ в кодировке (Base64)
`pkcs7Info.signers[N]`	информация о том кто подписал документ
`pkcs7Info.signers[N].certificate[0]`	информация о сертификате пользователя
`pkcs7Info.signers[N].certificate[1]`	информация о сертификате ЦРК
`pkcs7Info.signers[N].certificate[2]`	информация о корневом сертификате (если имеется)
`pkcs7Info.signers[N].OCSPResponse`	OCSP ответ от сервера ЦРК
`pkcs7Info.signers[N].signingTime`	дата на компьютере пользователя при подписании (при получении сервером подписанного документа следует сверить это поле с реальным временем если PKCS#7 документ не содержит токен штампа времени) ** токен штампа времени - содержит ЭЦП*

	документа и точную дату и время подписи, выдается сервером Доверительной третьей стороны в виде подписанного электронной цифровой подписью документа, которая подтверждает что ЭЦП документа была создана в определенный момент времени.
`pkcs7Info.signers[N].verified`	ЭЦП действительна (если `true` - да, если `false` нет)
`pkcs7Info.signers[N].certificateVerified`	цепочка сертификатов действительна (если `true` - да, если `false` нет)
`pkcs7Info.signers[N].revokedStatusInfo`	Если сертификат пользователя был приостановлен или отозван, то поле содержит дату и причину.
`pkcs7Info.signers[N].certificateValidAtSigningTime`	сертификат действителен на дату подписи (если `true` - да, если `false` нет). За дату подписи берется поле `pkcs7Info.signers[N].signingTime` или дата и время токена штампа времени (если присутствует)
`pkcs7Info.signers[N].exception`	ошибка при проверке подписи (причина ошибки при проверке подписи или статуса сертификата, возможная причина: не установлен `vpn-client` или срок vpn-ключа истек)
`UID`	Физ.ИНН.
`1.2.860.3.16.1.2`	ПИНФЛ
`1.2.860.3.16.1.1`	Юр.ИНН (поле отсутствует если субъект является физ. лицом)

ЭЦП документа считается действительной если поля `success, verified, certificateVerified, certificateValidAtSigningTime` равно `true`, поле `exception` отсутствует (или равно `null`), а также (если `pkcs7Info.signers[N]` не содержит токен штампа времени) `signingTime` приблизительно равно времени проверки PKCS#7 документа сервером. Если `pkcs7Info.signers[N]` содержит токен штампа времени, то проверка `signingTime` не обязательна.

Если поле `certificateValidAtSigningTime` равно `false` и поле `exception` равно тексту ошибки, то возможно `vpn-client` не работает или срок vpn-ключа истек.