Проблема работы сертификата Let's Encrypt на старых устройствах

С сайта https://www.ukraine.com.ua/

Внимание!

Возникшая ситуация никак не влияет на уровень безопасности сертификатов Let's Encrypt.

30 сентября 2021 года истёк срок действия корневого сертификата DST Root CA X3. В результате устаревшие устройства, которые давно не получали обновлений и не поддерживают новый корневой сертификат ISRG Root X1, перестали доверять старому сертификату и при посещении сайтов, использующих сертификаты от Let's Encrypt, выдают предупреждения или не могут установить защищённое соединение.

Перечень устройств, считающихся устаревшими

К устаревшим устройствам относятся системы возрастом старше 5 лет, среди которых:

- Windows XP до SP3 (а также для SP3 и Windows 7, если не производилось автоматическое обновление корневых сертификатов);
- macOS до 10.12.1;
- iOS до 10;
- Android до 2.3.6 (при этом доступ к сервисам еще может быть, из-за особенностей проверки корневых сертификатов, а версии до 7.1.1 перестанут поддерживать сертификат в 2024 году);
- Ubuntu до 16.04;
- Debian до 8;
- Sony PlayStation 3 и 4 с прошивками до 5.00;
- Старые модели смарт-телевизоров и умных домашних устройств;
- Устройства, использующие OpenSSL версии 1.0.x;

Способы решения проблемы

Решить проблему можно несколькими способами. Лучшем решением будет обновление ПО до последних версий, где уже включена поддержка нового корневого сертификата. Принимать меры по решению проблемы стоит только в том случае, если это необходимо, например, довольно крупная часть аудитории сервиса использует устаревшее ПО и они критичны для проекта. В ином случае стоит пренебречь текущей ситуацией.

Со стороны клиента

Со стороны клиента можно:

1. Вручную установить корневой сертификат ISRG Root X1, если он остутствует в хранилище используемой системы или ПО.
2. Удалить устаревший корневой сертификата DST Root CA X3. Наличие устаревшего корневого сертификата может мешать нормальной работе с сервисами, использующими сертификаты Let's Encrypt.

Внимание! Решить проблему данным способом можно не на всех устройствах.

Debian/Ubuntu

1. Для проверки наличия корневого сертификата в списке доверенных, выполните в терминале команду:

```
awk -v cmd='openssl x509 -noout -subject' ' /BEGIN/{close(cmd)};{print | cmd}' < /etc/ssl/certs/ca-certificates.crt | grep "ISRG Root X1"
```

Copy

Если в выводе команды будет фигурировать `subject=C = US, O = Internet Security Research Group, CN = ISRG Root X1`, то нет необходимости выполнять какие-либо действия, а если нет, то перейдите к следующему шагу.

2. Выполните в терминале команду:

```
curl -k https://letsencrypt.org/certs/isrgrootx1.pem.txt | sudo tee /usr/share/ca-certificates/mozilla/ISRG_Root_X1.crt ; sudo echo "mozilla/ISRG_Root_X1.crt" >> /etc/ca-certificates.conf ; sudo update-ca-certificates
```

Copy

3. Проверьте работу сервисов, с которыми возникали проблемы доступа.

CentOS

1. Для проверки наличия корневого сертификата в списке доверенных, выполните в терминале команду:

```
awk -v cmd='openssl x509 -noout -subject' ' /BEGIN/{close(cmd)};{print | cmd}' < /etc/ssl/certs/ca-bundle.crt | grep "ISRG Root X1"
```

Copy

Если в выводе команды будет фигурировать `subject=C = US, O = Internet Security Research Group, CN = ISRG Root X1`, то нет необходимости выполнять какие-либо действия, а если нет, то перейдите к следующему шагу.

2. Выполните в терминале следующие команды:

3.
```
trust dump --filter "pkcs11:id=%c4%a7%b1%a4%7b%2c%71%fa%db%e1%4b%90%75%ff%c4%15%60%85%89%10" | openssl x509 | sudo tee /etc/pki/ca-trust/source/blacklist/DST-Root-CA-X3.pem
```

```
sudo update-ca-trust
```

Copy

4. Проверьте работу сервисов, с которыми возникали проблемы доступа.

OpenSSL 1.0.x

Если в системе используется устаревшая версия OpenSSL, то необходимо удалить из доверенных корневых сертификатов устаревший следующим образом:

- Для Debian/Ubuntu отредактируйте файл `/etc/ca-certificates.conf` установив символ `!` в начале строки `mozilla/DST_Root_CA_X3.crt` и выполните команду:

```
update-ca-certificates
```

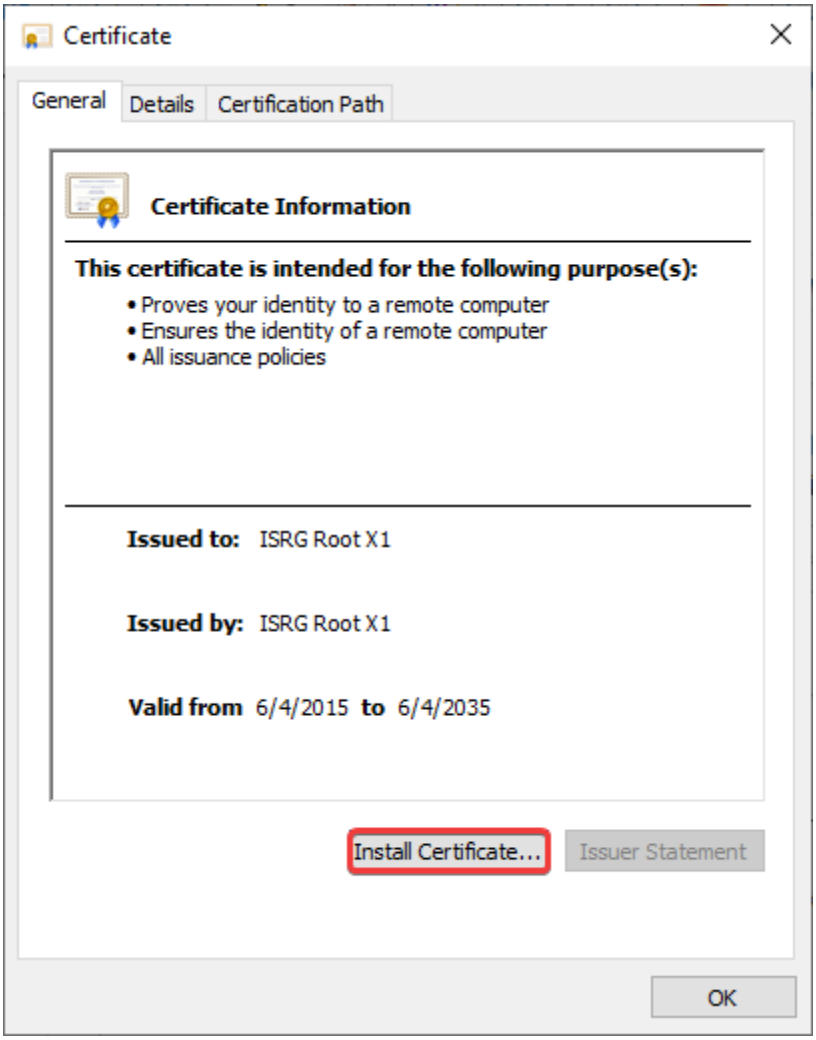
Copy

Windows 7

В операционной системе Windows 7 цепочка корневых сертификатов должна была обновиться, если включены обновления операционной системы, в ином случае корневой сертификат необходимо установить самостоятельно, выполнив следующие действия:

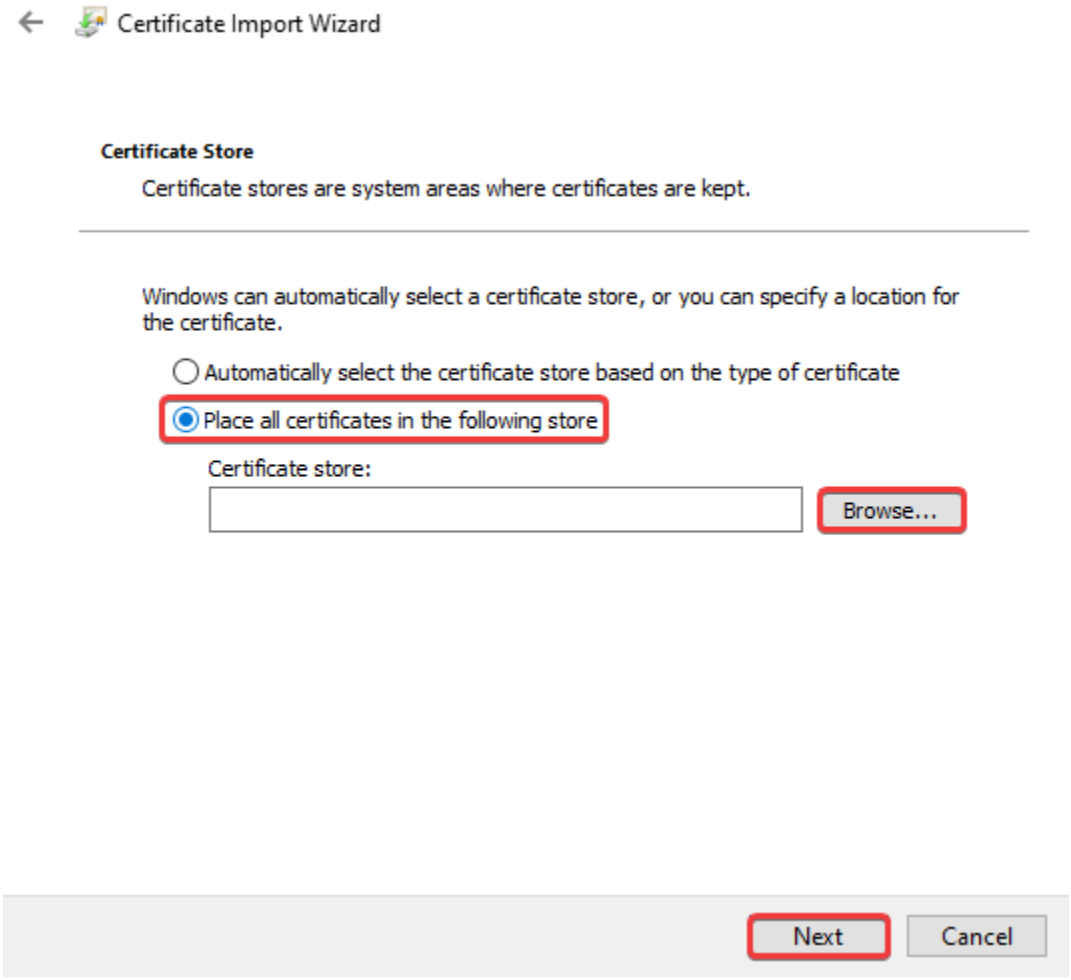
1. Скачайте корневой сертификат `ISRG Root X1` с сайта Let's Encrypt в формате `der`.
2. Запустите скачанный файл и разрешите его открытие, нажав «**Открыть**».

3. В появившемся окне нажмите «**Install Cerificate**»:

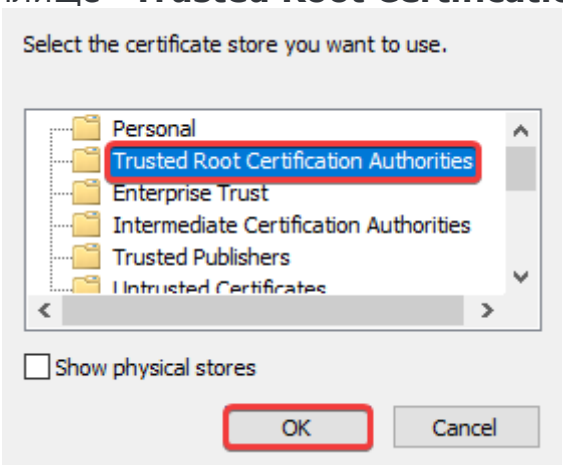


4. Выберите, для кого необходимо установить сертификат, и нажмите «**Далее**».

5. Выберите пункт «**Place all certificates in the following store**» и нажмите «**Browse**»:



6. Выберите хранилище «**Trusted Root Certification Authorities**» и нажмите «**OK**»:



7. Нажмите «**Next**», проверьте корректность выбранных данных и нажмите «**Finish**».
8. Проверьте работу сервисов, с которыми возникали проблемы доступа.

Со стороны сервера

Решение проблемы со стороны сервера возможно только путём использования других сертификатов.

1. Чтобы использовать другой сертификат, необходимо его приобрести в одном из центров сертификации или у их партнера. При выборе нового сертификата важно учитывать, какие функции он предоставляет и для каких сфер подходит. Для примера ниже приведены некоторые известные центры сертификации:
    - Comodo
    - GeoTrust
    - Symantec (DigiCert)
    - Thawte
2. Установите полученный сертификат для сайта.
3. После установки сертификата дождитесь обновления кешированной информации, что происходит обычно в течение 15 минут, и проверьте работу сайта на проблемном устройстве.