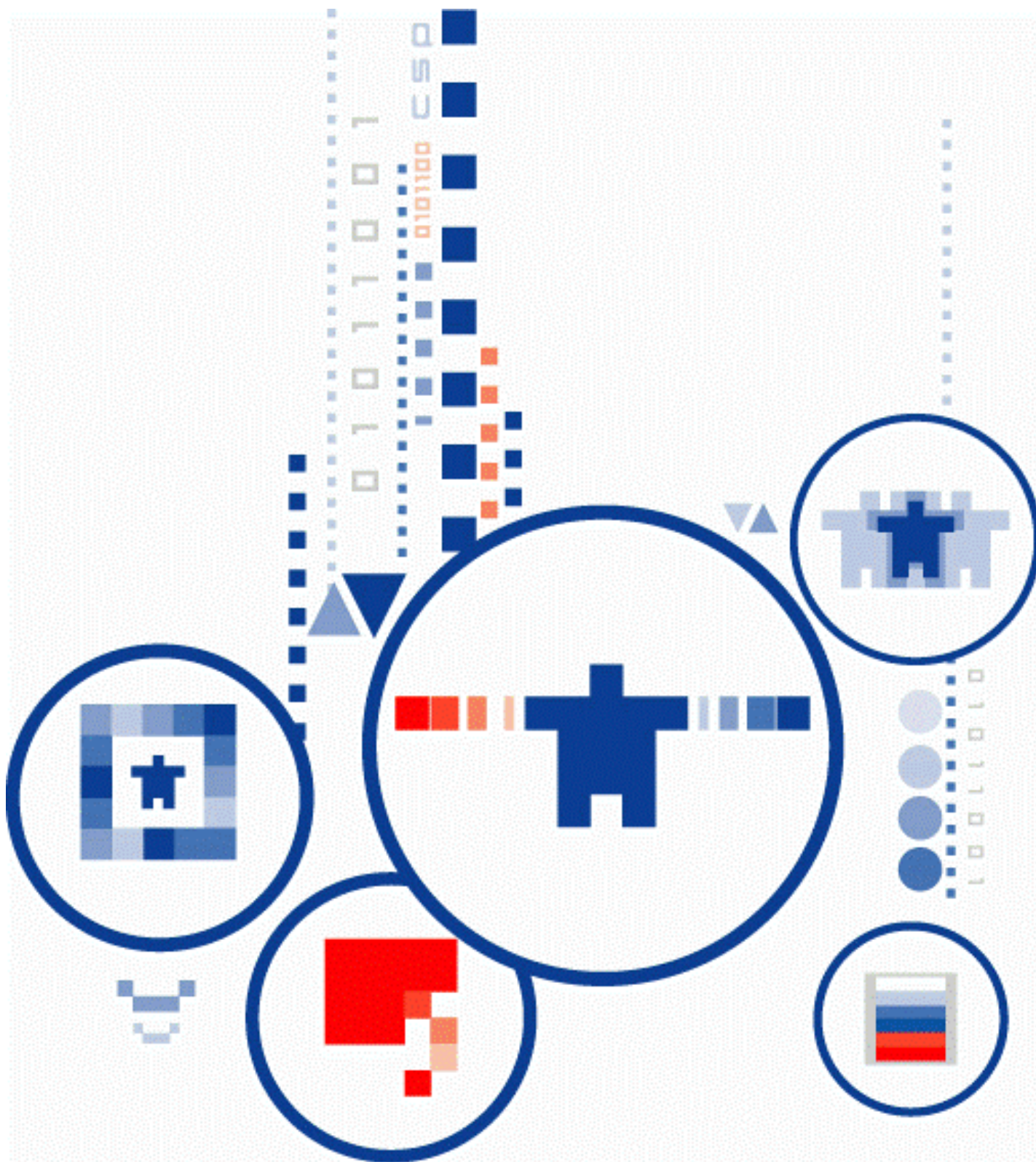




**Служба проверки электронной подписи и
сертификатов**

"КриптоПро SVS"

Руководство Администратора

Содержание

КриптоПро SVS. Руководство Администратора

Аннотация

Развертывание SVS

Системные требования

Установка и удаление SVS

Пример развертывания SVS в ОС *nix

Пример развертывания SVS в ОС Windows

Настройка SVS

Экземпляр SVS

Администрирование SVS

Установка корневых сертификатов и CRL

Получение актуального статуса сертификата

Отображение документов

Ограничение размера документов

Передача данных по безопасному соединению

Настройка проверки принадлежности УЦ к определенному списку

Проверка формата сертификата

XML-преобразования

Пакетная проверка подписи

Диагностика SVS

Журналы Windows

Диагностика ошибок при проверке CAdES-подписи

Журналирование сетевых взаимодействий

Командлеты администрирования

Add-VsCertificateVerifierPlugin

Add-VsConverterPlugin

Add-VsQualifiedCAThumbprints

Add-VsTransformPlugin

Disable-VsEndpoint

Disable-VsTracing

Enable-VsEndpoint

Enable-VsTracing

Get-VsCertificateVerifierPlugin

Get-VsConverterPlugin
Get-VsCustomization
Get-VsEndpoint
Get-VsEndpointGlobalSettings
Get-VsInstance
Get-VsLicense
Get-VsProperties
Get-VsQualifiedCAThumbprints
Get-VsSignatureFormat
Get-VsTracing
Get-VsTransformPlugin
New-VsInstance/Add-VsInstance
New-VsLicense
Remove-VsCertificateVerifierPlugin
Remove-VsConverterPlugin
Remove-VsInstance
Remove-VsQualifiedCAThumbprints
Remove-VsTransformPlugin
Reset-VsCustomization
Restart-VsInstance
Set-VsCertificateVerifierPlugin
Set-VsConverterPlugin
Set-VsCustomization
Set-VsEndpointGlobalSettings
Set-VsProperties
Set-VsSignatureFormat
Set-VsTracing
Update-VsInstance
Update-VsLicense
Add-VsFeInstance
Get-VsFeProperties
Remove-VsFeInstance
Set-VsFeProperties

Руководство Администратора КриптоПро SVS

Настоящий документ содержит описание процесса установки и конфигурирования службы проверки сертификатов и электронной подписи «КриптоПро SVS» (Signature Verification Service, далее - КриптоПро SVS), предназначенной для установления статуса сертификата ключа проверки электронной подписи и выполнения процедуры подтверждения подлинности электронных подписей документов различного формата.

КриптоПро SVS входит в состав [программно-аппаратного комплекса \(ПАК\) «Службы УЦ» версии 2.0.](#)

Документ предназначен для администраторов как руководство по установке и конфигурированию КриптоПро SVS.

В этом документе:

- [Развертывание SVS](#)
- [Настройка SVS](#)
- [Диагностика SVS](#)

Развертывание КриптоПро SVS

Развертывание «КриптоПро SVS» осуществляется в следующем порядке:

1. [Установка и настройка веб-сервера.](#)
 2. Установка Microsoft .NET Framework версии 4.8 (только для ОС Windows Server). Скачать Microsoft .NET Framework 4.8 можно по адресу <https://go.microsoft.com/fwlink/?linkid=2088631>. Соответствующий установочный файл находится на дистрибутивном диске.
 3. Установка КриптоПро .NET (только для ОС Windows Server). Актуальные версии и документация могут быть загружены с [официального сайта](#).
 4. Установка Windows PowerShell. Соответствующий установочный файл находится на дистрибутивном диске.
 5. Установка КриптоПро CSP. Выполняется согласно эксплуатационной документации. Актуальные версии и документация могут быть загружены с [официального сайта](#).
 6. [Установка КриптоПро SVS.](#)
 7. [Настройка КриптоПро SVS.](#)
- [Пример развертывания КриптоПро SVS для ОС Windows](#)
 - [Пример развертывания КриптоПро SVS для ОС на базе *nix](#)

Примечание

Во время выполнения установки КриптоПро SVS в ОС Windows автоматически будут установлены **КриптоПро TSP Client** и **КриптоПро OCSP Client**. При установке КриптоПро SVS в *nix-системах данные компоненты устанавливаются при установке пакетов CAAdES (см. [пример](#)).

Данные компоненты необходимы для проверки электронных подписей форматов *AdES и получения актуальных статусов сертификатов.

Системные требования

Требования к аппаратному обеспечению

Минимальные требования к аппаратному обеспечению представлены в таблице ниже.

ОБОРУДОВАНИЕ	ТРЕБОВАНИЯ
Центральный процессор	64-разрядный двухъядерный процессор с тактовой частотой 1,86 ГГц
Оперативная память	4 ГБ ОЗУ
Жесткий диск	4 ГБ свободного места
Сетевые адаптеры	Один сетевой адаптер, совместимый с операционной системой компьютера, для взаимодействия с внутренней сетью

Требования к программному обеспечению

Служба проверки сертификатов и электронной подписи КриптоПро SVS предназначена для функционирования в следующих операционных системах (ОС):

- Microsoft Windows Server 2008 R2 с установленным пакетом обновления Service Pack 1 и выше,
- Windows Server 2012,
- Windows Server 2012 R2,
- Microsoft Windows Server 2016,
- Microsoft Windows Server 2019 (только для уровня защиты KC2),
- операционная система специального назначения «Astra Linux Special Edition» (ОС CH «Astra Linux Special Edition»).

В качестве криптопровайдера может быть использовано СКЗИ «КриптоПро CSP» версии 4.0 варианта исполнения 2-Base, 3-Base и выше.

При использовании ОС Microsoft Windows 2008 R2 необходимо наличие установленного Internet Explorer версии не ниже 9.

Требования к веб-серверу

Требования к веб-серверу для ОС Microsoft Windows 2008 R2

Для настройки работы веб-сервера необходимо установить Microsoft Internet Information Services 7.5. В Мастере добавления ролей и компонентов необходимо добавить следующие роли веб-сервера IIS:

- ASP.NET;
- Расширяемость .NET (.NET Extensibility 4.5);
- Расширения ISAPI (ISAPI Extensions);
- Фильтры ISAPI (ISAPI Filters);
- Статическое содержимое (Static content);
- Фильтрация запросов (Request Filtering);
- Консоль управления IIS (IIS Management Console).

Примечание

Если установка Microsoft .NET Framework 4.6.1 происходила до установки роли IIS, то после добавления данной роли необходимо в командной строке выполнить команду (в одну строку):

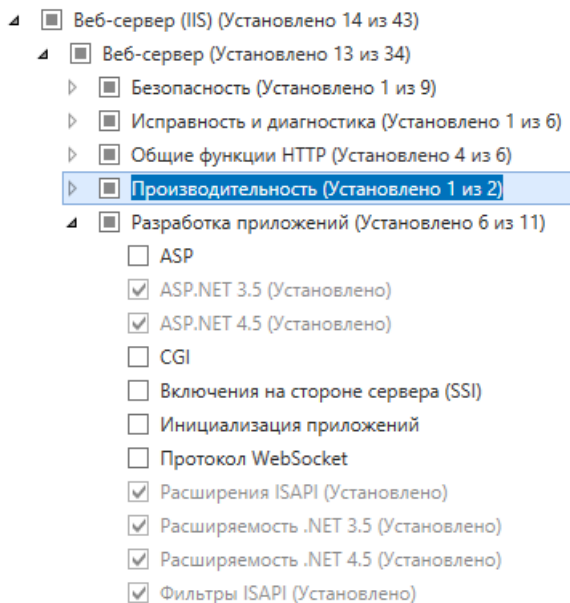
`%windir%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe iur`

Требования к веб-серверу для ОС Microsoft Windows 2012 и 2012 R2

Для настройки работы веб-сервера необходима установка Microsoft Internet Information Services (IIS) 8. В Мастере добавления ролей и компонентов необходимо добавить следующие роли веб-сервера IIS:

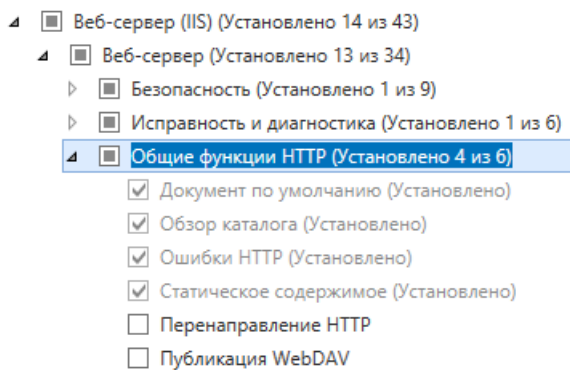
- ASP.NET 4.5;
- Расширяемость .NET (.NET Extensibility 4.5);
- Расширения ISAPI (ISAPI Extensions);
- Фильтры ISAPI (ISAPI Filters);

Указанные роли находятся в разделе «Веб-сервер (IIS) – Веб-сервер – Разработка приложений».



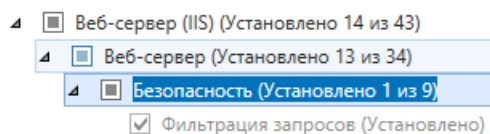
- Статическое содержимое (Static content);

Указанная роль находится в разделе «Веб-сервер (IIS) – Веб-сервер – Общие функции HTTP».



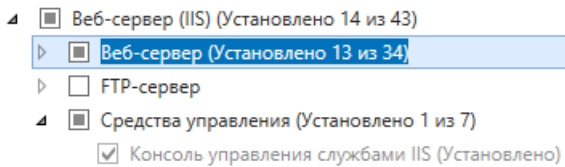
- Фильтрация запросов (Request Filtering);

Указанная роль находится в разделе «Веб-сервер (IIS) – Веб-сервер – Безопасность».



- Консоль управления службами IIS (IIS Management Console).

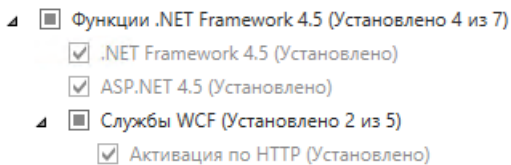
Указанная роль находится в разделе «Веб-сервер (IIS) – Средства управления – Консоль управления службами IIS».



Также необходимо выбрать и установить следующие компоненты IIS: Дополнительные службы .NET Framework 4.5:

- Активация по HTTP (HTTP Activation).

Указанный компонент находится в разделе «Компоненты - Функции .NET Framework 4.5 – Службы WCF – Активация по HTTP».



Установить необходимые компоненты можно как через Диспетчер Сервера, так и с помощью командной строки. Для установки указанных выше компонентов сервера выполните следующую команду:

```
dism.exe /Online /Enable-Feature /FeatureName:IIS-WebServerRole /FeatureName:IIS-WebServer /FeatureName:IIS-ASPNET45 /FeatureName:IIS-NetFxExtensibility45 /FeatureName:IIS-ISAPIExtensions /FeatureName:IIS-ISAPIFilter /FeatureName:IIS-StaticContent /FeatureName:IIS-ManagementConsole /FeatureName:IIS-RequestFiltering /FeatureName:WAS-WindowsActivationService /FeatureName:WCF-HTTP-Activation45 /FeatureName:IIS-NetFxExtensibility45 /FeatureName:NetFx4Extended-ASPNET45 /FeatureName:WAS-ConfigurationAPI
```

Требования к веб-серверу для ОС Microsoft Windows 2016/2019

Для настройки работы веб-сервера необходимо установить Microsoft Internet Information Services 10. В Мастере добавления ролей и компонентов необходимо добавить следующее:

Компоненты

- Служба активации процессов Windows:
 - Модель процесса;
 - API конфигурации;
- Функции .NET Framework 4.6:
 - .NET Framework 4.6
 - ASP.NET 4.6
- Службы WCF:
 - Активация по HTTP
- Платформа .NET 3.5.

Службы ролей

- Ведение журнала;
- Расширяемость .NET (.NET Extensibility 4.5);
- Расширения ISAPI (ISAPI Extensions);
- Фильтры ISAPI (ISAPI Filters);
- Статическое содержимое (Static content);
- Фильтрация запросов (Request Filtering);
- Консоль управления IIS (IIS Management Console).

Установить необходимые компоненты можно как через Диспетчер Сервера, так и с помощью командной строки. Для установки указанных выше компонентов сервера выполните следующую команду:

```
dism.exe /Online /Enable-Feature /FeatureName:IIS-WebServerRole /FeatureName:IIS-WebServer /FeatureName:IIS-ASPNET45 /FeatureName:IIS-NetFxExtensibility45 /FeatureName:IIS-ISAPIExtensions /FeatureName:IIS-ISAPIFilter /FeatureName:IIS-StaticContent /FeatureName:IIS-ManagementConsole /FeatureName:IIS-RequestFiltering /FeatureName:WAS-WindowsActivationService /FeatureName:WCF-HTTP-Activation45 /FeatureName:IIS-NetFxExtensibility45 /FeatureName:NetFx4Extended-ASPNET45 /FeatureName:WAS-ConfigurationAPI
```

Требования к веб-серверу для ОС CH Astra Linux Special Edition

КриптоПро SVS при эксплуатации в ОС CH Astra Linux Special Edition поддерживает следующие веб-серверы:

- nginx,
- apache.

Настройка веб-серверов выполняется согласно эксплуатационной документации к используемой версии КриптоПро CSP (см. документ "Руководство администратора безопасности. Linux" из соответствующего комплекта документации).

Пример настройки веб-сервера nginx

Установка дополнительных пакетов:

```
sudo apt-get install build-essential patch
```

Применение модуля СКЗИ для nginx:

```
wget https://nginx.org/download/nginx-1.18.0.tar.gz
tar -xvf ./nginx-1.18.0.tar.gz
cp ./ng-nginx.1.18.0.patch ./nginx-1.18.0 && cd ./nginx-1.18.0/
patch -p1 < ./ng-nginx.1.18.0.patch
```

Получение дополнительных исходных текстов:

```
wget https://ftp.pcre.org/pub/pcre/pcre-8.44.tar.gz
tar -xvf ./pcre-8.44.tar.gz && cd ./pcre-8.44
wget https://zlib.net/zlib-1.2.11.tar.gz
tar -xvf ./zlib-1.2.11.tar.gz
wget https://www.openssl.org/source/openssl-1.1.1h.tar.gz
tar -xvf ./openssl-1.1.1h.tar.gz
```

Сборка:

```
cd ./nginx-1.18.0
./configure \
--user=nginx \
--group=nginx \
--with-cc-opt='-fstack-protector -fstack-protector-strong --param=ssp-buffer-size=4 -Wformat -Werror=format-
security -Werror=implicit-function-declaration -Winit-self -Wp,-D_FORTIFY_SOURCE=2 -fPIC' \
--with-ld-opt='-Wl,-z,relro -Wl,-z,now -Wl,--as-needed -pie -L/opt/cprosp/lib/amd64 -lrdsup -lssp -lcapi10
-lcapi20' \
--prefix=/opt/nginx \
--conf-path=/etc/nginx/nginx.conf \
--error-log-path=/var/log/nginx/error.log \
--http-log-path=/var/log/nginx/access.log \
--lock-path=/var/run/lock/nginx.lock \
--pid-path=/var/run/nginx.pid \
--with-pcre=/home/test/src/pcre-8.44/ \
--with-pcre-jit \
--with-zlib=/home/test/src/zlib-1.2.11/ \
--with-http_ssl_module \
--with-http_ssfi_module \
--with-http_stub_status_module \
--with-openssl=/home/test/src/openssl-1.1.1h/ \
--with-openssl-opt='no-gost no-comp no-dtls no-deprecated no-dynamic-engine no-engine no-hw-padlock no-
nextprotoneg no-psk no-tests no-ts no-ui-console' \
--with-stream \
--with-stream_ssl_module \
--with-stream_ssfi_module \
--with-http_v2_module
```

Запуск сборки:

```
make
```

Копирование базовой конфигурации (пример конфигурации приведён в 4.1.2):

```
sudo cp ./nginx.conf.sample ./nginx-1.18.0/conf/nginx.conf
sudo make install
```

Создание системного пользователя:

```
sudo adduser --system --no-create-home --group nginx
sudo chown -R nginx:nginx /var/log/nginx/
```

Копирование init-скрипта:

```
sudo cp ./nginx.init /etc/init.d/nginx
```

Установка, удаление и обновление КриптоПро SVS

ОС Windows

Установка

Для установки компонентов Сервиса Проверки Подписи (КриптоПро SVS) запустите установку пакета `SVSInstall.exe`, расположенного на компакт-диске. Установка КриптоПро SVS должна осуществляться от имени пользователя с правами администратора. После коротких подготовительных процедур на экране появится окно мастера установки. Нажмите "Установить".

В следующем окне мастера установки ознакомьтесь с лицензионным соглашением на использование КриптоПро SVS. Если Вы согласны со всеми пунктами соглашения, выделите пункт "Я принимаю условия этого соглашения", и нажмите "Далее".

На следующем шаге мастера следует указать директорию, в которую будут установлены выбранные компоненты. Введите путь установки вручную или воспользуйтесь диалогом выбора папки, для открытия которого следует нажать на кнопку "Обзор".

На следующем шаге убедитесь, что параметры установки заданы верно, и нажмите кнопку "Установить".

После выполнения всех описанных шагов мастер установит КриптоПро SVS, сопровождая действия комментариями. По окончании установки мастер покажет окно с подтверждением успешной установки, в котором необходимо нажать кнопку "Готово". После завершения установки требуется перезагрузить компьютер.

Удаление

Для удаления КриптоПро SVS запустите установку пакета `SVSInstall.exe`, расположенного на компакт-диске, или запустите установщик на удаление из раздела Программы и Компоненты на Панели управления. Удаление КриптоПро SVS должно осуществляться от имени пользователя с правами администратора.

На следующей странице мастера будет выполнено удаление развернутых экземпляров служб установленных компонентов. Для продолжения нажмите кнопку "Удалить". После завершения удаления экземпляров служб нажмите кнопку "Далее".

Примечание

При удалении экземпляра Сервиса Проверки Подписи будут удалены хранилища сертификатов, созданные при разворачивании экземпляра.

После выполнения всех описанных шагов мастер удалит КриптоПро SVS, сопровождая действия комментариями. По окончании удаления мастер покажет окно с подтверждением успешного удаления, в котором необходимо нажать кнопку "Готово".

Обновление

Для обновления КриптоПро SVS запустите установку пакета `SVSInstall.exe`, расположенного на компакт-диске. После подготовительных процедур отобразится страница с информацией об обновлении. Для продолжения нажмите кнопку Обновить. После обновления файлов Сервиса Проверки Подписи отобразится страница с обновлением развернутых экземпляров сервиса. Для продолжения установки нажмите кнопку "Обновить".

ОС Astra Linux SE

Установка КриптоПро SVS в ОС Astra Linux SE представляет собой установку соответствующих пакетов, полученных в комплекте дистрибутивного диска.

Примеры команд приведены в общем [примере разворачивания и настройки КриптоПро SVS](#).

Пример развертывания КриптоПро SVS в *nix-системах

В данном разделе приведен пример развертывания КриптоПро SVS в *nix-системах. Пример позволяет установить и настроить минимально необходимые для обеспечения работоспособности компоненты. Полная информация о настройке и возможностях КриптоПро SVS приведена в разделе "[Настройка КриптоПро SVS](#)".

Используемые архивы и пакеты находятся на дистрибутивном диске КриптоПро SVS. КриптоПро SVS будет установлен в директорию `/opt/cprosvs/vssrv`.

Примечание

Команды bash, приведенные ниже, подразумевают выполнение из папки, куда было скопировано содержимое дистрибутивного диска с КриптоПро SVS и дополнительным ПО (например `/var/temp`).

#Установка КриптоПро CSP:

#Распаковка архива

```
sudo tar -xvf linux-amd64_deb.tgz
```

#Установка

#Внимание! Требуется лицензия на КриптоПро CSP для TLS-сервера

#Дополнительная информация содержится в эксплуатационной документации на КриптоПро CSP

```
sudo chmod u+x linux-amd64_deb/install.sh
```

```
sudo linux-amd64_deb/install.sh
```

#Дополнительный пакет для поддержки ГОСТ в nginx

```
sudo dpkg -i linux-amd64_deb/lsb-cprosp-devel_5.0.12001-6_all.deb
```

#Установка CAdeS:

#Распаковка архива

```
sudo mkdir cades-linux-amd64
```

```
sudo tar -xvf cades-linux-amd64.tar.gz -C cades-linux-amd64
```

#Установка

#Дополнительная информация содержится в эксплуатационной документации

```
sudo dpkg -i cades-linux-amd64/cprosp-pki-cades-64_2.0.14606-1_amd64.deb
```

#Установка NGINX (офлайн-версия КриптоПро):

Создать пользователя nginx

```
sudo adduser --system --no-create-home --group nginx
```

Установка nginx с дистрибутивного диска

```
sudo dpkg -i nginx_1.18.0~astra-gost_amd64_signed.deb
```

Установка nginx с нуля (если не был собран на дистрибутивном диске)

Распаковка архива nginx.tar.gz

```
# sudo tar -xvf nginx.tar.gz
```

#Выполнить gostnginx.sh

```
#sudo chmod u+x nginx/gostnginx.sh
```

```
#sudo nginx/gostnginx.sh
```

#Выполнить перезагрузку nginx:

```
#sudo service nginx restart
```

```
#Установка сертификата веб-сервера
$ sudo -u nginx /opt/cproscsp/bin/amd64/certmgr -install -file <certificate.pfx> -pfx -pin <pfx_pin> -store umy
# где <certificate.pfx> - имя PFX-файла с сертификатом,
# <pfx_pin> - пароль от PFX-файла.

# Установка корневого сертификата для сертификата веб-сервера
sudo -u nginx /opt/cproscsp/bin/amd64/certmgr -install -file <root.cer> -store uroot

# Установка промежуточного сертификата для сертификата веб-сервера
sudo -u nginx /opt/cproscsp/bin/amd64/certmgr -install -file <ca.cer> -store uca

# Получение серийного номера сертификата веб-сервера
$ sudo -u nginx /opt/cproscsp/bin/amd64/certmgr -list -store umy

# В конфигурационный файл Nginx(/etc/nginx/nginx.conf), в контекст server, отвечающий за взаимодействие
# по https, необходимо добавить серийный номер сертификата веб-сервера и ввести его в поле
# ssl_certificate:
sudo nano /etc/nginx/nginx.conf

Пример:

    ssl_certificate /etc/nginx/ssl/nginx.crt;
    ssl_certificate_key /etc/nginx/ssl/nginx.key;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_verify_client on;
    ssl_client_certificate /etc/nginx/ssl/root.crt; # Which store to search the root certificate in

Перезапуск nginx
$ sudo systemctl restart nginx
```

```
#Установка Powershell:
sudo dpkg -i powershell_7.2.4-1.deb_amd64.deb

#Альтернативный вариант (при необходимости изменить версию входящего в дистрибутивный комплект PowerShell)
#Установка пакета curl:
sudo apt install curl
#Импорт ключей GPG публичного репозитория Microsoft:
curl https://packages.microsoft.com/keys/microsoft.asc | sudo apt-key add -
#Подключение репозитория Microsoft:
echo "deb [arch=amd64] https://packages.microsoft.com/repos/microsoft-debian-stretch-prod stretch main" | sudo
tee /etc/apt/sources.list.d/microsoft.list
#Обновление списка пакетов:
sudo apt update
#Установка пакетов PowerShell
sudo apt install powershell
```

```
#Установка КриптоПро SVS:

sudo dpkg -i cprosvs-base_1.0.318-prerelease-1_amd64.deb
sudo dpkg -i cprosvs-fe_1.0.318-prerelease-1_amd64.deb

#Создание учетной записи, под которой будет запускаться Служба
sudo adduser --quiet --system --no-create-home <accountName>
sudo usermod -a -G vssrv <accountName>
```

```
Настройка КриптоПро SVS:

sudo pwsh
#Импорт PowerShell-модулей
#Модуль Сервиса Проверки Подписи
Import-Module
```

```

/opt/cprosvs/powershell/Modules/CryptoPro.VerificationService.PowerShell/CryptoPro.VerificationService.PowerShell.psd1
#Модуль веб-интерфейса Сервиса Проверки Подписи
Import-Module
/opt/cprosvs/powershell/Modules/CryptoPro.VerificationService.Frontend.PowerShell/CryptoPro.VerificationService.Frontend.PowerShell.psd1

#Создание экземпляра SVS
Add-VsInstance -ApplicationName %instanceName% -ListenPort %port% -DisplayName %instanceName% -ServiceAccountName %accountName%
#Пример:
#Add-VsInstance -ApplicationName vs -ListenPort 8080 -DisplayName vs -ServiceAccountName user1

#Ввод временной лицензии на SVS
New-VsLicense

# Добавление плагинов преобразования документов
Add-VsConverterPlugin -FileExtension pdf -Assembly CryptoPro.Plugins.DocumentConverter.PdfStub.dll
Add-VsConverterPlugin -FileExtension doc -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension dot -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension docm -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension dotm -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension docx -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension dotx -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension FlatOpc -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension FlatOpcMacroEnabled -Assembly
CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension FlatOpcTemplate -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension FlatOpcTemplateMacroEnabled -Assembly
CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension xml -Assembly CryptoPro.Plugins.DocumentConverter.Xml.dll -Parameters @{
"encoding"="UTF-8" }
Add-VsConverterPlugin -FileExtension odt -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension ott -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension ooxml -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension WordML -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension rtf -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension html -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension xhtml -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension mhtml -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension txt -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll

#Выйти из PS
exit

# Донастройка Nginx:

# В конфигурационный файл Nginx(/etc/nginx/nginx.conf), в контекст server секцию, отвечающий за взаимодействие на
# 443 порту (https), необходимо добавить:
sudo nano /etc/nginx/nginx.conf
include /etc/opt/cprosvs/vssrv/%instanceName%/nginx.conf

Пример конфигурации:

worker_processes 1;
error_log /var/log/nginx/error.log;
pid /var/run/nginx.pid;
worker_rlimit_nofile 8192;
events {
    worker_connections 4096;
}

```

```
,
http {
    log_format main '$remote_addr - $remote_user [$time_local] $status '
        '$request' $body_bytes_sent "$http_referer" '
        "$http_user_agent" "$http_x_forwarded_for";
    access_log /var/log/nginx/access.log main;
    server {
        listen 443;
        include mime.types;
        server_name astrarakort;
        include /etc/opt/cprosvs/vssrv/svs_appname/nginx.conf;
        # include /etc/opt/cprosvs/vsfe/fe_appname/nginx.conf;
        ssl on;
        ssl_certificate 0x01CCA90B0169AE098C4F5AEEB275FA6CAB; # GOST Serial, необходимо ставить первым в
        список
        # ssl_certificate 0x00E3CD25AA5310D07F; # RSA cert serial (опционально, необходимо при использовании
        GOST+RSA На одном порту)
        ssl_protocols TLSv1.2;
    }
}
```

#Установка сертификатов, используемых при построении и проверке цепочки сертификатов подписи:

Установка корневых сертификатов в хранилище mroot:

```
sudo /opt/cprocsp/bin/amd64/certmgr -install -store mroot -file /path_to/root.cer
```

В хранилище m<svs_appname>-root:

```
sudo /opt/cprocsp/bin/amd64/certmgr -install -store mverify-root -file /path_to/root.cer
```

Установка промежуточных сертификатов в хранилище m<svs_appname>-ca:

```
sudo /opt/cprocsp/bin/amd64/certmgr -install -store mverify-ca -file /path_to/ca.cer
```

Установка CRL в хранилище m<svs_appname>-ca:

```
sudo /opt/cprocsp/bin/amd64/certmgr -install -crl -store mverify-ca -file /path_to/ca.crl
```

Перезапуск nginx

```
sudo systemctl restart nginx.service
```

Проверка работоспособности nginx

```
sudo systemctl status nginx.service
```

#Перезапуск демонов

```
sudo systemctl daemon-reload
```

#Запуск сервиса SVS

```
sudo systemctl start cprosvs-vssrv-%intanceName%.service
```

#Проверка статуса службы SVS

```
sudo systemctl status cprosvs-vssrv-%intanceName%.service
```

#Просмотр журнала работы службы

```
sudo tail -f /var/log/syslog
```

```

#Настройка Веб-интерфейса КриптоПро SVS:

#Установка Веб-интерфейса КриптоПро SVS (если не была выполнена ранее)
sudo dpkg -i cprosvs-fe_1.0.318-prerelease-1_amd64.deb

sudo pwsh
Import-Module
/opt/cprosvs/powershell/Modules/CryptoPro.VerificationService.Frontend.PowerShell/CryptoPro.VerificationService.Frontend.PowerShell.psd1

#Создание экземпляра Веб-интерфейса КриптоПро SVS:
Add-VsFeInstance -DisplayName %instanceName% -ApplicationName %instanceName%
# Пример: Add-VsFeInstance -DisplayName verify -ApplicationName verify

#Настройка экземпляра Веб-интерфейса КриптоПро SVS:
#VSAppName - имя веб-приложения Сервиса Проверки Подписи (не Веб-Интерфейса Сервиса Проверки Подписи)
Set-VsFeProperties -DisplayName {{VsFeAppName}} -BaseUrl "https://{{hostName}}/{{VsAppName}}/rest/api" -
SubPath /{{VsFeAppName}}/
# Пример: Set-VsFeProperties -DisplayName verify -BaseUrl "https://astrarakort/vs/rest/api" -SubPath
/verify/

# Настройка allowedCorsOrigins (если компоненты развернуты на разных серверах)
# Список допустимых источников запросов (адресов, конечных точек и т.д.) к API SVS для протокола CORS
(возможно указание нескольких имен через запятую).
# Например, имя машины, на которой развернут Веб-интерфейс SVS (Переменная server_name из контекста server,
соответствующего Веб-интерфейсу SVS, файла конфигурации /etc/nginx/nginx.conf)
Set-VsProperties -AllowedCorsOrigins https://<server_name>

# Донастройка nginx
#По аналогии с предыдущим пунктом необходимо добавить в конфигурацию nginx информацию об экземпляре Веб-
Сервиса SVS:

# В конфигурационный файл Nginx(/etc/nginx/nginx.conf), в контекст server секцию, отвечающий за взаимодействие
на
# 443 порту (https), необходимо добавить:

# ВНИМАНИЕ! Строки должны находиться в контексте server с настроенным сертификатом проверки подлинности
сервера (TLS).
sudo nano /etc/nginx/nginx.conf
include /etc/opt/cprosvs/vssrv/svs_appname/nginx.conf;
include /etc/opt/cprosvs/vsfe/fe_appname/nginx.conf;

# Активация и запуск Сервиса Проверки:
sudo systemctl enable cprosvs-vssrv-svs_appname.service
sudo systemctl start cprosvs-vssrv-svs_appname.service

# Перезапуск службы КриптоПро SVS
sudo systemctl restart cprosvs-vssrv-<instanceName>.service
# ИЛИ
Restart-VsInstance -DisplayName

# Перезапуск nginx
sudo systemctl restart nginx.service

# Проверка статуса службы nginx
sudo systemctl status nginx.service

```

Создание и настройка экземпляра КриптоПро SVS в ОС Windows

Данный раздел определяет последовательность действий при разворачивании и настройке экземпляра Сервиса Проверки Подписи (КриптоПро SVS).

После завершения выполнения действий, описанных в данном разделе, **веб-интерфейс** Сервиса Проверки Подписи будет доступен по следующему адресу:

```
http://<hostname>/verify/
```

Программный интерфейс Сервиса Проверки Подписи будет доступен по следующему адресу:

```
http://<hostname>/verify/rest/api
```

Примечание

Если используется Сервис Проверки Подписи версии ниже, чем 2.0.2636, программный интерфейс Сервиса Проверки Подписи будет доступен по адресу: `http://<hostname>/verify/service.svc`

Предварительные условия:

- Выполнены все пункты из [развертывания КриптоПро SVS](#)

Базовая последовательность шагов по настройке (обязательные)

1. Создание экземпляра службы.

Пример:

```
New-VsInstance -DisplayName SVS -ApplicationName verify -SiteName "Default Web Site"
```

2. Ввод лицензии.

Пример:

```
New-VsLicense [-DisplayName <string>] [-SN <string>] [-CompanyName <string>]
```

Примечание

При вызове команды без параметров активируется временная лицензия на 3 месяца.

Примечание

Вызов командлета необходим при создании каждого нового экземпляра Сервиса Проверки Подписи.

3. Настройка адреса Веб-интерфейса SVS.

Адрес Веб-интерфейса SVS используется для взаимодействия веб-интерфейса с экземпляром сервиса SVS и должен быть доступен конечным пользователям.

Адрес Веб-интерфейса SVS имеет следующий вид: `https://<hostname>/<app_name>/rest/api`. Взаимодействие по протоколу HTTPS обязательно.

```
Set-VsProperties -VsAddress https://<hostname>/<app_name>/rest/api
```

4. Установка корневых сертификатов и CRL.

При разворачивании экземпляра Сервиса Проверки Подписи автоматически будут созданы хранилища сертификатов с именами **<ApplicationName>-TSL** и **<ApplicationName>-Ca**, где **<ApplicationName>** – имя веб-приложения,

указанное в командлете [New-VsInstance](#) в параметре `-ApplicationName`.

- В хранилище **<ApplicationName>-TSL** необходимо установить [корневые сертификаты](#).
- В хранилище **<ApplicationName>-Ca** необходимо установить сертификаты подчиненных УЦ и списки (CRL), которые будут использоваться при построении цепочек доверия для [проверки актуальных статусов сертификатов](#).

5. Настройка привязок веб-сервера IIS.

По умолчанию экземпляр Сервиса Проверки Подписи требует наличия http- и https-привязок на сервере приложений IIS. Если на IIS настроена только http-привязка, то необходимо отключить конечную точку Сервиса Проверки Подписи, требующую безопасного соединения. Для этого выполните следующую команду:

```
Disable-VsEndpoint -Name BasicHttps
```

Подробнее о передаче данных по безопасному соединению:

- [Включение https](#)

Опциональные настройки:

Дополнительно можно выполнить следующие настройки.

- [Режим проверки статуса сертификатов](#)
- [Ограничение набора форматов подписи, доступных для проверки](#)
- [Сопоставление расширений файлов с форматами подписи](#)
- [Кастомизация веб-интерфейса SVS](#)
- [Отображение документов](#)
- [Установка корневых сертификатов и CRL](#)
- [Получение актуального статуса сертификата](#)
- [Ограничение размера документов](#)
- [Передача данных по безопасному соединению](#)
- [Настройка проверки УЦ на принадлежность к определенному списку](#)
- [Настройка проверки формата сертификатов](#)
- [XML-преобразования](#)
- [Пакетная проверка подписи](#)
- [Шаблоны отчетов](#)

Полный список командлетов администрирования КриптоПро SVS

- [Список](#)

Пример настройки КриптоПро SVS (Windows)

```

# Создание экземпляра SVS
New-VsInstance -DisplayName SVS -ApplicationName verify -SiteName "Default Web Site"

# Ввод временной лицензии на 3 месяца
New-VsLicense

# Установка онлайн-режима проверки статуса сертификатов при помощи службы OSCP
Set-VsProperties -RevocationMode Online

# Ограничение набора форматов подписи, доступных для проверки - отключение проверки необработанной подписи
ГОСТ Р 34.10-2012
Set-VsSignatureFormat -Format GOST3410 -IsEnabled 0

# Сопоставление расширений файлов с форматами подписи - установка списка расширений для подписи формата CMS
Set-VsSignatureFormat -Format CMS -Extensions sig, p7b, p7s

# Отображение документов
Add-VsConverterPlugin -FileExtension pdf -Assembly DSS.DocumentConverter.PdfStub.dll
Add-VsConverterPlugin -FileExtension doc -Assembly DSS.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension dot -Assembly DSS.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension docm -Assembly DSS.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension dotm -Assembly DSS.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension docx -Assembly DSS.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension dotx -Assembly DSS.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension FlatOpc -Assembly DSS.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension FlatOpcMacroEnabled -Assembly DSS.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension FlatOpcTemplate -Assembly DSS.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension FlatOpcTemplateMacroEnabled -Assembly DSS.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension xml -Assembly DSS.DocumentConverter.Xml.dll
Add-VsConverterPlugin -FileExtension odt -Assembly DSS.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension ott -Assembly DSS.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension ooxml -Assembly DSS.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension WordML -Assembly DSS.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension rtf -Assembly DSS.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension html -Assembly DSS.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension xhtml -Assembly DSS.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension mhtml -Assembly DSS.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension txt -Assembly DSS.DocumentConverter.Word.dll

# Ограничение размера документов в 10 Мбайт (задается в байтах)
Set-VsEndpointGlobalSettings -MaxMessageSize 10485760

# Настройка проверки формата сертификатов
# Регистрация плагина
Add-VsCertificateVerifierPlugin -Assembly SVS.CertificateVerifier.Qualified.dll
# Добавление отпечатков корневых сертификатов Минцифры РФ
Add-VsQualifiedCATHumbprints -Thumbprint 4bc6dc14d97010c41a26e058ad851f81c842415a
Add-VsQualifiedCATHumbprints -Thumbprint aff05c9e2464941e7ec2ab15c91539360b79aa9d

# Настройка шаблона отчета о пакетной проверке подписи (Windows)
Set-VsProperties -WordFilePath "C:\Program Files\Crypto
Pro\DSS\VerificationService\templates\packagereporttemplate.docx"
Set-VsProperties -XsltFilePath "C:\Program Files\Crypto
Pro\DSS\VerificationService\templates\packagereporttemplate.xslt"
Restart-VsInstance

```

Настройка КриптоПро SVS

Примечание

Перед настройкой КриптоПро SVS убедитесь, что выполнены предыдущие необходимые действия по его [развертыванию](#).

Сервис Проверки Подписи предоставляет пользователям программный интерфейс для проверки подписи и сертификатов. Также Сервис Проверки Подписи предоставляет веб-интерфейс для проверки подписи и сертификатов.

Сервис Проверки Подписи позволяет проверять электронные подписи следующих форматов:

1. Усовершенствованная подпись (CMS Advanced Electronic Signatures, CAdES) а. Присоединенная подпись б. Отделенная подпись
2. XML Digital Signature (XMLDSig).
3. Электронная подпись ГОСТ Р 34.10–2012.
4. Подпись документов формата PDF.
5. Подпись документов Microsoft Office.

Также Сервис Проверки Подписи позволяет проверять [статус сертификата ЭП](#) и/или [формат сертификата](#).

В этом разделе:

- [Создание и настройка экземпляра сервиса SVS \(Windows\)](#)
- [Создание и настройка экземпляра сервиса SVS \(*nix\)](#)
- [Администрирование SVS](#)
- [Отображение документов](#)
- [Установка корневых сертификатов и CRL](#)
- [Получение актуального статуса сертификата](#)
- [Ограничение размера документов](#)
- [Передача данных по безопасному соединению](#)
- [Настройка проверки УЦ на принадлежность к определенному списку](#)
- [Настройка проверки формата сертификатов](#)
- [XML-преобразования](#)
- [Пакетная проверка подписи](#)
- [Кастомизация Веб-интерфейса SVS](#)

Администрирование SVS

Настройка Сервиса Проверки Подписи осуществляется с помощью Windows PowerShell. Команды администрирования включены в модуль `CryptoPro.DSS.PowerShell.VerificationService` для ОС Windows, а также модули `CryptoPro.VerificationService.PowerShell` и `CryptoPro.VerificationService.Frontend.PowerShell` для *nix-систем.

Список командлетов, входящих в состав PowerShell модуля SVS, можно получить, выполнив следующую команду:

```
#Windows
Get-Command -Module CryptoPro.DSS.PowerShell.VerificationService -CommandType Cmdlet

#*nix
#Модуль Сервиса Проверки Подписи
Get-Command -Module CryptoPro.VerificationService.PowerShell
#Модуль веб-интерфейса Сервиса Проверки Подписи
Get-Command -Module CryptoPro.VerificationService.Frontend.PowerShell
```

Для получения справки по каждому из командлетов выполните следующую команду:

```
Get-Help <имя_командлета>
```

Например:

```
Get-Help Set-VsProperties
или
Get-Help Set-VsProperties -Full
```

Командлеты администрирования

- [Add-VsCertificateVerifierPlugin](#)
- [Add-VsConverterPlugin](#)
- [Add-VsQualifiedCAThumbprints](#)
- [Add-VsTransformPlugin](#)
- [Disable-VsEndpoint](#)
- [Disable-VsTracing](#)
- [Enable-VsEndpoint](#)
- [Enable-VsTracing](#)
- [Get-VsCertificateVerifierPlugin](#)
- [Get-VsConverterPlugin](#)
- [Get-VsCustomization](#)
- [Get-VsEndpoint](#)
- [Get-VsEndpointGlobalSettings](#)
- [Get-VsInstance](#)
- [Get-VsLicense](#)
- [Get-VsProperties](#)
- [Get-VsQualifiedCAThumbprints](#)
- [Get-VsSignatureFormat](#)
- [Get-VsTracing](#)
- [Get-VsTransformPlugin](#)
- [New-VsInstance](#)
- [New-VsLicense](#)
- [Remove-VsCertificateVerifierPlugin](#)
- [Remove-VsConverterPlugin](#)
- [Remove-VsInstance](#)
- [Remove-VsQualifiedCAThumbprints](#)

- [Remove-VsTransformPlugin](#)
- [Reset-VsCustomization](#)
- [Restart-VsInstance](#)
- [Set-VsCertificateVerifierPlugin](#)
- [Set-VsConverterPlugin](#)
- [Set-VsCustomization](#)
- [Set-VsEndpointGlobalSettings](#)
- [Set-VsProperties](#)
- [Set-VsSignatureFormat](#)
- [Set-VsTracing](#)
- [Update-VsInstance](#)
- [Update-VsLicense](#)
- [Add-VsFeInstance](#)
- [Get-VsFeProperties](#)
- [Remove-VsFeInstance](#)
- [Set-VsFeProperties](#)

Установка корневых сертификатов и CRL

Перед началом использования КриптоПро SVS необходимо установить корневые сертификаты, которые будут использоваться при построении и проверке цепочки сертификатов подписи. Корневые сертификаты КриптоПро SVS устанавливаются в хранилище `<ApplicationName>-TSL`.

Примечание

Если во время использования КриптоПро SVS список корневых сертификатов изменялся (сертификаты добавлялись или удалялись), то для вступления изменений в силу необходимо перезапустить сервис.

Сертификаты подчиненных УЦ должны быть установлены в хранилище `<ApplicationName>-CA` или в хранилище Промежуточные Центры Идентификации Локального компьютера.

Если для проверки статусов сертификатов не используется служба OCSP, то необходимо установить списки сертификатов, досрочно прекративших действие (CRL). CRL устанавливаются в хранилище `<ApplicationName>-CA` или в хранилище Промежуточные Центры Идентификации Локального компьютера.

Примечание

При большом количестве сертификатов подчиненных УЦ и CRL рекомендуется устанавливать их только в хранилище `<ApplicationName>-CA`.

Если сервер SVS не имеет доступа в сеть Internet, то необходимо перевести его в режим проверки статуса сертификатов Offline, то есть по локально установленным CRL. Для переключения SVS в режим проверки Offline выполните команду:

```
Set-VsProperties -RevocationMode Offline
```

Получение актуального статуса сертификата

КриптоПро SVS поддерживает следующие режимы проверки актуального статуса сертификата:

- Не проверять
- Offline-проверка (CRL)
- Online-проверка (OCSP)

Примечание

Если включен режим "Не проверять", SVS не будет проверять актуальный статус сертификата, но проверит цепочку сертификатов, формат сертификата и др.

Режим проверки устанавливается с помощью командлета командлета [Set-VsProperties](#) с параметром `-RevocationMode`.

В **Offline-режиме** проверка статуса сертификата осуществляется по локально установленным спискам сертификатов, досрочно прекративших действие (CRL). CRL должны быть установлены в хранилище `<ApplicationName>-CA` или в хранилище Промежуточные Центры Идентификации Локального компьютера.

При проверке подписи CAdES-BES, CAdES-T, PDF, если CRL не установлен локально и в сертификате подписи присутствует расширение CDP (см. ISO/IEC 9594-8:2020 или Rec. ITU-T X.509 (10/2019)), будет сделана попытка загрузить CRL по сети. При проверке подписи других видов (MS Office, XMLDSig, необработанная подпись) или сертификата используются только локально установленные CRL.

В **Online-режиме** проверка актуального статуса сертификата осуществляется по протоколу OCSP или при помощи CRL, установленных локально или загруженных по сети. Адрес службы OCSP может быть задан следующими способами:

- в расширении AIA сертификата,
- в свойствах корневого сертификата в хранилище сертификатов,
- в групповой политике OCSP-клиента.

В случае подписи формата CAdES-X Long Type 1 при проверке статуса сертификата обращение к службе OCSP или CRL не производится, так как все необходимые доказательства подлинности содержатся в самой подписи.

Отображение документов

Веб-интерфейс Пользователя предоставляет пользователям возможность визуализации документов при проверке подписи. Поддерживается просмотр документов следующих форматов: PDF, DOC, DOT, DOCM, DOTM, DOCX, DOTX, FlatOpc, FlatOpcMacroEnabled, FlatOpcTemplate, FlatOpcTemplateMacroEnabled, XML, ODT, OTT, OOXML, WordML, RTF, HTML, XHTML, MHTML и TXT.

Плагины, позволяющие визуализировать документы данных форматов, находятся в директории **<Путь установки>\Plugins\Converters** и отвечают за отображение документов следующих форматов:

- PDF;
- DOC, DOT, DOCM, DOTM, DOCX, DOTX, FlatOpc, FlatOpcMacroEnabled, FlatOpcTemplate, FlatOpcTemplateMacroEnabled, XML, ODT, OTT, OOXML, WordML, RTF, HTML, XHTML, MHTML и TXT,
- XML.

Для *unix-систем имена плагинов имеют следующие наименования:

- `CryptoPro.Plugins.DocumentConverter.PdfStub.dll`,
- `CryptoPro.Plugins.DocumentConverter.Word.dll`,
- `CryptoPro.Plugins.DocumentConverter.Xml.dll`.

Для Windows имена плагинов имеют следующие наименования:

- `DSS.DocumentConverter.PdfStub.dll`,
- `DSS.DocumentConverter.Word.dll`,
- `DSS.DocumentConverter.Xml.dll`.

Для активации возможности просмотра документов необходимо зарегистрировать нужные форматы и соответствующие плагины с помощью PowerShell. Для каждого экземпляра веб-приложения в директории **<Путь установки>\VerificationService** создается свой собственный конфигурационный файл с именем `<Имя экземпляра веб-приложения>_convert.config`.

Данный сценарий регистрирует форматы документов, для которых возможен просмотр с помощью установленных плагинов.

Пример для Windows

```
Add-VsConverterPlugin -FileExtension pdf -Assembly DSS.DocumentConverter.PdfStub.dll

Add-VsConverterPlugin -FileExtension doc -Assembly DSS.DocumentConverter.Word.dll

Add-VsConverterPlugin -FileExtension dot -Assembly DSS.DocumentConverter.Word.dll

Add-VsConverterPlugin -FileExtension docm -Assembly DSS.DocumentConverter.Word.dll

Add-VsConverterPlugin -FileExtension dotm -Assembly DSS.DocumentConverter.Word.dll

Add-VsConverterPlugin -FileExtension docx -Assembly DSS.DocumentConverter.Word.dll

Add-VsConverterPlugin -FileExtension dotx -Assembly DSS.DocumentConverter.Word.dll

Add-VsConverterPlugin -FileExtension FlatOpc -Assembly DSS.DocumentConverter.Word.dll

Add-VsConverterPlugin -FileExtension FlatOpcMacroEnabled -Assembly DSS.DocumentConverter.Word.dll

Add-VsConverterPlugin -FileExtension FlatOpcTemplate -Assembly DSS.DocumentConverter.Word.dll

Add-VsConverterPlugin -FileExtension FlatOpcTemplateMacroEnabled -Assembly DSS.DocumentConverter.Word.dll

Add-VsConverterPlugin -FileExtension xml -Assembly DSS.DocumentConverter.Xml.dll

Add-VsConverterPlugin -FileExtension odt -Assembly DSS.DocumentConverter.Word.dll

Add-VsConverterPlugin -FileExtension ott -Assembly DSS.DocumentConverter.Word.dll

Add-VsConverterPlugin -FileExtension ooxml -Assembly DSS.DocumentConverter.Word.dll

Add-VsConverterPlugin -FileExtension WordML -Assembly DSS.DocumentConverter.Word.dll

Add-VsConverterPlugin -FileExtension rtf -Assembly DSS.DocumentConverter.Word.dll

Add-VsConverterPlugin -FileExtension html -Assembly DSS.DocumentConverter.Word.dll

Add-VsConverterPlugin -FileExtension xhtml -Assembly DSS.DocumentConverter.Word.dll

Add-VsConverterPlugin -FileExtension mhtml -Assembly DSS.DocumentConverter.Word.dll

Add-VsConverterPlugin -FileExtension txt -Assembly DSS.DocumentConverter.Word.dll
```

Пример для *nix

```

Add-VsConverterPlugin -FileExtension pdf -Assembly CryptoPro.Plugins.DocumentConverter.PdfStub.dll
Add-VsConverterPlugin -FileExtension doc -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension dot -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension docm -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension dotm -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension docx -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension dotx -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension FlatOpc -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension FlatOpcMacroEnabled -Assembly
CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension FlatOpcTemplate -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension FlatOpcTemplateMacroEnabled -Assembly
CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension xml -Assembly CryptoPro.Plugins.DocumentConverter.Xml.dll -Parameters @{
"encoding"="UTF-8" }
Add-VsConverterPlugin -FileExtension odt -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension ott -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension ooxml -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension WordML -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension rtf -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension html -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension xhtml -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension mhtml -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll
Add-VsConverterPlugin -FileExtension txt -Assembly CryptoPro.Plugins.DocumentConverter.Word.dll

```

Если просмотр загруженного документа поддерживается установленными плагинами и выполнена регистрация в конфигурационном файле, то документ отображается во вкладке «Загрузка документа» Мастера подписи.



Ограничение размера документов

При разворачивании экземпляра сервиса устанавливается ограничение на размер передаваемых сообщений в 5 Мбайт. Для изменения размера сообщений необходимо выполнить следующие настройки:

- Изменить настройки конечных точек сервиса при помощи командлета [Set-VsEndpointGlobalSettings](#)

После выполнения командлета дополнительные настройки на IIS не требуются.

Примечание

Данная настройка устанавливает ограничение на общий размер передаваемых сообщений. Документ, который передается на проверку, должен быть меньше установленного значения на 15-20%.

Пример:

```
# Ограничение размера документов в 10 Мбайт (задается в байтах)
Set-VsEndpointGlobalSettings -MaxMessageSize 10485760
```

При передаче больших документов может потребоваться увеличить ограничение на время приема/передачи данных, по умолчанию оно составляет 30 сек. Данное изменение также производится с помощью команды [Set-VsEndpointGlobalSettings](#).

Передача данных по безопасному соединению

При разворачивании экземпляра Сервиса Проверки Подписи по умолчанию разрешена передача данных как по http, так и по https. По умолчанию экземпляр Сервиса Проверки Подписи требует наличия http- и https-привязок на сервере приложений IIS. Если на IIS настроена только http-привязка, то необходимо отключить конечную точку Сервиса Проверки Подписи, требующую безопасного соединения. Для этого выполните следующую команду:

```
Disable-VsEndpoint -Name BasicHttps
```

Для того чтобы разрешить передачу данных только по безопасному соединению (отключить конечную точку Сервиса Проверки Подписи, работающую по http), выполните следующую команду:

```
Disable-VsEndpoint -Name BasicHttp
```

Примечание

Дополнительно можно настроить IIS на работу только по безопасному соединению либо удалив http привязку, либо настроив перенаправление с http на https, например, как описано в [данной статье](#).

Настройка проверки принадлежности УЦ к определенному списку

Квалифицированная электронная подпись (КЭП) создается с помощью сертифицированных ФСБ криптографических средств и имеет сертификат от аккредитованного удостоверяющего центра, выступающего гарантом подлинности подписи. Электронный документ, подписанный КЭП, во всех случаях приравнивается законодательством к бумажному документу с собственноручной подписью.

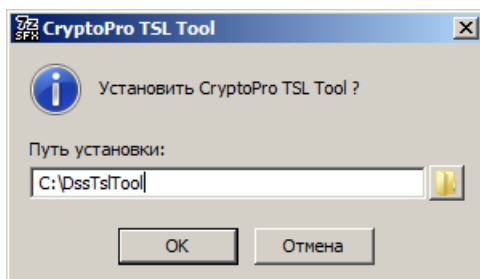
Подтверждение подлинности ЭП сертификата, изданного удостоверяющим центром, входящим в список аккредитованных удостоверяющих центров Министерства цифрового развития, связи и массовых коммуникаций, и соответствующих электронных подписей при помощи КриптоПро SVS возможно после выполнения следующих условий:

- Корневой сертификат Головного удостоверяющего центра должен быть установлен в хранилище сертификатов SVS.
- Сертификаты подчиненных Удостоверяющих Центров: «УЦ 1 ИС ГУЦ», «УЦ 2 ИС ГУЦ» должен быть установлен в хранилище «Промежуточные центры сертификации» локального компьютера.
- Сертификат аккредитованного УЦ в режиме подчинения должен быть установлен в хранилище «Промежуточные центры сертификации» локального компьютера.
- КриптоПро SVS должен иметь возможность проверки статуса сертификата по CRL или OCSP-ответу. Для этого необходимо либо установить локально и регулярно обновлять CRL, либо обеспечить доступ с сервера SVS в интернет для возможности загрузки CRL или проверки актуального статуса сертификата по протоколу OCSP.

Для удобства установки всех необходимых сертификатов аккредитованных УЦ и CRL в состав установки КриптоПро SVS включена утилита КриптоПро TSL (`Dss.Ts1Tool.exe`). Утилита предназначена для выполнения следующих действий:

- Установка корневого сертификата Головного удостоверяющего центра
- Загрузка TSL (списка аккредитованных УЦ, Trust-service Status List)
- Установка сертификатов подчиненных УЦ, перечисленных в TSL (сертификаты аккредитованных УЦ и сертификаты подчинённых УЦ)
- Загрузки и установки CRL аккредитованных УЦ
- Удалению CRL аккредитованных УЦ с истёкшим сроком действия

Утилита распространяется в самораспаковывающемся архиве `DssTs1Tool.exe`, который устанавливается в каталог **C:\Program Files\Crypto Pro\DSS\VerificationService**. Для начала работы с утилитой необходимо распаковать архив:



После распаковки архива необходимо ознакомиться со справкой к утилите. Для этого в командной строке следует перейти в каталог, куда была распакована утилита, и выполнить следующую команду.

```
DSS.Ts1Tool.exe --help
```

Пример базового использования утилиты `Dss.Ts1Tool`:

- Первоначальная установка всех необходимых сертификатов и CRL:

```
DSS.Ts1Tool.exe --rootstorages SVS-TSL --castorages SVS-CA --onlyvalidca 1
```

Примечание

Имя хранилища сертификатов для установки сертификата головного удостоверяющего Центра зависит от имени Веб-приложения SVS и имеет вид `<ApplicationName>-TSL`. Имя хранилища сертификатов и CRL для установки сертификатов

подчиненных удостоверяющих Центров имеет вид <ApplicationName>-CA.

Примечание

При обновлении с версий SVS 2.0.2300 и предыдущих рекомендуется очистить хранилище Промежуточные центры сертификации локального компьютера от ранее установленных сертификатов и CRL. Большое количество сертификатов и CRL в данном хранище замедляет как работу SVS, так и системы в целом.

Примечание

Для того чтобы устанавливать сертификаты и CRL удостоверяющих центров, имеющих аккредитацию на момент запуска утилиты, используется параметр `--onlyvalidca 1`.

- Обновление сертификатов аккредитованных УЦ и CRL

```
DSS.TslTool.exe --skiproot --removeoutOfdatecrl --removeoutOfdatecert --rootstorages SVS-TSL --castorages SVS-CA
```

Примечание

Выполнение данной команды можно добавить в планировщик Windows для регулярного обновления CRL.

В случае если сервер SVS не имеет выхода в интернет, то сертификаты аккредитованных УЦ и CRL могут быть установлены из файла. Для этого на машине, имеющей выход в Интернет, следует запустить утилиту со следующими параметрами.

```
DSS.TslTool.exe --downloadcrlonly --skipcerts --skiproot
```

После выполнения данной команды в каталог `<dsstsltool_installdir>\tmp` будут сохранены TSL и CRL. Каталог для сохранения объектов, загруженных из сети, при необходимости может быть изменен.

Примечание

Для запуска утилиты `Dss.TslTool.exe` на другом хосте необходимо наличие .NET Framework 4.6.1. Установочный файл может быть взят с дистрибутивного диска.

Далее необходимо перенести каталог с загруженными файлами на сервер КриптоПро SVS. Для установки сертификатов аккредитованных УЦ и CRL из файла необходимо запустить утилиту со следующими параметрами:

```
DSS.TslTool.exe --crlfromfolder C:\temp\ --tslfile C:\temp\tsl.xml --castorages SVS-CA
```

Настройка проверки формата сертификатов

Сервис Проверки Подписи «КриптоПро SVS» позволяет настроить дополнительную проверку соответствия полей сертификата установленной форме.

Проверка происходит на основании структуры полей, представленных в следующих правилах.

- **Версия** (version). Версия сертификата должна быть не ниже 3.
- **Серийный номер** (serial number). Проверяется наличие номера и отсутствие в нем недопустимых символов.
- **Алгоритм подписи** (signature). В поле algorithm, входящем в состав поля signature, должен содержаться идентификатор используемого алгоритма подписи:
 - ГОСТ Р 34.10–2012 с ключом длиной 256 бит: "1.2.643.7.1.1.3.2", szOID_CP_GOST_R3411_12_256_R3410
 - ГОСТ Р 34.10–2012 с ключом длиной 512 бит: "1.2.643.7.1.1.3.3", szOID_CP_GOST_R3411_12_512_R3410
 - (для архивного хранения и проверки подписи) ГОСТ Р 34.10-2001: "1.2.643.2.2.3", szOID_CP_GOST_R3411_R3410EL
- **Имя издателя** (issuer) — проверяется только наличие его в сертификате.
- **Дата и время начала действия сертификата** (notBefore).
- **Дата и время окончания действия сертификата** (notAfter).
- **Имя владельца сертификата** (subject). Возможна проверка следующих компонентов имени владельца сертификата (компоненты имени проверяются на допустимые символы, длину, если такие требования имеются):
 - ФИО или наименование владельца (и другие сведения, если требуется) (commonName, title, surname, givenName)
 - Местонахождение (countryName, stateOrProvinceName, localityName, streetAddress)
 - СНИЛС (SNILS)
 - ОГРН (OGRN)
 - ОГРНИП (OGRNIP)
 - ИНН (INN)
 - ИНН юридического лица (ЮЛ) (INNLE)
 - совпадение общего имени и наименования организации (CN=O)
 - тип идентификации заявителя (identificationKind)
- **Открытый ключ** (subjectPublicKeyInfo). Проверяется только наличие его в сертификате.
- **Дополнения (расширения) сертификата** (Extensions). Проверяется только наличие следующих расширений в сертификате.
 - Authority Key Identifier, OID.2.5.29.35, идентификатор ключа УЦ.
 - Key Usage, OID.2.5.29.15, область использования ключа.
 - Certificate Policies, OID.2.5.29.32, политики сертификата. Для данного расширения проверяется содержимое в соответствии с требованиями, указанными в Приказе ФСБ РФ от 27 декабря 2011 г. N 795.
 - Subject Sign Tool, OID.1.2.643.100.111, сведения о средстве ЭП владельца сертификата.
 - Issuer Sign Tool, OID.1.2.643.100.112, сведения о средствах ЭП УЦ и средствах УЦ.
 - ExtendedKeyUsage, OID.2.5.29.37, расширенное использование ключа. Состав дополнения (расширения) зависит от информационной системы, в которой используется сертификат.
 - CDP, OID.2.5.29.31, точки распространения списков сертификатов, досрочно прекративших действие (CRL).
 - IdentificationKind, OID.1.2.643.100.114, идентификация заявителя.

Проверка сертификата выполняется при помощи специального плагина. Для активации проверки сертификатов необходимо зарегистрировать плагин с помощью Windows PowerShell. После установки КриптоПро SVS плагин находится в директории <Путь установки>\Plugins\certverifiers\ и называется SVS.CertificateVerifier.Qualified.dll.

Для регистрации и настройки плагина проверки формата сертификатов используются командлеты [Add-VsCertificateVerifierPlugin](#), [Get-VsCertificateVerifierPlugin](#), [Remove-VsCertificateVerifierPlugin](#).

Для настройки проверки того, что сертификаты выданы определенным УЦ, необходимо выполнение следующих действий:

- зарегистрировать отпечатки корневых сертификатов в КриптоПро SVS. Работа с отпечатками производится при помощи командлетов [Add-VsQualifiedCATHumbprints](#), [Get-VsQualifiedCATHumbprints](#) и [Remove-VsQualifiedCATHumbprints](#). Если отпечатки не заданы, данная проверка сертификатов проводиться не будет.
- установить корневые сертификаты УЦ в выделенное хранилище КриптоПро SVS. Хранилище создается автоматически при установке КриптоПро SVS и имеет название вида `<Имя веб-приложения SVS>-TSL`.

Пример настройки плагина

```
# Регистрация плагина и настройка пути к файлу TSL (Windows)
Add-VsCertificateVerifierPlugin -Assembly SVS.CertificateVerifier.Qualified.dll -PluginDescription "Проверка сертификата на соответствие установленной форме" -Parameters @{ 'TSLPath'='C:\TSL.xml' }
# Регистрация плагина и настройка пути к файлу TSL (*nix)
Add-VsCertificateVerifierPlugin -Assembly
CryptoPro.Plugins.VerificationService.CertificateVerifier.Qualified.dll -PluginDescription "Проверка сертификата на соответствие установленной форме" -Parameters @{ 'TSLPath'='/path_to/TSL.xml' }

# Добавление отпечатков корневых сертификатов Минцифры РФ
Add-VsQualifiedCATHumbprints -Thumbprint 4bc6dc14d97010c41a26e058ad851f81c842415a
Add-VsQualifiedCATHumbprints -Thumbprint aff05c9e2464941e7ec2ab15c91539360b79aa9d
Add-VsQualifiedCATHumbprints -Thumbprint 2f0cb09be3550ef17ec4f29c90abd18bfcaad63a
```

Если плагин зарегистрирован и настроен, в веб-интерфейсе КриптоПро SVS при проверке сертификата будет выводиться дополнительная информация о соответствии его заданным правилам. При проверке ЭП также будет осуществляться проверка данного сертификата.

Дополнительные параметры плагина:

- **LocationCheck** – требовать обязательного наличия компонентов местонахождения. Возможные значения: true, false. Значение по умолчанию false;
- **OrganizationNameStrictCheck** – требовать совпадения значений компонентов имени CN и О в сертификате. Возможные значения: true, false. Значение по умолчанию false;
- **INNforLECheckMode** – режим проверки ИНН ЮЛ. Возможные значения: Any, Soft, Strict. Значение по умолчанию Soft.
 - **Any** – требуется присутствие ИНН и/или INNLE;
 - **Soft** – требуется присутствие INNLE; присутствие INN доускается;
 - **Strict** – требуется присутствие только INNLE.
- **TSLPath** - полный путь к файлу TSL.

Для проверки УЦ на принадлежность к заданному списку УЦ необходимо указать путь к файлу со списком УЦ `Tsl.xml` в параметре **TSLPath**.

Файл `Tsl.xml` публикуется по адресу `https://e-trust.gosuslugi.ru/app/scc/portal/api/v1/portal/ca/getxml`.

Загрузка файла `Tsl.xml` возможна следующими способами:

- при помощи утилиты [Dss.TslTool.exe](#)

```
DSS.TslTool.exe --skipcrl --skipcerts --skiproot
```

Файл TSL будет загружен в папку `tmp` в каталоге утилиты [Dss.TslTool.exe](#).

- при помощи команды `wget` в консоли Powershell

```
wget https://e-trust.gosuslugi.ru/app/scc/portal/api/v1/portal/ca/getxml -OutFile E:\tmp\tsl.xml
```

SVS автоматически отслеживает изменения файла TSL, путь к которому указан в параметре **TSLPath**. Скопировать

актуальный файл TSL можно с помощью Powershell-скрипта, приведенного ниже. Данный скрипт возможно добавить в планировщик задач и выполнять раз в сутки (или чаще).

Пример скрипта копирования TSL:

```
$ErrorActionPreference = "Stop"

# Полный путь к загруженному файлу TSL
$sourceFile = "E:\tmp\tsl_source\tsl.xml"

# Полный путь к файлу TSL, используемому SVS
$destinationFile = "E:\tmp\tsl_target\tsl.xml"

# Загрузка файла TSL
wget https://e-trust.gosuslugi.ru/app/scc/portal/api/v1/portal/ca/getxml -OutFile $sourceFile

if (!(Test-Path $sourceFile -PathType Leaf)) {
    # Загруженный файл TSL отсутствует
    Write-Host "Файл TSL отсутствует! " $sourceFile
    exit 2;
}

$targetFolder1 = Split-Path $destinationFile -Parent
if (!(Test-Path $targetFolder1 -PathType Container)) {
    # Не существует каталог, в который требуется скопировать файл TSL
    Write-Host "Каталог не существует! " $targetFolder1
    exit 2;
}

if (!(Test-Path $destinationFile -PathType Leaf)) {

    Write-Host "Копирование нового файла TSL..."

    # Целевой файл TSL отсутствует
    # Просто копируем файл TSL
    Copy-Item $sourceFile -Destination $destinationFile

} else {
    # Целевой файл TSL присутствует
    # Копируем файл TSL при помощи временного файла

    Write-Host "Замена существующего файла TSL... "

    $targetFolder = Split-Path $destinationFile -Parent
    $tmpTslPath = Join-Path -Path $targetFolder -ChildPath "temp_tsl.xml"

    if (Test-Path $tmpTslPath -PathType Leaf) {
        # Если временный файл существует, удалим его
        Remove-Item $tmpTslPath -Force
    }

    # Копируем TSL во временный файл
    Copy-Item $sourceFile -Destination $tmpTslPath

    # Перемещаем TSL в целевой файл
    Move-Item $tmpTslPath -Destination $destinationFile -Force
}
```

Настройка выполнения проверки полей сертификата по умолчанию

Проверка соответствия полей сертификата установленной форме при помощи описанного в данном разделе плагина может применяться по умолчанию как в веб-интерфейсе SVS, так и при обращении к SVS с использованием REST API. Для этого в настройках плагина необходимо указать флаг `CheckByDefaultRequired`.

Пример:

```
Set-VsCertificateVerifierPlugin -ID 1 -CheckByDefaultRequired 1
```

В зависимости от интерфейса SVS данная настройка будет применена следующим образом:

- **в веб-интерфейсе SVS** - напротив пункта "Проверка сертификата на соответствие установленной форме" (или иной формулировке, если это было указано при настройке плагина) в разделе "Дополнительные проверки" по умолчанию будет активирован чекбокс. Пользователь может самостоятельно отключить проверку, деактивировав данный чекбокс перед отправкой сертификата на проверку.
- **при использовании REST API SVS** - параметр зависит от переданного в запросе списка [CertVerifiersPluginsIds](#):
 - если список передан - проверка не учитывается, будут применены плагины, указанные в списке;
 - если список передан со значением **NULL** - проверка не учитывается, никакие дополнительные проверки к сертификату применяться не будут;
 - если список **НЕ** передан (отсутствует в запросе) - проверка учитывается, сертификат будет проверен в соответствии с настройками плагина, описанного в данном разделе.

Для прикладных систем, взаимодействующих с КриптоПро SVS через REST API, но не умеющих обрабатывать результаты дополнительных проверок сертификатов (параметр [CertificateVerificationResult](#)), можно включить неуспешный результат проверки в основное сообщение об ошибке (параметр [Message](#)). Данное поведение можно настроить при помощи следующей команды.

```
Set-VsProperties -IncludeCertPluginErrorInfoInMainError 1  
Restart-VsInstance
```

XML-преобразования

Сервис Проверки Подписи КриптоПро SVS позволяет регистрировать дополнительные XML-преобразования, используемые при проверке электронной подписи XML-документов (XMLDSig)(<https://www.w3.org/TR/xmlsig-core1/>). Преобразования являются библиотеками, устанавливаемыми по умолчанию в директорию `C:\Program Files\Crypto Pro\DSS\Plugins\Transforms` для Windows и папку `/opt/cprosvs/plugins/transforms/` для *nix.

В КриптоПро SVS доступны следующие XML-преобразования:

- [XML-Signature XPath Filter 2.0](#)
Идентификатор: `http://www.w3.org/2002/06/xmlsig-filter2`;
- Преобразование, разработанное для Федеральной таможенной службы (ФТС)
Идентификатор: `urn:xml-dsig:transformation:v1.1`.

Регистрация XML-преобразований осуществляется при помощи командлета [Add-VsTransformPlugin](#).

Пример (ОС *nix):

```
#Преобразование для ФТС
Add-VsTransformPlugin -Assembly CryptoPro.Plugins.Xml.Transforms.dll -Classname
CryptoPro.Plugins.Xml.Transforms.XmlFssTransform -Identifiers "urn:xml-dsig:transformation:v1.1"

#Преобразование XML-Signature XPath Filter 2.0
Add-VsTransformPlugin -Assembly CryptoPro.Plugins.Xml.Transforms.dll -Classname
CryptoPro.Plugins.Xml.Transforms.Filter2SubstractTransform -Identifiers "http://www.w3.org/2002/06/xmlsig-
filter2"
```

Пример (ОС Windows):

```
#Преобразование для ФТС
Add-VsTransformPlugin -Assembly CryptoPro.DSS.Xml.Transforms.dll -Classname
CryptoPro.DSS.Xml.Transforms.XmlFssTransform -Identifiers "urn:xml-dsig:transformation:v1.1"

#Преобразование XML-Signature XPath Filter 2.0
Add-VsTransformPlugin -Assembly CryptoPro.DSS.Xml.Transforms.dll -Classname
CryptoPro.DSS.Xml.Transforms.Filter2SubstractTransform -Identifiers "http://www.w3.org/2002/06/xmlsig-
filter2"
```

Настройка проверки подписи пакета документов

КриптоПро SVS поддерживает возможность проверки подписи пакета документов как при помощи собственного веб-интерфейса, так и при помощи [программного интерфейса](#).

Пакетная проверка подписи не требует отдельных настроек и работает по умолчанию после развертывания и настройки КриптоПро SVS. Тем не менее, необходимо учитывать следующие настройки, которые могут влиять на работу пакетной проверки подписи.

1. Регистрация [расширений](#) файлов подписи, соответствующих формату подписи.
2. Ограничения максимального [размера](#) пакета документов.
3. [Шаблон отчета](#).

Регистрация расширений файлов подписи

Данная настройка позволяет КриптоПро SVS определять формат подписи на основании расширений загруженных файлов. При пакетной проверке подписи необходимо соблюдать следующие правила:

- Для одного формата подписи допускается указание нескольких расширений файлов.
- Все файлы в отправленном на проверку пакете должны иметь подпись одного и того же формата.
- Расширения файлов в пакете могут быть различными, но из списка зарегистрированных расширений для данного формата подписи.

Пример регистрации распространенных расширений для файлов подписи формата CMS:

```
Set-VsSignatureFormat -Format CMS -IsEnabled 1 -Extensions sig, p7s, sign, *
Restart-VsInstance
```

При необходимости список расширений можно увеличить.

Настройка ограничения размера пакета документов

По умолчанию КриптоПро SVS обрабатывает запросы размером не более 5Mb. Для пакетной проверки подписи необходимо увеличить допустимый максимальный размер запроса.

Пример команды для увеличения размера запроса до ~60Mb:

```
Set-VsEndpointGlobalSettings -DisplayName Verify -MaxMessageSize 60000000
Restart-VsInstance
```

При необходимости ограничения могут быть увеличены.

Настройка шаблона отчета

Шаблон отчета представляет собой пару следующих документов:

- Шаблон-контейнер - представляет собой Word-документ (.docx).
- Шаблон результатов проверки - представляет собой XSL-преобразование (XSL Transform, .XSLT).

По умолчанию КриптоПро SVS использует встроенные в него шаблоны отчетов. В случае если требуется изменить данные шаблоны, следует выполнить следующие действия.

1. Скопировать образцы шаблонов из директории `C:\Program Files\Crypto Pro\DSS\VerificationService\templates` для ОС Windows или директории `/opt/cprosvs/svsrv/templates/` для *nix-систем в другую удобную директорию за пределами директории, куда установлен КриптоПро SVS. Если скопировать образцы в папки КриптоПро SVS или изменить в данной папке без перемещения, изменения могут быть утеряны при обновлении КриптоПро SVS.
2. Отредактировать (при необходимости) файлы шаблонов.
3. Зарегистрировать новые шаблоны отчетов в КриптоПро SVS (требуется перезапуск экземпляра сервиса):

```
Set-VsProperties -WordFilePath "<path>\packagereporttemplate.docx"  
Set-VsProperties -XsltFilePath "<path>\packagereporttemplate.xslt"  
Restart-VsInstance
```

Формат шаблонов отчетов

Шаблон-контейнер определяет фиксированные части отчета: колонтитул, заголовки, нумерацию страниц и т.п.

Единственное требование к шаблону-контейнеру – наличие метки для размещения результатов проверки пакета документов. Метка представляет собой текст следующего вида:

```
<data>
```

При формировании отчета метка будет замещена результатом проверки пакета документов.

Шаблон результатов проверки представляет собой XSL-преобразование (XSL Transform, XSLT). Результатом применения XSLT должен быть HTML-документ.

В случае если образцы шаблонов отчетов были утеряны, их можно загрузить по следующим ссылкам:

- [Шаблон-контейнер](#)
- [Шаблон результатов проверки](#)

Диагностика КриптоПро SVS

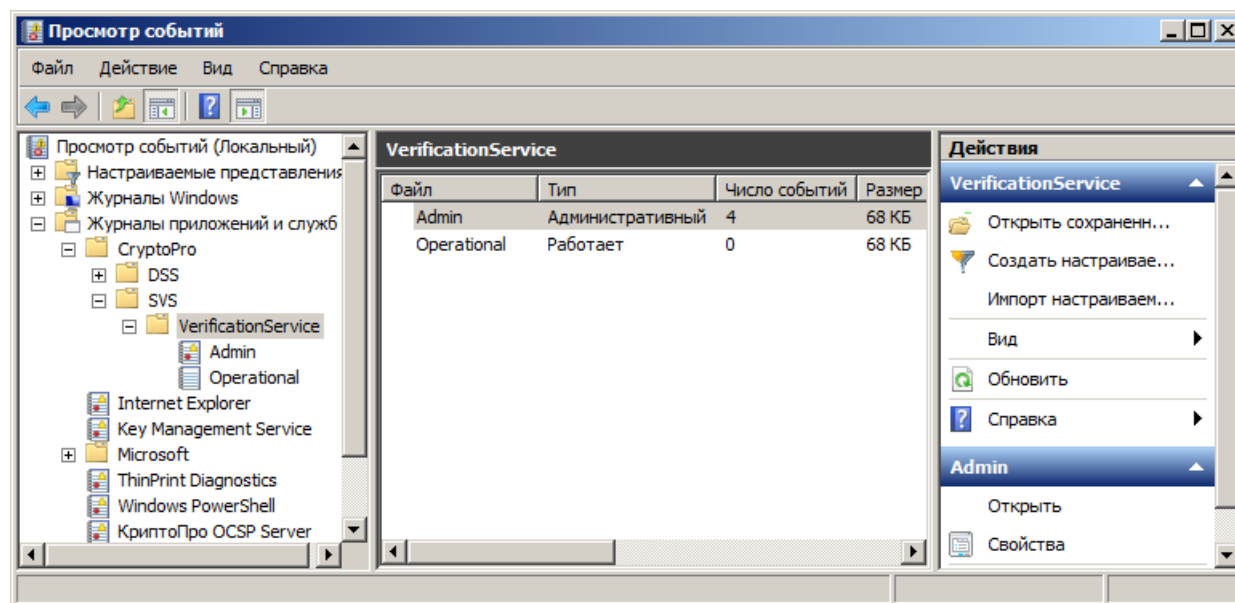
В этом разделе:

- [Журналы Windows](#)
- [Диагностика ошибок при проверке CAdES-подписи](#)
- [Журналирование сетевых взаимодействий](#)

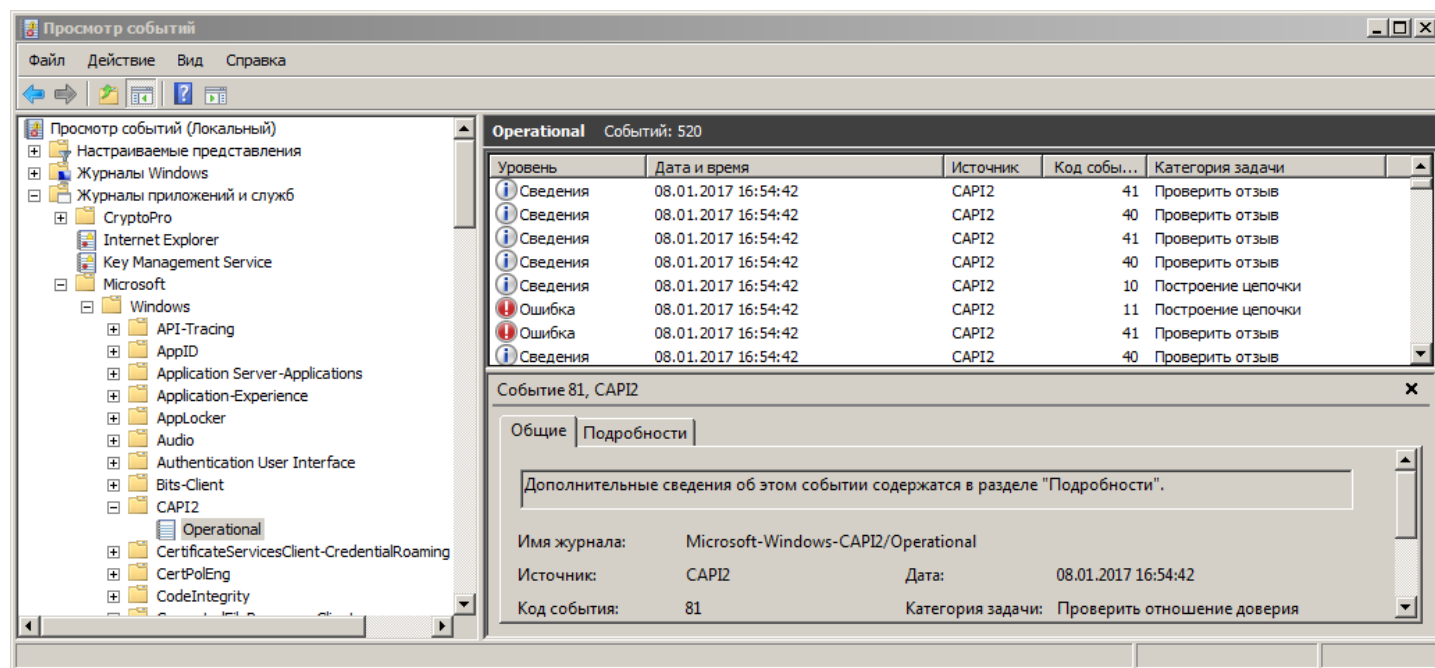
Журналы Windows

Основным средством диагностики Сервиса Проверки Подписи являются журналы Windows. При создании экземпляра службы регистрируются два журнала: Admin и Operational. Журнал Admin предназначен для администраторов Сервиса Проверки Подписи. Журнал Operational предназначен для сбора журналов Сервиса Проверки Подписи при диагностике и исправлении сложных ошибок.

Ошибки на ранних стадиях запуска Сервиса Проверки Подписи могут быть записаны в журнал Приложений (Applications). Обычно источниками событий при ошибках запуска веб-приложения являются **ASP.NET 4.0.30319.0** и **System.ServiceModel 4.0.0.0**.



Для диагностики ошибок построения цепочек сертификатов, проверки статусов сертификатов можно использовать журнал CAPI2. Для начала работы с журналом его требуется включить. Для включения журнала щёлкните по нему правой кнопкой мыши и выберите пункт "Включить журнал" в контекстном меню. После устранения ошибки аналогичным образом отключите журнал.



Диагностика ошибок при проверке подписи форматов CAdES

Если информационных сообщений сервиса и журналов Windows недостаточно для устранения ошибок при проверке подписи формата CAdES, то необходимо включить трассировку. Для включения трассировки выполните следующие действия:

- Установите утилиту [DbgView](#)
- Создайте 2 файла с расширением `.reg` и содержимым, как указано ниже.

CPTTrace.reg:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Trace]
"reprov.dll"=""
"cades.dll"=""
"ocspcli.dll"=""
"ocsp.exe"=""
"tspcli.dll"=""
"tsp.exe"=""
"pkivalidator.dll"=""
"ProcessFlags"=dword:00000002
```

CPTTrace(x64).reg:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Crypto Pro\Trace]
"reprov.dll"=""
"cades.dll"=""
"ocspcli.dll"=""
"ocsp.exe"=""
"tspcli.dll"=""
"tsp.exe"=""
"pkivalidator.dll"=""
"ProcessFlags"=dword:00000002
```

- Установите созданные файлы. Для установки дважды щелкните по ним, в открывшемся окне подтвердите установку ключа Реестра Windows.
- Перезапустите IIS.
- Запустите утилиту DbgView с правами администратора
- Воспроизведите ошибку.

После завершения диагностики необходимо отключить трассировку CAdES. Для отключения трассировки создайте файл с расширением `.reg` и содержимым, как указано ниже:

CPTTrace.un.reg:

```
Windows Registry Editor Version 5.00

[-HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Trace]

[-HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Crypto Pro\Trace]
```

Установите созданный файл. Для установки дважды щелкните по нему, в открывшемся окне подтвердите установку ключа Реестра Windows. Перезапустите IIS.

Журналирование сетевых взаимодействий

Внимание!

Настройки, приведенные в данном разделе, не могут быть выполнены в ОС CH Astra Linux Special Edition.

Сервис Проверки Подписи позволяет вести журналирование и протоколирование сообщений, которыми обмениваются веб-клиент и веб-служба Сервиса Проверки Подписи.

Журналирование используется для вывода информации о потоке выполнения и отдельных действий различных компонентов распределенного приложения. Механизм протоколирования сообщений, в свою очередь, предназначен для сохранения содержимого сообщений, которыми обмениваются веб-клиент и веб-служба.

В Сервисе Проверки Подписи возможности журналирования предоставляются технологией Windows Communication Foundation (WCF). Основными источниками журналирования WCF являются **System.ServiceModel** и **System.ServiceModel.MessageLogging**. Источник журналирования **System.ServiceModel** — наиболее общий источник журналирования WCF, записывающий основные этапы приложения по всему стеку связи WCF: от входа и выхода из транспорта до входа и выхода из пользовательского кода. Источник журналирования **System.ServiceModel.MessageLogging** записывает все сообщения, проходящие через систему.

Сервис Проверки Подписи позволяет настроить журналирование из вышеуказанных источников отдельно для каждого из своих компонентов. Для каждого из источников журналирования можно настроить уровень журналирования и путь к файлу, в который будет записываться журнал. Файлы журналов имеют расширение `.svclog`, и для просмотра таких файлов используется программа `SvcTraceViewer.exe`.

Настройка журналирования осуществляется с помощью командлетов, входящих в состав модуля **CryptoPro.DSS.PowerShell.VS**.

Командлеты журналирования

Список командлетов журналирования:

- [Get-VsTracing](#)
- [Set-VsTracing](#)
- [Enable-VsTracing](#)
- [Disable-VsTracing](#)

Командлет Get-VsTracing

Командлет Get-VsTracing позволяет вывести на экран значения параметров журналирования Сервиса Проверки Подписи.

Синтаксис:

```
Get-VsTracing [-DisplayName <string>]
```

Командлет Set-VsTracing

Командлет Set-VsTracing позволяет установить значения параметров журналирования Сервиса Проверки Подписи.

Синтаксис:

```
Set-VsTracing
[-ServiceModelListenerLogFile <string>]
[-ServiceModelListenerSourceLevel <SourceLevels> {Off | Critical | Error | Warning | Information | Verbose |
ActivityTracing | All}]
[-ServiceModelListenerMaxLogFileSize <int>]
[-ServiceModelListenerCircularFilesCount <int>]
[-ServiceModelMessageLoggingListenerLogFile <string>]
[-ServiceModelMessageLoggingListenerSourceLevel <SourceLevels> {Off | Critical | Error | Warning | Information
| Verbose | ActivityTracing | All}]
[-ServiceModelMessageLoggingListenerMaxLogFileSize <int>]
[-ServiceModelMessageLoggingListenerCircularFilesCount <int>]
[-DisplayName <string>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
DisplayName	string	Отображаемое имя экземпляра компонента Сервера Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
ServiceModelListenerLogFile	string	Путь к файлу журнала из источника ServiceModel.
ServiceModelListenerSourceLevel	SourceLevels	Уровень журналирования из источника ServiceModel.
ServiceModelListenerMaxLogFileSize	int	Максимальный размер файла журнала из источника ServiceModel (в байтах). Размер файла журнала может принимать значение от ~5Mb до ~50Mb.
ServiceModelMessageLoggingListenerCircularFilesCount	int	Максимальное количество создаваемых файлов журналов от источника ServiceModelMessageLogging. Если значение выставлено в 0, то количество создаваемых файлов журналов не ограничено.
ServiceModelListenerCircularFilesCount	int	Максимальное количество создаваемых файлов журналов от источника ServiceModel. Если значение выставлено в 0, то количество создаваемых файлов журналов не ограничено.
ServiceModelMessageLoggingListenerLogFile	string	Путь к файлу журнала из источника ServiceModelMessageLogging.
ServiceModelMessageLoggingListenerSourceLevel	SourceLevels	Уровень журналирования из источника ServiceModelMessageLogging.
ServiceModelMessageLoggingListenerMaxLogFileSize	int	Максимальный размер файла журнала из источника ServiceModelMessageLogging (в байтах). Размер файла журнала может принимать значение от ~5Mb до ~50Mb.

SourceLevels — перечисление уровней журналирования, принимающее значения All, Off, Critical, Error, Warning, Information, Verbose, ActivityTracing. Более подробную информацию о данном перечислении можно узнать на сайте [MSDN](#).

Параметры **ServiceModelListenerCircularFilesCount** и **ServiceModelMessageLoggingListenerCircularFilesCount** определяют количество создаваемых файлов журналов. Значение «0» данных параметров означает отсутствие ограничения на количество создаваемых файлов журналов. По достижению максимального размера файла (определяется параметрами **ServiceModelMessageLoggingListenerMaxLogFileSize** и **ServiceModelListenerMaxLogFileSize**) будет создан новый файл, в который в дальнейшем будет продолжаться запись журнала. При достижении максимального количества файлов журналов запись вновь начнётся с первого файла.

Примечание

К моменту включения журналирования каталог для записи файлов журналов должен существовать. В противном случае при запуске Сервиса Проверки Подписи произойдет критическая ошибка.

Учётной записи Сервиса Проверки Подписи требуется выдать права на запись в указанный каталог.

Командлет Enable-VsTracing

Командлет Enable-VsTracing активирует журналирование Сервиса Проверки Подписи.

Синтаксис:

```
Enable-VsTracing [-DisplayName <string>]
```

Командлет Disable-VsTracing

Командлет Enable-VsTracing деактивирует журналирование Сервиса Проверки Подписи.

Синтаксис:

```
Disable-VsTracing [-DisplayName <string>]
```

Пример настройки журналирования SVS

Данный сценарий задаёт настройку журналирования Сервиса Проверки Подписи.

```
# Настройка параметров журналирования
Set-VsTracing -ServiceModelListenerLogFile "C:\VsLogs\vs_trace.svclog" -ServiceModelListenerSourceLevel All -
ServiceModelListenerMaxLogFileSize 10000000 -ServiceModelMessageLoggingListenerLogFile
"C:\VsLogs\vs_msg.svclog" -ServiceModelMessageLoggingListenerSourceLevel All -
ServiceModelMessageLoggingListenerMaxLogFileSize 10000000 -ServiceModelListenerCircularFilesCount 10 -
ServiceModelMessageLoggingListenerCircularFilesCount 10

# Включение журналирования
Enable-VsTracing
```

Командлет Add-VsCertificateVerifierPlugin

Регистрирует новый плагин проверки сертификата.

Синтаксис:

```
Add-VsCertificateVerifierPlugin -Assembly <string> [-DisplayName <string>] [-Classname <string>] [-CheckByDefaultRequired <bool>] [-PluginDescription <string>] [-Parameters <hashtable>]
```

Пример:

```
# Windows
Add-VsCertificateVerifierPlugin -Assembly SVS.CertificateVerifier.Qualified.dll -PluginDescription "Проверка сертификата на соответствие установленной форме" -Parameters @{'TSLPath'='C:\TSL.xml'}

# *nix
Add-VsCertificateVerifierPlugin -Assembly
CryptoPro.Plugins.VerificationService.CertificateVerifier.Qualified.dll -PluginDescription "Проверка сертификата на соответствие установленной форме" -Parameters @{'TSLPath'='/path_to/TSL.xml'}
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
Assembly	string	Полный путь до файла со сборкой плагина. В качестве значения данного параметра можно указать полный путь до файла со сборкой, либо только имя dll-файла сборки, если плагин находится в следующей директории: <Путь установки>\Plugins\CertificatesVerifiers. Для регистрации плагина проверки сертификата на соответствие установленной форме в данном параметре нужно указать следующее значение: Windows - SVS.CertificateVerifier.Qualified.dll, *nix - CryptoPro.Plugins.VerificationService.CertificateVerifier.Qualified.dll.
CheckByDefaultRequired	bool	Использовать ли по умолчанию плагин для проверки сертификата. Параметр используется только при работе через REST API Сервиса Проверки Подписи. При этом значение CertVerifiersPluginsIds должно быть равным NULL или не указано в запросе к REST API (см. ЖТЯИ.00094-03 94 03. ПАК Службы УЦ 2.0. КриптоПро SVS. Руководство разработчика).
Classname	string	Имя класса, который реализует интерфейс ISVSCertificateVerifier.
DisplayName	string	Отображаемое имя экземпляра Сервиса Проверки Подписи.
Parameters	hashtable	Дополнительные настройки плагина. Параметр зарезервирован для использования в будущем.
PluginDescription	string	Описание плагина, которое отображается на Веб-интерфейсе Сервиса Проверки Подписи. Если не указано, используется значение, заданное в плагине.

Командлет Add-VsConverterPlugin

Регистрация нового плагина для преобразования документов.

Синтаксис:

```
Add-VsConverterPlugin [-DisplayName <string>] -FileExtension <string> -Assembly <string> [-Classname <string>] [-Priority <int>] [-Parameters <Hashtable>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
Assembly	string	Полный путь до файла сборки плагина. В качестве значения данного параметра можно указать только имя файла сборки, в этом случае полный путь будет отсчитываться относительно директории: <Путь установки>\Plugins\Converters\<Тип плагина>.
Classname	string	Имя класса, реализующего интерфейс IDSSDocumentConverter.
DisplayName	string	Имя экземпляра Сервиса Проверки Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
FileExtension	string	Расширение документа.
Parameters	Hashtable	Дополнительные параметры плагина.
Priority	int	Приоритет плагина относительно остальных зарегистрированных для данного расширения плагинов.

В PowerShell для задания параметра типа Hashtable можно применить следующую конструкцию:

```
@{paramName1=paramValue1; paramName2=paramValue2;...;paramNameN=paramValueN}
```

где paramName?, paramValue? – название и значение параметра соответственно.

Пример регистрации предустановленных плагинов для отображения документов

Командлет Add-VsQualifiedCATHumbprint

Добавляет отпечаток сертификата, выданного аккредитованным УЦ.

Синтаксис:

```
Add-VsQualifiedCATHumbprint -Identifier <string> [-DisplayName <string>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
Thumbprint	string	Отпечаток сертификата.
DisplayName	string	Отображаемое имя экземпляра Сервиса Проверки Подписи.

Командлет Add-VsTransformPlugin

Регистрирует пользовательское XML-преобразование на Сервисе Проверки Подписи.

Синтаксис:

```
Add-VsTransformPlugin -Assembly <string> -Identifiers <string[]> [-DisplayName <string>] [-Classname <string>]
```

Пример (ОС *nix):

```
#Преобразование для ФТС
Add-VsTransformPlugin -Assembly CryptoPro.Plugins.Xml.Transforms.dll -Classname
CryptoPro.Plugins.Xml.Transforms.XmlFssTransform -Identifiers "urn:xml-dsig:transformation:v1.1"

#Преобразование XML-Signature XPath Filter 2.0
Add-VsTransformPlugin -Assembly CryptoPro.Plugins.Xml.Transforms.dll -Classname
CryptoPro.Plugins.Xml.Transforms.Filter2SubstractTransform -Identifiers "http://www.w3.org/2002/06/xmldsig-
filter2"
```

Пример (ОС Windows):

```
#Преобразование для ФТС
Add-VsTransformPlugin -Assembly CryptoPro.DSS.Xml.Transforms.dll -Classname
CryptoPro.DSS.Xml.Transforms.XmlFssTransform -Identifiers "urn:xml-dsig:transformation:v1.1"

#Преобразование XML-Signature XPath Filter 2.0
Add-VsTransformPlugin -Assembly CryptoPro.DSS.Xml.Transforms.dll -Classname
CryptoPro.DSS.Xml.Transforms.Filter2SubstractTransform -Identifiers "http://www.w3.org/2002/06/xmldsig-
filter2"
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
Assembly	string	Полный путь до файла со сборкой плагина. В качестве значения данного параметра можно указать полный путь до файла со сборкой, либо только имя dll-файла сборки, если плагин находится в следующей директории: <Путь установки>\Plugins\Transforms
Classname	string	Имя класса с реализацией XML-преобразования.
DisplayName	string	Отображаемое имя экземпляра Сервиса Проверки Подписи.
Identifiers	string[]	Список идентификаторов регистрируемого преобразования.

Командлет Disable-VsEndpoint

Используется для отключения конечных точек Сервиса Проверки Подписи.

Внимание!
Командлет не используется в ОС CH Astra Linux Special Edition.

Синтаксис

```
Disable-VsEndpoint -Name <string> [-DisplayName <string>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
DisplayName	string	Имя экземпляра . Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Name	string	Имя конечной точки.

Командлет Disable-VsTracing

Командлет Enable-VsTracing деактивирует журналирование Сервиса Проверки Подписи.

Внимание!

Командлет не используется в ОС CH Astra Linux Special Edition.

Синтаксис:

```
Disable-VsTracing [-DisplayName <string>]
```

Командлет Enable-VsEndpoint

Используется для включения конечных точек Сервиса Проверки Подписи.

Внимание!
Командлет не используется в ОС CH Astra Linux Special Edition.

Синтаксис

```
Enable-VsEndpoint -Name <string> [-DisplayName <string>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
DisplayName	string	Имя экземпляра . Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Name	string	Имя конечной точки.

Командлет Enable-VsTracing

Командлет Enable-VsTracing активирует журналирование Сервиса Проверки Подписи.

Внимание!

Командлет не используется в ОС CH Astra Linux Special Edition.

Синтаксис:

```
Enable-VsTracing [-DisplayName <string>]
```

Командлет Get-VsCertificateVerifierPlugin

Позволяет получить информацию о зарегистрированных плагинах проверки формата сертификата. Может принимать на вход только имя экземпляра SVS, для которого необходимо вывести информацию о плагинах проверки сертификатов.

Синтаксис:

```
Get-VsCertificateVerifierPlugin [-DisplayName <string>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
DisplayName	string	Имя экземпляра Сервиса Проверки Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.

Командлет Get-VsConverterPlugin

Данный командлет используется для вывода на консоль всех зарегистрированных плагинов для преобразования документов.

Синтаксис:

```
Get-VsConverterPlugin [-DisplayName <string>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
DisplayName	string	Имя экземпляра Сервиса Проверки Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
FileExtension	string	Расширение документа (будут отображены только плагины, зарегистрированные с этим расширением).

Командлет Get-VsCustomization

Данный командлет используется для вывода на консоль всех настроек отображения Веб-интерфейса Сервиса Проверки Подписи.

Внимание!

Командлет не используется в ОС CH Astra Linux Special Edition.

Синтаксис:

```
Get-VsCustomization [-DisplayName <string>]
```

Командлет Get-VsEndpoint

Используется для вывода на консоль информации о конечных точках Сервиса Проверки Подписи.

Внимание!

Командлет не используется в ОС CH Astra Linux Special Edition.

Синтаксис

```
Get-VsEndpoint [-DisplayName <string>]
```

Командлет Get-VsEndpointGlobalSettings

Используется для вывода на консоль общих настроек конечных точек Сервиса Проверки Подписи.

Внимание!

Командлет не используется в ОС CH Astra Linux Special Edition.

Синтаксис

```
Get-VsEndpointGlobalSettings [-DisplayName <string>]
```

Командлет Get-VsInstance

Командлет выводит на консоль список созданных экземпляров Сервиса Проверки Подписи.

Синтаксис:

```
Get-VsInstance [-DisplayName <string>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
DisplayName	string	Имя экземпляра Сервиса Проверки Подписи. Если значение не указано, будут отображены все экземпляры.

Командлет Get-VsLicense

Выводит на консоль информацию о лицензии Сервиса Проверки Подписи.

Синтаксис:

```
Get-VsLicense [-DisplayName <string>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
DisplayName	string	Имя экземпляра Сервиса Проверки Подписи. Если значение не указано, будет отображена информация о лицензии экземпляра по умолчанию.

Командлет Get-VsProperties

Командлет Get-VsProperties позволяет отобразить основные параметры Сервиса Проверки Подписи.

Синтаксис:

```
Get-VsProperties [-DisplayName <string>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
DisplayName	string	Имя экземпляра Сервиса Проверки Подписи. Если значение не указано, будут отображены параметры экземпляра по умолчанию.

Командлет Get-VsQualifiedCATHumbprint

Получает сведения о заданных отпечатках сертификатов.

Синтаксис:

```
Get-VsQualifiedCATHumbprint -Identifier <string> [-DisplayName <string>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
DisplayName	string	Имя экземпляра Сервиса Проверки Подписи. Если значение не указано, будут отображены параметры экземпляра по умолчанию.

Командлет Get-VsSignatureFormat

Выводит на консоль настройки поддерживаемых для проверки форматов подписи.

Синтаксис:

```
Get-VsSignatureFormat [-DisplayName <string>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
DisplayName	string	Имя экземпляра Сервиса Проверки Подписи. Если значение не указано, будут отображены параметры экземпляра по умолчанию.

Командлет Get-VsTracing

Командлет Get-VsTracing позволяет вывести на экран значения параметров журналирования Сервиса Проверки Подписи.

Внимание!

Командлет не используется в ОС CH Astra Linux Special Edition.

Синтаксис:

```
Get-VsTracing [-DisplayName <string>]
```

Командлет Get-VsTransformPlugin

Выводит на консоль список зарегистрированных на Сервисе Проверки Подписи пользовательских XML-преобразований.

Синтаксис:

```
Get-VsTransformPlugin [-Identifier <string>] [-DisplayName <string>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
Identifier	string	Если задано, выводит на консоль информацию о пользовательском преобразовании, зарегистрированном с переданным идентификатором.
DisplayName	string	Отображаемое имя экземпляра Сервиса Проверки Подписи.

Командлет Add-VsInstance/New-VsInstance

Создает новый экземпляр Сервиса Проверки Подписи.

К основным параметрам относятся:

- название веб-сайта IIS, на котором следует развернуть веб-приложение Сервиса Проверки Подписи;
- отображаемое имя экземпляра Сервиса Проверки Подписи.

Примечание

Начиная с версии КриптоПро SVS 3.0 рекомендуется использовать имя командлета Add-VsInstance.

Синтаксис:

```
Add-VsInstance -SiteName <string> -DisplayName <string> [-ApplicationName <string>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
ApplicatonName	string	Название веб-приложения Сервиса Проверки Подписи. Если параметр не задан, используется значение vs.
DisplayName	string	Отображаемое имя экземпляра Сервиса Проверки Подписи.
ListenPort	int	Порт, который прослушивает КриптоПро SVS (параметр используется только в *nix-системах).
SiteName	string	Название веб-сайта, на котором следует развернуть веб-приложение Сервиса Проверки Подписи.
ServiceAccountName	string	Имя учетной записи, под которой работает Сервис Проверки Подписи (параметр используется только в *nix-системах).

Пример:

```
Add-VsInstance -DisplayName SVS -ApplicationName verify -SiteName "Default Web Site"
```

Данная команда разворачивает экземпляр Сервиса Проверки Подписи на веб-сайте IIS по умолчанию, создает хранилища сертификатов с именем **verify-TSL** и **verify-CA** для локального компьютера.

Пользователи могут обратиться к веб-интерфейсу Сервиса Проверки Подписи по адресу: `http://<hostname>/verify/` (см. примечание ниже). Программный интерфейс Сервиса Проверки Подписи будет доступен по адресу: `http://<hostname>/verify/rest/api`.

Примечание

Если используется Сервис Проверки Подписи версии ниже, чем 2.0.2636, программный интерфейс Сервиса Проверки Подписи будет доступен по адресу: `http://<hostname>/verify/service.svc`.

Примечание

Если используется Сервис Проверки Подписи версии ниже, чем 3.0, для работы Веб-интерфейса требуется создание и настройка **отдельного экземпляра** Веб-интерфейса SVS.

Командлет New-VsLicense

Задаёт временную или новую лицензию Сервиса Проверки Подписи.

Синтаксис:

```
New-VsLicense [-DisplayName <string>] [-SN <string>] [-CompanyName <string>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
CompanyName	string	Наименование организации
DisplayName	string	Отображаемое имя экземпляра Сервиса Проверки Подписи.
SN	string	Лицензия

Примечание

При вызове команды без параметров активируется временная лицензия на 3 месяца.

Примечание

Вызов командлета необходим при создании каждого нового экземпляра Сервиса Проверки Подписи.

Командлет Remove-VsCertificateVerifierPlugin

Удаляет зарегистрированный ранее плагин проверки сертификата.

Синтаксис:

```
Remove-VsCertificateVerifierPlugin -Assembly <string> [-DisplayName <string>] [-Classname <string>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
ID	int	Идентификатор плагина.
DisplayName	string	Отображаемое имя экземпляра Сервиса Проверки Подписи.

Командлет Remove-VsConverterPlugin

Удаление зарегистрированного плагина для преобразования.

Синтаксис:

```
Remove-VsConverterPlugin [-DisplayName <string>] -FileExtension <string> -Assembly <string> -Classname <string>
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
Assembly	string	Полный путь до файла сборки плагина. В качестве значения данного параметра можно указать только имя файла сборки, в этом случае полный путь будет отсчитываться относительно директории: <Путь установки>\Plugins\Converters\<Тип плагина>.
Classname	string	Имя класса, реализующего интерфейс IDSSDocumentConverter.
DisplayName	string	Имя экземпляра Сервиса Проверки Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
FileExtension	string	Расширение документа.

Командлет Remove-VsInstance

Удаляет созданный экземпляр Сервиса Проверки Подписи.

Синтаксис:

```
Remove-VsInstance [-DisplayName <string>]
```

Примечание

В ОС Windows при удалении экземпляра Сервиса Проверки Подписи будут удалены хранилища сертификатов, созданные при разворачивании экземпляра.

ПАРАМЕТР	ТИП	ОПИСАНИЕ
DisplayName	string	Имя экземпляра Сервиса Проверки Подписи. Если значение не указано, будет удален экземпляр по умолчанию.

Командлет Remove-VsQualifiedCATHumbprint

Удаляет отпечаток сертификата, выданного аккредитованным УЦ.

Синтаксис:

```
Remove-VsQualifiedCATHumbprint -Identifier <string> [-DisplayName <string>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
ClearAll	switch	Флаг, наличие которого удаляет все заданные отпечатки сертификатов.
DisplayName	string	Отображаемое имя экземпляра Сервиса Проверки Подписи.
Thumbprint	string	Отпечаток сертификата.

Командлет Remove-VsTransformPlugin

Удаляет ранее зарегистрированное пользовательское преобразование с Сервиса Проверки Подписи.

Синтаксис:

```
Remove-VsTransformPlugin -Identifier <string> [-DisplayName <string>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
Identifier	string	Идентификатор удаляемого преобразования.
DisplayName	string	Отображаемое имя экземпляра Сервиса Проверки Подписи.

Командлет Reset-VsCustomization

Данный командлет используется для восстановления настроек по умолчанию отображения Веб-интерфейса Сервиса Проверки Подписи.

Внимание!

Командлет не используется в ОС CH Astra Linux Special Edition.

Синтаксис:

```
Reset-VsCustomization [-DisplayName <string>]
```

Командлет Restart-VsInstance

Перезапускает пул приложения SVS.

Внимание!

Командлет не используется в ОС CH Astra Linux Special Edition.

Синтаксис:

```
Restart-VsInstance -DisplayName <string>
```

Командлет Set-VsCertificateVerifierPlugin

Позволяет настроить плагин проверки формата сертификата. Командлет может принимать на вход объект в режиме конвейера.

Синтаксис:

```
Set-VsCertificateVerifierPlugin -ID <int> [-DisplayName <string>] [-CheckByDefaultRequired <bool>] [-PluginDescription <string>] [-Parameters <Hashtable>] [-OverrideParameters]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
DisplayName	string	Отображаемое имя экземпляра Сервиса Проверки Подписи.
CheckByDefaultRequired	bool	Использовать ли по умолчанию плагин для проверки сертификата. Параметр используется только при работе через REST API Сервиса Проверки Подписи. При этом значение CertVerifiersPluginsIds должно быть равным NULL или не указано в запросе к REST API.
ID	int	Идентификатор плагина.
OverrideParameters	bool	Наличие этого параметра определяет, перезаписывать ли текущие настройки при следующем вводе параметров (только добавить новую информацию или перезаписать параметры полностью).
Parameters	hashtable	Дополнительные настройки плагина. Параметр зарезервирован для использования в будущем.
PluginDescription	string	Описание плагина, которое отображается на Веб-интерфейсе Сервиса Проверки Подписи. Если не указано, используется значение, заданное в плагине.

Командлет Set-VsConverterPlugin

Изменение параметров плагина для преобразования документов.

Синтаксис:

```
Set-VsConverterPlugin [-DisplayName <string>] -FileExtension <string> -Assembly <string> [-Classname <string>] [-Parameters <Hashtable>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
Assembly	string	Полный путь до файла сборки плагина. В качестве значения данного параметра можно указать только имя файла сборки, в этом случае полный путь будет отсчитываться относительно директории: <Путь установки>\Plugins\Converters\<Тип плагина>.
Classname	string	Имя класса, реализующего интерфейс IDSSDocumentConverter.
DisplayName	string	Имя экземпляра Сервиса Проверки Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
FileExtension	string	Расширение документа.
Override	bool	Наличие этого параметра определяет, перезаписывать ли текущие настройки при следующем вводе параметров (только добавить новую информацию или перезаписать параметры полностью).
Parameters	Hashtable	Дополнительные параметры плагина.

В PowerShell для задания параметра типа Hashtable можно применить следующую конструкцию:

```
@{paramName1=paramValue1; paramName2=paramValue2;...;paramNameN=paramValueN}
```

где paramName?, paramValue? – название и значение параметра соответственно.

Пример регистрации предустановленных плагинов для отображения документов

Командлет Set-VsCustomization

Данный командлет используется для изменения настроек отображения Веб-интерфейса Сервиса Проверки Подписи.

Внимание!

Командлет не используется в ОС CH Astra Linux Special Edition.

Синтаксис:

```
Set-VsCustomization [-DisplayName <string>] [-Title <string>] [-Copyright <string>] [-LogotypeFile <string>] [-HelpFile <string>] [-MainColor <string>] [-AdditionalColor <string>] [-FontColor <string>] [-Font <string>] [-FavIconFile <string>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
DisplayName	string	Имя экземпляра Сервиса Проверки Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Title	string	Заголовок веб-приложения.
Copyright	string	Копирайт.
LogotypeFile	string	Полный путь до файла с логотипом. Размер логотипа – максимум 55 pix высоты и 220 pix в ширину.
HelpFile	string	Полный путь до файла со справкой. Файл справки представляет собой HTML-документ. Внимание! Параметр не используется.
MainColor	string	Основной цвет интерфейса веб-приложения (меню, выделенные кнопки). Цвет задается в формате HEX.
AdditionalColor	string	Дополнительный цвет интерфейса веб-приложения (выделенный элемент меню, выпадающий список под учетной записью). Цвет задается в формате HEX.
FontColor	string	Цвет шрифта заголовка, пунктов меню. Цвет задается в формате HEX.
Font	string	Тип шрифта.
FavIconFile	string	Полный путь до файла с favicon. Допустимое расширение для файла – ico.

Пример настройки кастомизации Веб-интерфейса SVS:

```
Set-VsCustomization -AdditionalColor f37c20 -MainColor 02458d
Set-VsCustomization -FontColor f37c20 -Font Calibri
Set-VsCustomization -FavIconFile E:\Temp\favicon.ico -LogotypeFile E:\Temp\logo.jpg
Set-VsCustomization -Title "Сервер электронной подписи Тест" -Copyright "Тест"
```



Переместите документ(-ы) или нажмите, чтобы выбрать.

Командлет Set-VsEndpointGlobalSettings

Используется для изменения общих настроек конечных точек Сервиса Проверки Подписи.

Внимание!

Командлет не используется в ОС CH Astra Linux Special Edition.

Синтаксис

```
Set-VsEndpointGlobalSettings [-MaxRecieveTimeOut <int>] [-MaxSendTimeOut <int>] [-MaxMessageSize <int>] [-
DisplayName <string>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
DisplayName	string	Имя экземпляра Сервиса Проверки Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
MaxRecieveTimeOut	int	Максимальное время получения сообщения в секундах. По умолчанию равен 30 секунд.
MaxSendTimeOut	int	Максимальное время отправки сообщения в секундах. По умолчанию равен 30 секунд.
MaxMessageSize	int	Максимальный размер сообщения в байтах. По умолчанию равен 5Mb.

Командлет Set-VsProperties

Командлет Set-VsProperties позволяет задать основные параметры Сервиса Проверки Подписи.

Синтаксис:

```
Set-VsProperties [-RevocationMode <string> {NoCheck | Online | Offline}] [-RevocationFlags <string> {EndCertificateOnly | EntireChain | ExcludeRoot}] [-UrlRetrievalTimeOut <uint32>] [-DisplayName <string>]] - CadesUseOcspAuthorizedPolicy <bool>
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
AllowedCorsOrigins	string	Список допустимых источников запросов (адресов, конечных точек и т.д.) к API SVS для протокола CORS (возможно указание нескольких имен через запятую). Например, переменная(-ые) server_name из контекста server, соответствующего Веб-интерфейсу SVS, файла конфигурации /etc/nginx/nginx.conf.
CadesUseOcspAuthorizedPolicy	bool	Разрешает использование групповой политики КриптоПро OCSP Client "Службы OCSP: сертификаты уполномоченных служб OCSP" при проверке полномочий службы актуальных статусов.
CadesUseProxy	bool	Флаг, позволяющий получить\запретить настройки прокси-сервера из Internet Explorer. По умолчанию имеет значение true (Прокси-сервер, настроенный в Internet Explorer, НЕ используется). Параметр используется только в ОС Windows.
DisplayName	string	Отображаемое имя экземпляра Сервиса Проверки Подписи.
RevocationFlags	string Допустимые значения: EndCertificateOnly EntireChain ExcludeRoot	Режим проверки цепочки сертификатов. EndCertificateOnly – проверка статуса делается только для конечного сертификата в цепочке. EntireChain – проверка статуса делается для всех сертификатов в цепочке. ExcludeRoot – проверка статуса делается для всех сертификатов в цепочке, кроме корневого.
RevocationMode	string Допустимые значения: NoCheck Online Offline	Режим проверки статуса сертификата. NoCheck – статус сертификатов не проверяется. Offline – статусы сертификатов проверяются по кэшированным CRL. Online – аналогичен режиму Offline, но в случае истечения срока действия CRL будет сделана попытка скачать актуальный CRL.
SessionTimeout		Максимальное время простоя (отсутствия действий пользователя) на Веб-интерфейсе SVS в минутах
UrlRetrievalTimeOut	int	Максимальное время скачивания объектов по сети. Если задано значение 0, то время скачивания не ограничено. Значение указывается в секундах.
WordFilePath	string	Путь к файлу шаблона-контейнера отчета .
XsltFilePath	string	Путь к файлу шаблона результатов проверки .

ПАРАМЕТР	ТИП	ОПИСАНИЕ
IncludeCertPluginErrorInfoInMainError	bool	Флаг, указывающий, влияют ли дополнительные проверки сертификата (при помощи дополнительных плагинов) на итоговый результат проверки. Если данный флаг взведен, непрошедший дополнительную проверку сертификат получит общий статус "Недействителен", даже если основные проверки были успешно пройдены.
AllowCRLEvidenceForXLT1	bool	Флаг, показывающий, что разрешено использовать CRL как доказательство действительности сертификата (вместо ответа службы OCSP) в подписи формата CAdES XLT1.
VsAddress	string	Адрес REST-интерфейса SVS в формате <code>https\hostname>/<ApplicationName>/rest</code> . Параметр используется только в ОС Windows.

Примечание

Параметр `-RevocationMode` **не учитывается** при проверке подписи формата CAdES X Long Type 1. В случае проверки данного формата подписи всегда выполняется проверка статуса сертификата.

Пример:

```
Set-VsProperties -RevocationMode Offline -RevocationFlags EndCertificateOnly
```

Данная команда задаёт режим проверки статуса сертификатов - по локально сохраненному CRL и проверку только конечного сертификата в цепочке сертификации.

Командлет Set-VsSignatureFormat

Задаёт настройки поддерживаемых для проверки форматов подписи.

Синтаксис:

```
Set-VsSignatureFormat -Format <string> {XMLDSig | CMS | MSOffice | PDF | GOST3410} [-IsEnabled <bool>] [-Extensions <List[string]>] [-DisplayName <string>]]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
DisplayName	string	Имя экземпляра Сервиса Проверки Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
Extensions	List[string]	Список расширений файлов, связанных с данным форматом. По умолчанию зарегистрированы следующие расширения: * pdf - для формата PDF; * docx - для формата docx; * xml - для XML-документов; * sig, * - для CMS-подписи (включая CAdES); * * - для необработанной подписи ГОСТ Р 34.10-2012.
Format	string Допустимые значения: XMLDSig, GOST3410, MSOffice, PDF, CMS.	Форматы подписи, которые будут доступны в веб-интерфейсе и веб-сервисе для проверки. По умолчанию доступны все указанные форматы подписи.
IsEnabled	bool	Включить/отключить формат подписи.

Примечание
Для проверки ЭП формата CAdES необходимо использовать параметр CMS.

Форматы подписи, для которых значение параметра IsEnabled выставлено в false, не будут отображаться в веб-интерфейсе пользователя и не будут доступны для проверки через веб-сервис.

Через параметр Extensions можно задать список расширений файлов, связанных с каждым из форматов подписи. Настройка будет применяться на веб-интерфейсе сервиса проверки для определения подходящего формата подписи для проверки.

Пример

```
Set-VsSignatureFormat -Format CMS -Extensions sig, p7b, p7s
```

Если формат подписи не связан с определённым расширением файла, то в списке расширений нужно указать wildcard (*).

Пример

```
Set-VsSignatureFormat -Format GOST3410 -Extensions *
```

Командлет Set-VsTracing

Командлет Set-VsTracing позволяет установить значения параметров журналирования Сервиса Проверки Подписи.

Внимание!

Командлет не используется в ОС CH Astra Linux Special Edition.

Синтаксис:

```
Set-VsTracing
[-ServiceModelListenerLogFile <string>]
[-ServiceModelListenerSourceLevel <SourceLevels> {Off | Critical | Error | Warning | Information | Verbose | ActivityTracing | All}]
[-ServiceModelListenerMaxLogFileSize <int>]
[-ServiceModelListenerCircularFilesCount <int>]
[-ServiceModelMessageLoggingListenerLogFile <string>]
[-ServiceModelMessageLoggingListenerSourceLevel <SourceLevels> {Off | Critical | Error | Warning | Information | Verbose | ActivityTracing | All}]
[-ServiceModelMessageLoggingListenerMaxLogFileSize <int>]
[-ServiceModelMessageLoggingListenerCircularFilesCount <int>]
[-DisplayName <string>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
DisplayName	string	Отображаемое имя экземпляра компонента Сервера Подписи. Если значение не указано, будет использован экземпляр, назначенный по умолчанию.
ServiceModelListenerLogFile	string	Путь к файлу журнала из источника ServiceModel.
ServiceModelListenerSourceLevel	SourceLevels	Уровень журналирования из источника ServiceModel.
ServiceModelListenerMaxLogFileSize	int	Максимальный размер файла журнала из источника ServiceModel (в байтах). Размер файла журнала может принимать значение от ~5Mb до ~50Mb.
ServiceModelMessageLoggingListenerCircularFilesCount	int	Максимальное количество создаваемых файлов журналов от источника ServiceModelMessageLogging. Если значение выставлено в 0, то количество создаваемых файлов журналов не ограничено.
ServiceModelListenerCircularFilesCount	int	Максимальное количество создаваемых файлов журналов от источника ServiceModel. Если значение выставлено в 0, то количество создаваемых файлов журналов не ограничено.
ServiceModelMessageLoggingListenerLogFile	string	Путь к файлу журнала из источника ServiceModelMessageLogging.
ServiceModelMessageLoggingListenerSourceLevel	SourceLevels	Уровень журналирования из источника ServiceModelMessageLogging.
ServiceModelMessageLoggingListenerMaxLogFileSize	int	Максимальный размер файла журнала из источника ServiceModelMessageLogging (в байтах). Размер файла журнала может принимать значение от ~5Mb до ~50Mb.

SourceLevels — перечисление уровней журналирования, принимающее значения All, Off, Critical, Error, Warning,

Information, Verbose, ActivityTracing. Более подробную информацию о данном перечислении можно узнать на сайте [MSDN](#).

Параметры **ServiceModelListenerCircularFilesCount** и **ServiceModelMessageLoggingListenerCircularFilesCount** определяют количество создаваемых файлов журналов. Значение «0» данных параметров означает отсутствие ограничения на количество создаваемых файлов журналов. По достижению максимального размера файла (определяется параметрами **ServiceModelMessageLoggingListenerMaxLogFileSize** и **ServiceModelListenerMaxLogFileSize**) будет создан новый файл, в который в дальнейшем будет продолжаться запись журнала. При достижении максимального количества файлов журналов запись вновь начнётся с первого файла.

Примечание

К моменту включения журналирования каталог для записи файлов журналов должен существовать. В противном случае при запуске Сервиса Проверки Подписи произойдет критическая ошибка.

Учётной записи Сервиса Проверки Подписи требуется выдать права на запись в указанный каталог.

Командлет Update-VsInstance

Командлет осуществляет обновление конфигурации экземпляра Сервиса Проверки Подписи.

Синтаксис:

```
Update-VsProperties [-DisplayName <string>]
```

Примечание

Командлет необходимо запускать только в случае возникновения ошибок во время штатного обновления КриптоПро SVS через [установщик](#).

ПАРАМЕТР	ТИП	ОПИСАНИЕ
DisplayName	string	Отображаемое имя экземпляра Сервиса Проверки Подписи. Если значение не указано, будет обновлен экземпляр по умолчанию.

Командлет Update-VsLicense

Обновляет лицензию Сервиса Проверки Подписи.

Синтаксис:

```
Update-VsLicense [-DisplayName <string>] [-SN <string>] [-CompanyName <string>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
CompanyName	string	Наименование организации
DisplayName	string	Отображаемое имя экземпляра Сервиса Проверки Подписи.
SN	string	Серийный номер лицензии

Примечание

Вызов командлета необходим при создании каждого нового экземпляра Сервиса Проверки Подписи.

Командлет Add-VsFeInstance

Внимание!

Командлет используется только в версиях КриптоПро SVS 3.0 и новее.

Создает новый экземпляр Веб-интерфейса КриптоПро SVS.

К основным параметрам относятся:

- название веб-сайта IIS, на котором следует развернуть веб-приложение Сервиса Проверки Подписи;
- отображаемое имя экземпляра Сервиса Проверки Подписи.

Синтаксис:

```
Add-VsFeInstance [-ApplicationName <string>] [-ListenPort <int>] [-DisplayName <string>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
ApplicatonName	string	Название веб-приложения Сервиса Проверки Подписи. Если параметр не задан, используется значение verify.
DisplayName	string	Отображаемое имя экземпляра Веб-интерфейса Сервиса Проверки Подписи.
ListenPort	int	Порт, который прослушивает КриптоПро SVS (параметр используется только в *nix-системах).

Пример:

```
Add-VsFeInstance -DisplayName vsfe -ApplicationName verify
```

Пользователи могут обратиться к Веб-интерфейсу Сервиса Проверки Подписи по адресу: `http://<hostname>/verify/`.

Командлет Get-VsFeProperties

Внимание!

Командлет используется только в версиях КриптоПро SVS 3.0 и новее.

Командлет позволяет отобразить основные параметры Сервиса Проверки Подписи.

Синтаксис:

```
Get-VsFeProperties [-DisplayName <string>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
DisplayName	string	Имя экземпляра Веб-интерфейса Сервиса Проверки Подписи. Если значение не указано, будут отображены параметры экземпляра по умолчанию.

Командлет Remove-VsFeInstance

Внимание!

Командлет используется только в версиях КриптоПро SVS 3.0 и новее.

Удаляет созданный экземпляр Веб-интерфейса Сервиса Проверки Подписи.

Синтаксис:

```
Remove-VsFeInstance [-DisplayName <string>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
DisplayName	string	Имя экземпляра Веб-интерфейса Сервиса Проверки Подписи. Если значение не указано, будет удален экземпляр по умолчанию.

Командлет Set-VsFeProperties

Внимание!

Командлет используется только в версиях КриптоПро SVS 3.0 и новее.

Командлет позволяет задать основные параметры Веб-интерфейса Сервиса Проверки Подписи.

Синтаксис:

```
Set-VsFeProperties [-BaseUrl <string>] [-FooterText <string>] [-LogoUrl <string>] [-SubPath <string>] [-MainDarkColor <string>] [-SuccessColor <string>] [-MainLightColor <string>] [-TextDarkColor <string>] [-TextLightColor <string>] [-SecondaryColor <string>] [-IconColor <string>] [-ErrorColor <string>] [-DisplayName {Verify}] [<CommonParameters>]
```

ПАРАМЕТР	ТИП	ОПИСАНИЕ
BaseUrl	string	Адрес сервиса SVS, обрабатывающего запросы по REST API в формате <code>https://<hostname>/<SVSAppName>/rest/api</code> .
DisplayName	string	Отображаемое имя экземпляра Веб-интерфейса Сервиса Проверки Подписи.
ErrorColor	string	Цвет всплывающих окон с ошибками и текста с недействительным статусом электронной подписи или сертификата, не прошедшего проверку. Цвет по умолчанию: <code>#E30520</code>
FooterText	string	Текст на футере сайта.
IconColor	string	Цвет иконок интерфейса. Цвет по умолчанию: <code>#444444</code>
LogoUrl	string	Ссылка на файл логотипа в верхнем левом углу сайта.
MainDarkColor	string	Цвет "шапки" сайта, футера, облака в области перетаскивания документов на главной странице (не при наведении). Цвет по умолчанию: <code>#444444</code>
MainLightColor	string	Фон сайта. Цвет по умолчанию: <code>#f6f6f6</code>
SecondaryColor	string	Акцентный цвет: кнопки, облако в области перетаскивания документов на главной странице (при наведении), информационные сообщения. Цвет по умолчанию: <code>#2967b1</code>
SubPath	string	Путь публикации Веб-интерфейса на веб-сервере в формате <code>/SVSAppName/</code> . Параметр не используется в ОС Windows.
SuccessColor	string	Цвет текста с действительным статусом электронной подписи или сертификата, прошедшего проверку. Цвет по умолчанию: <code>#00A969</code>
TextDarkColor	string	Основной цвет текста сайта, расположенного на светлом фоне (MainLightColor). Цвет по умолчанию: <code>#444444</code>

ПАРАМЕТР	ТИП	ОПИСАНИЕ
TextLightColor	string	Цвет текста на "шапке" сайта, футере и других объектах с темным фоном (MainDarkColor). Цвет по умолчанию: #f6f6f6
PreviewLoadTimeoutInSeconds	int	Время, в течение которого готовится предпросмотр документа. Если время истекло, а документ не был загружен, предпросмотр будет отменен. Значение указывается в секундах.

Пример:

```
Set-VsFeProperties -DisplayName Verify -BaseUrl https://mysvs.ru/vs/rest/api -FooterText <string> -SubPath Verify
```

