Инструкция по подключению к сервису интеграции в тестовом контуре ГИИС ДМДК

I. Общие сведения

Тестовый контур ГИИС ДМДК доступен по адресу: https://dmdk.goznak.ru/

Интеграционный сервис тестового контура доступен по адресу: https://dmdk-exch.goznak.ru/ws/v1/exchange.wsdl

Работа в тестовом контуре ГИИС ДМДК возможна с использованием следующих сертификатов:

- тестовых сертификатов, выданных тестовым УЦ КриптоПро;
- сертификатов усиленной квалифицированной электронной подписи, выданных аккредитованными УЦ.

Для начала использования интеграционного сервиса в тестовом контуре необходимо:

1. Установить криптопровайдер КриптоПро CSP.
2. Установить сертификаты тестового УЦ КриптоПро:
   а) Корневой сертификат;
   б) Промежуточный сертификат;
   в) Сертификат, выпущенный на информационную систему Участника;
   г) Сертификат, выпущенный на руководителя организации Участника.
3. Установить программное обеспечение для организации TLS канала stunnel из состава КриптоПро CSP.
4. Зарегистрировать организацию в ГИИС ДМДК.
5. Зарегистрировать профиль информационного обмена.
6. Встать на специальный учет в ФПП.

Настройка рабочего места осуществляется в соответствии с инструкцией «РП ГИИС ДМДК 1. Настройка ПК для работы с ГИИС ДМДК», размещенной на сайте dmdk.ru в разделе «Для бизнеса».

II. Установка криптопровайдера КриптоПро CSP

Осуществляется в соответствии с Руководством пользователя на программный продукт.

III. Установка сертификатов тестового УЦ

В случае использования тестовых сертификатов дополнительно необходимо выполнить следующие действия:

1) Установить корневой сертификат тестового Удостоверяющего центра в хранилище **Доверенные корневые центры сертификации**;

2) Установить промежуточный сертификат тестового Удостоверяющего центра в хранилище **Промежуточные центры сертификации**.

3) Выпустить и установить тестовый сертификат руководителя организации-участника (пользователя):
   a. Перейти по ссылке http://testca2012.cryptopro.ru/ui/ и выполнить регистрацию. Для корректной работы с ГИИС ДМДК в сертификате участника необходимо заполнить ИНН, ОГРН организации, СНИЛС пользователя. ОГРН организации и ФИО руководителя в сертификате должны быть реальными. ИНН организации необходимо дополнить двумя лидирующими нулями
   b. Перейти по ссылке http://testca2012.cryptopro.ru/ui/ и выполнить вход в личный кабинет с Логином и Паролем из предыдущего шага.
   c. Создать сертификат (перейти в раздел меню Сертификаты и нажать на кнопку «Создать», в появившемся окне оставить значения по-умолчанию и нажать на кнопку «Создать»)
   d. Выбрать созданный сертификат и нажать на ссылку «Скачать»
   e. Установить скачанный сертификат

4) Выпустить и установить тестовый сертификат на информационную систему Участника, с указанием реальных ИНН, ОГРН\ОГРНИП организации Участника.

Требования к сертификату ключа на информационную систему

Сертификат ключа проверки электронной подписи должен содержать следующие **стандартные атрибуты**:

- уникальный номер квалифицированного сертификата;
- даты начала и окончания действия квалифицированного сертификата;
- ключ проверки электронной подписи;
- наименование используемого средства электронной подписи и (или) стандарты, требованиям которых соответствует ключ электронной подписи и ключ проверки электронной подписи;
- наименования средств электронной подписи и средств аккредитованного удостоверяющего центра, которые использованы для создания ключа электронной подписи, ключа проверки электронной подписи, квалифицированного сертификата, а также реквизиты документа, подтверждающего соответствие указанных средств требованиям, установленным в соответствии с Федеральным законом;
- наименование и место нахождения аккредитованного удостоверяющего центра, который выдал квалифицированный сертификат;

– номер квалифицированного сертификата аккредитованного удостоверяющего центра;
– ограничения использования квалифицированного сертификата (если такие ограничения установлены).

Сертификат ключа проверки электронной подписи должен содержать следующие **дополнительные атрибуты**:

– «Улучшенный ключ» (OID 2.5.29.37) – в данном дополнении должны быть указаны OID 1.3.6.1.5.5.7.3.2 («Проверка подлинности клиента») и OID 1.3.6.1.5.5.7.3.4 («Защищенная электронная почта»);
– «Точка распространения списка отозванных сертификатов» (OID 2.5.29.31) – данное дополнение должно содержать протоколы доступа и адреса публикации списка отозванных сертификатов, на основании которого может быть установлен статус сертификата ключа проверки электронной подписи.

Сертификат ключа проверки электронной подписи на информационную систему должен содержать следующие атрибуты имени:

Атрибут	**Значение для юридического лица**	**Значение для индивидуального предпринимателя**
Стандартные атрибуты имени		
Общее имя (CN, OID 2.5.4.3)	Наименование юридического лица	Фамилия, имя, отчество (если имеется) индивидуального предпринимателя
Организация (O, OID.2.5.4.10)	Наименование юридического лица	*Не применимо*
Подразделение юридического лица (OU, OID 2.5.4.11)	Наименование подразделения юридического лица (необязательный атрибут)	*Не применимо*
Страна (C, OID 2.5.4.6)	Код страны в соответствии с ISO 3166 = «RU»	
Субъект РФ (S, OID 2.5.4.8)	Наименование субъекта РФ, где зарегистрирована организация или индивидуальный предприниматель	
Населённый пункт (L, OID 2.5.4.7)	Наименование населённого пункта, где зарегистрирована организация или индивидуальный предприниматель	
Адрес (STREET, OID 2.5.4.9)	Часть адреса места нахождения организации или индивидуального предпринимателя, включающая наименование улицы, номер дома, а также корпуса, строения, квартиры, помещения (если имеется)	
Дополнительные атрибуты имени		
ИНН (OID 1.2.643.3.131.1.1)	ИНН юридического лица (12 цифр = «00» + ИНН)	ИНН индивидуального предпринимателя (12 цифр)
ОГРН (OID 1.2.643.100.1)	ОГРН организации (13 цифр)	*Не применимо*
ОГРНИП (OID 1.2.643.100.5)	*Не применимо*	ОГРН индивидуального предпринимателя (15 цифр)

IV. Установка программного обеспечения для организации TLS

На ОС семейства Windows

Для организации защищенного канала связи TLS необходимо:

1. Скачать приложение для создания TLS-туннеля stunnel.x86/x64: https://www.cryptopro.ru/products/csp/downloads
2. Сохранить в произвольном каталоге, например, в c:\stunnel.
3. Запустить командную строку от имени администратора и выполнить: c:\stunnel\stunnel.x64 –install
4. Создать пользователя Windows, от имени которого будет работать сервис stunnel.
5. В сеансе данного пользователя установить сертификаты корневого и промежуточно тестового УЦ КриптоПро в хранилища «Доверенные корневые центры сертификации» и «Промежуточные центры сертификации» соответственно.
6. В сеансе данного пользователя установить личный (пользовательский) сертификат, выпущенный на информационную систему Участника, в хранилище Личное.
7. Открыть КриптоПро CSP, выбрать закладку сервис, нажать кнопку «Протестировать», далее кнопку «По сертификату» и выбрать личный сертификат. В открывшемся окне ввести текущий пароль, обязательно поставив галочку «Сохранить пароль в системе», и нажать ОК.
8. Открыть диспетчер сертификатов выполнив команду certmgr.msc. Найти и открыть личный сертификат, выбрать закладку «Состав» и нажать кнопку «Копировать в файл». Откроется Мастер экспорта сертификатов. В нём необходимо экспортировать сертификат без закрытого ключа в формате X.509 (.CER) в кодировке DER и сохранить его с именем clicer.cer в произвольном каталоге, например, c:\stunnel.
9. В каталоге c:\windows\system32 создать файл конфигурации stunnel.conf со следующим содержимым:

```
output=c:\stunnel\stunnel.log
socket=l:TCP_NODELAY=1
socket=r:TCP_NODELAY=1
debug=7
[https]
client=yes
accept=127.0.0.1:1500
connect=195.209.130.19:443
cert=C:\stunnel\clicer.cer
verify=0
```

В примере указан порт 1500, можно использовать любой другой свободный.

Параметр *connect* – адрес сервиса интеграции в тестовом контуре (не менять).

Параметр *accept* – адрес, который необходимо указывать в прикладном ПО для подключения к сервису интеграции.

10. Открыть Службы выполнив команду services.msc. Выбрать службу Stunnel Service. Тип запуска установить «Автоматически». Вход в систему с учетной записью созданного пользователя. Запустить службу.

Последовательность действий для проверки корректности настройки ПО stunnel и работоспособности сервиса интеграции описана в приложении 1.

На ОС семейства Linux (на примере Astra Linux)

Для организации защищенного канала связи TLS необходимо:

1. Установить КриптоПро CSP, выбрав при установке пункт stunnel, либо установить его позже, выполнив установку пакетов cprocsp-stunel-*.deb или cprocsp-stunel-*.rpm .
2. Создать пользователя Linux, от имени которого будет работать stunnel.
3. В сеансе данного пользователя установить сертификаты корневого и промежуточно тестового УЦ КриптоПро в хранилища «Доверенные корневые центры сертификации» и «Промежуточные центры сертификации» соответственно, используя графическую утилиту «Инструменты КриптоПро», или при помощи команд:

```
/opt/cprocsp/bin/amd64/certmgr -inst -store uroot -file rootca.cer
/opt/cprocsp/bin/amd64/certmgr -inst -store uCA -file subca.cer
```

В случае успешной установки вывод каждой из команд должен заканчиваться [ErrorCode: 0x00000000].

4. В сеансе данного пользователя установить личный (пользовательский) сертификат, выпущенный на информационную систему Участника, в хранилище Личное. Для этого необходимо скопировать сертификат, предварительно экспортированный в формат pfx и установить его выполнив команду, указав пароль от pfx файла:

```
/opt/cprocsp/bin/amd64/certmgr -install -pfx -file *.pfx -pin пароль
```

В случае успешной установки сертификата вывод команды должен заканчиваться [ErrorCode: 0x00000000].

5. Для сохранения пароля от контейнера, если он был задан, необходимо выполнить команду, указав путь к контейнеру и пароль:

```
/opt/cprocsp/sbin/amd64/cpconfig -ini
"\\LOCAL\\KeyDevices\\passwords\\HDIMAGE\\00f3956b.000" -add string
passwd пароль
```

Для того чтобы определить путь к контейнеру необходимо выполнить команду

```
/opt/cprocsp/bin/amd64/certmgr -list
```

и у нужного сертификата взять часть значения параметра Container между «\\» и «\»

6. Экспортировать сертификат со ссылкой на закрытый ключ, выполнив команду, указав полный путь к контейнеру:

```
/opt/cprocsp/bin/amd64/certmgr -export -dest
/home/user/stunnel/client.cer -cont '\\.\HDIMAGE\00f3956b2-9dde-97b1-
0216-f3544a4c7c3'
```

Для того чтобы определить путь к контейнеру необходимо вывести список всех контейнеров, выполнив команду:

```
/opt/cprocsp/bin/amd64/csptest -keyset -enum_cont -verifycontext -fqcn
```

Из списка необходимо выбрать полное имя, соответствующее краткому из значения параметра Container соответствующего сертификта

7. В произвольном каталоге, например в папке stunnel домашней директории пользователя, создать файл конфигурации stunnel.conf со следующим содержимым:

```
output=/home/user/stunnel/stunnel.log
pid =/home/user/stunnel.pid
socket=l:TCP_NODELAY=1
socket=r:TCP_NODELAY=1
debug=7
[https]
client=yes
accept=127.0.0.1:1500
connect=195.209.130.19:443
cert=/home/user/stunnel/clicer.cer
verify=0
```

В примере указан порт 1500, можно использовать любой другой свободный.

Параметр *connect* – адрес сервиса интеграции в тестовом контуре (не менять).

Параметр *accept* – адрес, который необходимо указывать в прикладном ПО для подключения к сервису интеграции.

8. Запустить stunnel выполнив команду:

```
/opt/cprocsp/sbin/amd64/stunnel_thread /home/user/stunnel/stunnel.conf
```

Для остановки необходимо завершить процесс stunnel. При необходимости можно настроить автозапуск stunnel, например, создав сервис systemd .

Последовательность действий для проверки корректности настройки ПО stunnel и работоспособности сервиса интеграции описана в приложении 1.

V. Регистрация организации в ГИИС ДМДК

Осуществляется в соответствии с руководством пользователя РП ГИИС ДМДК 2. Порядок регистрации в системе, размещенной на сайте dmdk.ru

VI. Настройка профиля информационного обмена в ГИИС ДМДК

Для настройки информационного обмена между ГИИС ДМДК и ИС Участника пользователь должен иметь роль «Администратор организации».

Для настройки информационного обмена необходимо:

1) Перейти в раздел «Управление профилями» и нажать кнопку «Создать профиль информационного обмена».

2) В открывшейся форме заполнить обязательные поля (см. Рисунок 1).

3) Добавить сертификат на информационную систему (см. Рисунок 2).

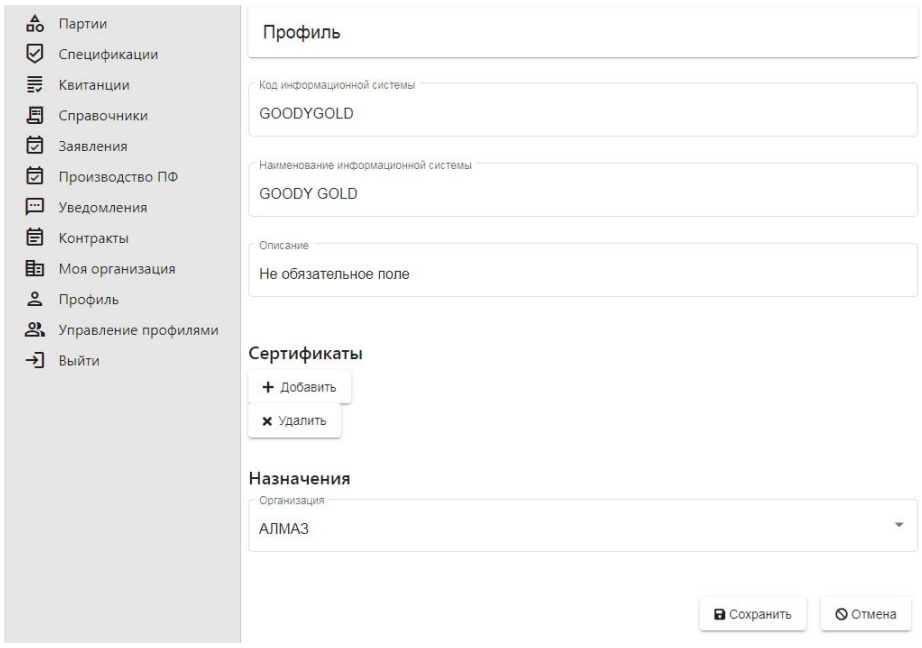


Рисунок 1 – Форма редактирования профиля

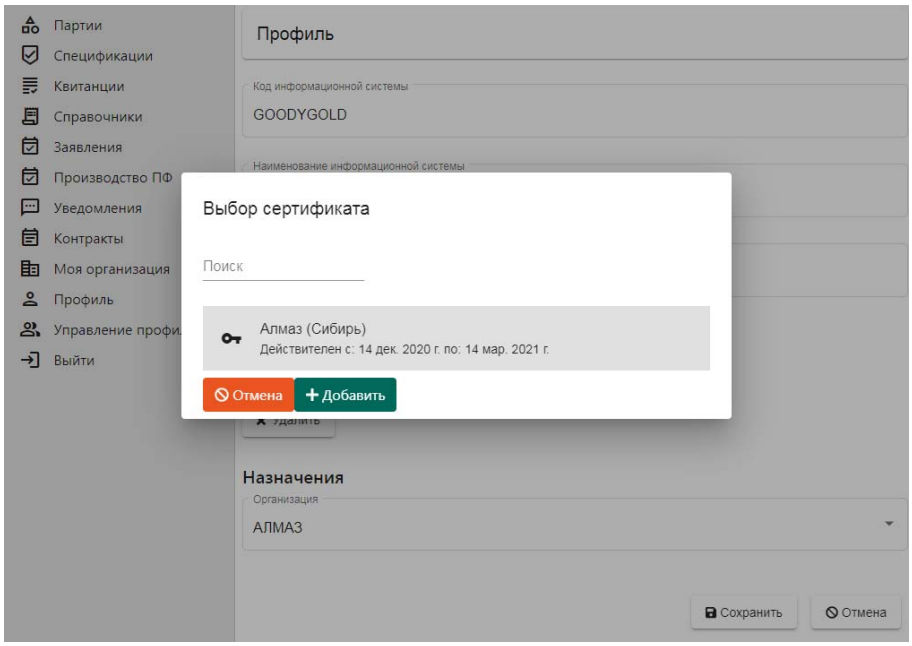


Рисунок 2 – Форма добавления сертификата

4) Сохранить изменения – в списке назначений появится профиль информационной системы.

VII. Постановка на специальный учет в ФПП.

Осуществляется в соответствии с руководством пользователя РП ГИИС ДМДК 3. Постановка на специальный учет, размещенной на сайте dmdk.ru.

Приложение 1. Проверка работоспособности интеграционного сервиса

Для проверки корректности настройки ПО stunnel и работоспособности сервиса интеграции необходимо:

1. Загрузить и установить приложение SoapUI.

2. Создать новый SOAP проект (New SOAP Project).

3. Указать имя проекта и Initial WSDL: http://127.0.0.1:[порт]/ws/v1/exchange.wsdl (порт – это номер порта, который был указан в настройках Stunnel).

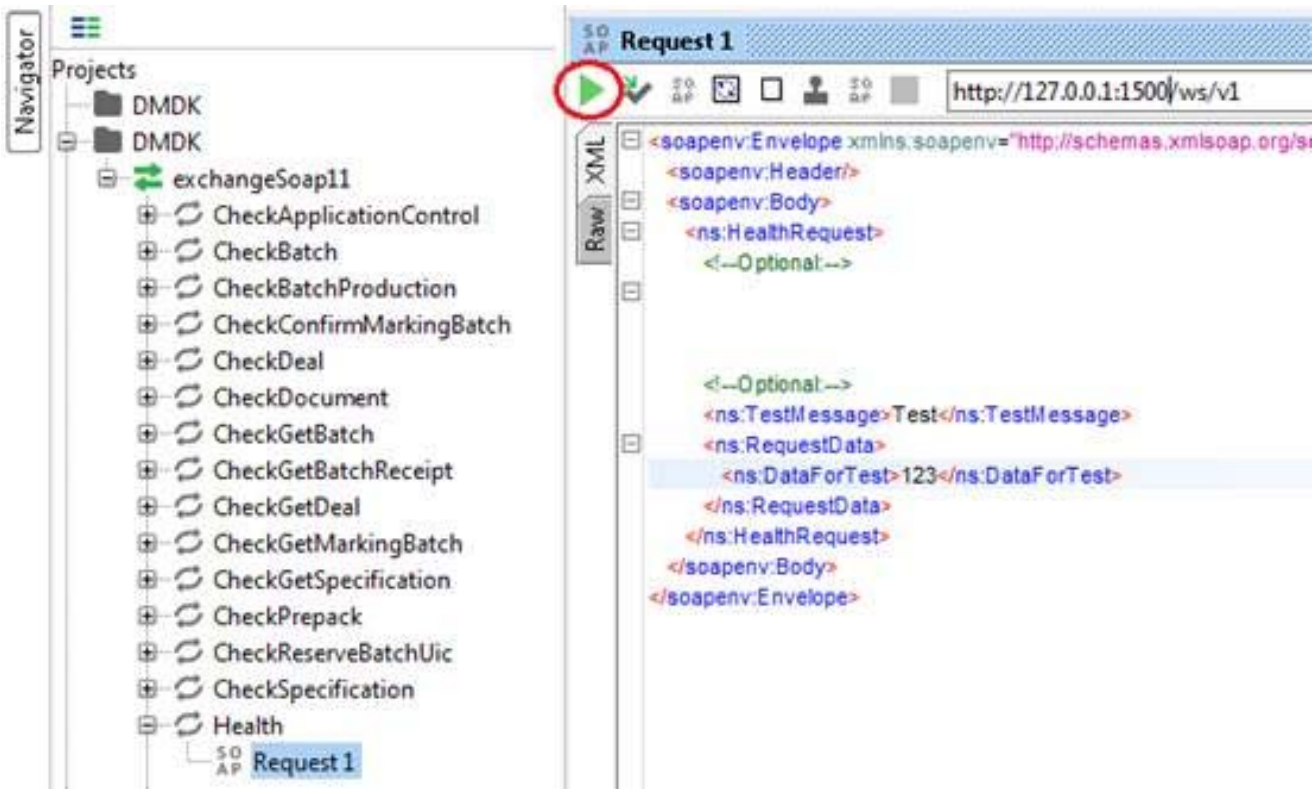
4. После нажатия кнопки «Ok» в главном окне в разделе Projects отобразятся доступные методы (это уже говорит о том, что вы «достучались» до сервиса).

5. Развернуть метод Health, выбрать Request1, в окне редактирования запроса удалить блок, связанный с подписью:

```
<ns:CallerSignature>
<!--You may enter ANY elements at this point-->
</ns:CallerSignature>
```

и указать любые значения в тегах <ns:TestMessage> </ns:TestMessage> и <ns:DataForTest> </ns:DataForTest>.

Запрос должен иметь следующий вид:



6. Отправить запрос (зеленая стрелка). В правом окне должен отобразиться результат следующего вида:

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
<ns2:HealthResponse xmlns:ns2="urn://xsd.dmdk.goznak.ru/exchange/1.0" xmlns:ns3="urn://x-artefacts-smev-gov-ru/services/message-exchange/types/basic/1.1" xmlns:ns4="urn://xsd.dmdk.goznak.ru/batch/1.0" xmlns:ns5="urn://xsd.dmdk.goznak.ru/contractor/1.0" xmlns:ns6="urn://xsd.dmdk.goznak.ru/types/1.0" xmlns:ns7="urn://xsd.dmdk.goznak.ru/deal/1.0" xmlns:ns8="urn://xsd.dmdk.goznak.ru/specification/1.0">
<ns2:DmdkSignature>
<ds:Signature Id="sigID1" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod Algorithm="urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102012-gostr34112012-256"/>
<ds:Reference URI="">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:Transform Algorithm="urn://smev-gov-ru/xmldsig/transform"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-256"/>
<ds:DigestValue>CVLK7YLuFSR50xHY8s4JcLkZvWNHMtJDntIZ4KgAyo0=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>

<ds:SignatureValue>l3xZXQvS6JJ0xbtdbb9OYcSyrFiqoaG0eJSQvdUw3Ko0Tx1DQls5z7mdRbB+qW8GiFMkL202V29OKx5eOpUVbg==</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>MIIHjjCCBzugAwIBAgIRArHFTADsrKmCRAvyFuGU1I4wCgYIKoUDBwEBAwIwggFbMSAwHgY
JKoZIhvcNAQkBFhFpbmZvQGNyeXB0b3Byby5ydTEYMBYGBSqFA2QBEg0xMDM3NzAwMDg1NDQ0MRowGAYIKo
UDA4EDAQESDDAwNzcxNzEwNzk5MTELMAkGA1UEBhMCUlUxGDAWBgNVBAgMDzc3INCc0L7RgdC60LLQsDE
VMBMGA1UEBwwM0JzQvtGB0LrQstCwMS8wLQYDVQQJDCbRg9C7LiDQodGD0YnRkdCy0YHQutC40Lkg0LLQsNC
7INC0LiAxODElMCMGA1UECgwc0J7QntCeICLQmtCg0JjQn9Ci0J4t0J/QoNCeIjFrMGkGA1UEAwxi0KLQtdGB0YLQvt
Cy0YvQuSDQv9C+0LTRh9C40L3QtdC90L3Ri9C5INCj0KYg0J7QntCeICLQmtCg0JjQn9Ci0J4t0J/QoNCeIiDQk9Ce0KHQ
oiAyMDEyICjQo9CmIDIuMCkwHhcNMjEwMzE1MDQyOTMxWhcNMjEwNjE1MDQzOTMxWjAtMQswCQYDVQQGE
wJSVTEeMBwGA1UEAwwV0JDQniDCq9CT0J7Ql9Cd0JDQmsK7MGYwHwYIKoUDBwEBAQEwEwYHKoUDAgIkAA
YIKoUDBwEBAgIDQwAEQCeL2cjN120ra/F81D01jTTVkYUEiGjUeS3eHx9XnB5Q1dVcQNjN48O7AEEiPqhhfOB1kVxn
7+a9JUDrsn8zFN+jggT9MIIE+TAOBgNVHQ8BAf8EBAMCBPAwHwYJKwYBBAGCNxUHBBIwEAYIKoUDAgIuAAgC
AQECAQAwHQYDVR0OBBYEFGMWKsOCywFWolLPFA4llF6XaSKZMCYGA1UdJQQfMB0GCCsGAQUFBwMEBggr
BgEFBQcDAgYHKoUDAgIiBjAyBgkrBgEEAYI3FQoEJTAjMAoGCCsGAQUFBwMEMAoGCCsGAQUFBwMCMAkGB
yqFAwICIgYwgacGCCsGAQUFBwEBBIGaMIGXMDgGCCsGAQUFBzABhixodHRwOi8vdGVzdGNhMjAxMi5jcnlwdG9
wcm8ucnUvb2NzcC9vY3NwLnNyZjBbBggrBgEFBQcwAoZPaHR0cDovL3Rlc3RjYTIwMTIuY3J5cHRvcHJvLnJ1L2FpYS
8wNjRiNjMyNTMzNjYyYTI0MzgxODcyNDM3YTNiYjdjYmIyY2FmYzczLmNydDAdBgNVHSAEFjAUMAgGBiqFA2Rx
AjAIBgYqhQNkcQEwKwYDVR0QBCQwIoAPMjAyMTAzMTUwNDI5MzFagQ8yMDIxMDYxNTA0MjkzMVowggEaBg
UqhQNkcASCAQ8wggELDDTQodCa0JfQmCAi0JrRgNC40L/RgtC+0J/RgNC+IENTUCIgKNCy0LXRgNGB0LjRjyA0LjA
pDDHQn9CQ0JogItCa0YDQuNC/0YLQvtCf0YDQviDQo9CmIiDQstC10YDRgdC40LggMi4wDE/QodC10YDRgtC40YTQ
uNC60LDRgiDRgdC+0L7RgtCy0LXRgtGB0YLQstC40Y8g4oSWINCh0KQvMTI0LTMzODAg0L7RgiAxMS4wNS4yMDE
4DE/QodC10YDRgtC40YTQuNC60LDRgiDRgdC+0L7RgtCy0LXRgtGB0YLQstC40Y8g4oSWINCh0KQvMTI4LTM1OTI
g0L7RgiAxNy4xMC4yMDE4MCwGBSqFA2RvBCMMIdCh0JrQl9CYICLQmtGA0LjQv9GC0L7Qn9GA0L4gQ1NQIjBgBg
NVHR8EWTBXMFWgU6BRhk9odHRwOi8vdGVzdGNhMjAxMi5jcnlwdG9wcm8ucnUvY2RwLzA2NGI2MzI1MzM2NjJh
MjQzODE4NzI0MzdhM2JiN2NiYjJjYWZjNzMuY3JsMAwGBSqFA2RyBAMCAQIwggGXBgNVHSMEggGOMIIBioAUB
ktjJTNmKiQ4GHJDeju3y7LK/HOhggFdpIIBWTCCAVUxIDAeBgkqhkiG9w0BCQEWEWluZm9AY3J5cHRvcHJvLnJ1MR
gwFgYFKoUDZAESDTEwMzc3MDAwODU0NDQxGjAYBggqhQMDgQMBARIMMDA3NzE3MTA3OTkxMQswCQYD
VQQGEwJSVTEYMBYGA1UECAwPNzcg0JzQvtGB0LrQstCwMRUwEwYDVQQHDAzQnNC+0YHQutCy0LAxLzAtBg
NVBAkMJtGD0LsuINCh0YPRidGR0LLRgdC60LjQuSDQstCw0Lsg0LQuIDE4MSUwIwYDVQQKDBzQntCe0J4gItCa0K
DQmNCf0KLQni3Qn9Cg0J4iMWUwYwYDVQQDDFzQotC10YHRgtC+0LLRi9C5INCz0L7Qu9C+0LLQvdC+0Lkg0KPQ
piDQntCe0J4gItCa0KDQmNCf0KLQni3Qn9Cg0J4iINCT0J7QodCiIDIwMTIgKNCj0KYgMi4wKYIRAm3PtACtq0uIRg2Y
+dz8Ly4wCgYIKoUDBwEBAwIDQQCZEFnWPoDwJQuXDVFcokG2m9UCgUTsNquglaFwUhlyKmtUiD6WHS6GyiWmx
oBzP1oyF4SSMxbIEVA+PkBtFdj4</ds:X509Certificate>

```
            </ds:X509Data>
          </ds:KeyInfo>
        </ds:Signature>
      </ns2:DmdkSignature>
      <ns2:ResponseData>
        <ns2:Result>Running</ns2:Result>
      </ns2:ResponseData>
    </ns2:HealthResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Значение «Running» говорит о том, что сервис работает.