

Бесплатный StartSSL сертификат для wss

⚠ Данный сертификат больше не поддерживается основными браузерами.

Документ описывает процесс подключения бесплатного SSL сертификата полученного на сайте www.startssl.com

Создание key и scr файлов

Заказывать сертификат будем хоста **app-d1.webitel.com**.

1. Переходим в директорию **/opt/webitel/ssl**
2. Создаем **приватный ключ**:

```
openssl genrsa -out wss.key 2048
```

```
root@app-d1 ~/webitel/certs master openssl genrsa -out wss.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
```

3. Создаем **запрос сертификата**:

```
openssl req -new -sha256 -key wss.key -out wss.csr
```

```
root@app-d1 ~/webitel/certs master openssl req -new -sha256 -key wss.key -out wss.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:UA
State or Province Name (full name) [Some-State]:Lviv Region
Locality Name (eg, city) []:Lviv
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Webitel Ltd.
Organizational Unit Name (eg, section) []:on-demand
Common Name (e.g. server FQDN or YOUR name) []:app-d1.webitel.com
Email Address []:support@webitel.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Запрос бесплатного сертификата Calss 1 на 1 год

Регистрируемся на www.startssl.com

1. Подтверждаем право владения нашим доменом **webitel.com**:

Tool Box Certificates Wizard **Validations Wizard**

Select Validation

- Select the type and attribute of validation you'd like to perform.
- Please note that you might need to have instant access to your email account(s) or documents in image format ready.

Domain Validation
 Email Validation
 Personal Identity Validation
 Organization Extended Validation

[Continue](#)

2. Создаем запрос на сертификат:

Tool Box Certificates Wizard Validations Wizard [Bug Report](#)

Select Certificate Purpose

- Make sure you have already validated a domain name or email address before using this tool! Select the "Validations Wizard" for this task.
- Depending on your preferences and type of software, you need to have a prepared certificate request (CSR) ready for submission.

Web Server SSL/TLS Certificate
 Client S/MIME and Authentication Certificate

[Continue](#)

3. Копируем наш запрос в форму на сайте:

Tool Box Certificates Wizard Validations Wizard [Bug Report](#)

Free SSL Certificate – Class 1 DV SSL Certificate

Please enter your domain details:

Verified domain(s): **webitel.com**

Domain: ✓

* The following domains will be added to Subject Alternative Name additionally:
webitel.com

Free SSL Certificate support 1 domain 1 year only. If you want to add more domains more years, please finish the "[Personal Identity Validation](#)" for personal use that only cost US\$59.90 for unlimited multi-domain and wildcard SSL certificate for 2 years period for FREE.
Or go to "[Organization Extended Validation](#)" for organization use that only cost US\$199.90 for unlimited multi-domain and wildcard OV SSL certificate for 3 years period and one EV SSL certificate for 2 years period for FREE .

Please submit your Certificate Signing Request (CSR):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIG5DCCAcwCAQAwZ4xCzAJBgNVBAYTAUFRb3RlYXV0eS9YDQo1DA1Mdm12IEJlZ21y
b3JENMAsGAIUEBwwEETHZodJEVMBGAIUEGcwWV2V1aXR1bC9BMDQwMRE1wEAYDYGQOL
DALxh1lkZW1hbm9xGzAZBgNVBAMTEmFwcC1kMS53Z21JdGCVslmNvYXTEiMCAgCSaG
Algorithm :RSA
Key length :2048
```

4. После того, как сертификат будет готов, мы получим уведомление на Email. Можем скачать наш сертификат:

Tool Box Certificates Wizard Validations Wizard [Bug Report](#)

Certificate List

No	Order Number	Common Name	Products	Issuance Date	Status	Action
24	151222202349451	app-d1.webitel.com	Class 1 SSL	2015-12-23	Issued	Retrieve

Создание PEM файла для webitel

1. В полученном архиве можно увидеть несколько готовых примеров под разное ПО. Нам подойдет **Apache**:

```
app-d1.webitel.com
Apache\ Server
  1_root_bundle.crt
  2_app-d1.webitel.com.crt
Apache\ Server.zip
IIS\ Server.zip
Nginx\ Server.zip
Other\ Server.zip
```

2. Файлы 1_root_bundle.crt и 2_app-d1.webitel.com.crt копируем на сервер webitel в директорию **/opt/webitel/ssl**
3. Создаем PEM файл:

```
cat 2_app-d1.webitel.com.crt wss.key 1_root_bundle.crt > wss.pem
cp wss.pem tls.pem
cp wss.pem dtls-srtp.pem
```

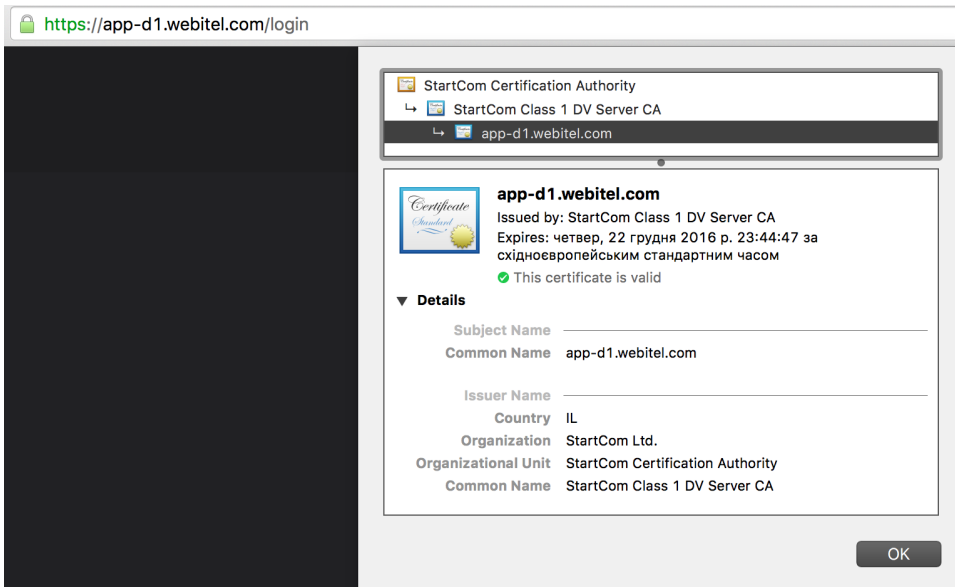
4. Результат в **/opt/webitel/ssl**:

```
certs
1_root_bundle.crt
2_app-d1.webitel.com.crt
dtls-srtp.pem
tls.pem
wss.csr
wss.key
wss.pem
```

Подключение сертификата к webitel

1. В файле **env/environment** изменить на:

```
# WebSocket protocol: ws or wss (WebSocket with SSL)
export WEBITEL_WS="wss"
# WebSocket protocol: off or on (for HTTPS)
export WEBITEL_SSL="on"
# WebSocket protocol: http or https
export WEBITEL_PROTO="https"
# Webitel IP or hostname.
# Please, use the FQDN hostname for HTTPS site
export WEBITEL_HOST="app-d1.webitel.com"
```



Похожие статьи

- [Как восстановить Elasticsearch из режима read-only?](#)
- [Как перевести сайт bpm'online on-site на HTTPS с помощью бесплатного сертификата](#)
- [Бесплатный StartSSL сертификат для wss](#)
- [Плохое качество связи в браузере Chrome под Ubuntu Linux](#)
- [Работа http сайта в Chrome с webrtc](#)