Порядок создания сертификатов и ключей mTLS для авторизации партнеров в контуре НЛ

# Общие положения

Адрес сервера: [https://partner-api-dev.nl-dev.ru/partner-api/](https://partner-api-dev.nl-dev.ru/partner-api/swagger-ui/index.html?configUrl=/partner-api/v3/api-docs/swagger-config)

Порядок получения доступа к API:

1. Предоставить ip-адреса серверов партнера, с которых будет производиться подключение для добавления в white list НЛ
2. Предоставить НЛ публичную часть (публичный ключ) корневого сертификата (или цепочку сертификатов) своего центра сертификации для установки доверия на стороне НЛ
3. Сгенерировать приватный ключ для создания клиентского сертификата
4. Поставить запрос на создание сертификата (csr) от приватного ключа
5. Подписать сертификат в своем центре сертификации
6. Создать подключение с помощью подписанного клиентского сертификата

Примечание:

Сертификаты НЛ подписаны публичными Центрами сертификации и по умолчанию являются доверительными на всех операционных системах

Ограничения:

1. Клиентский сертификат должен быть в формате x509v3 и использовать алгоритм шифрования RSA или более криптостойкий
2. Алгоритм подписи SHA256 с RSA шифрованием или более криптостойкий
3. Длина ключа не менее 4096 бит
4. Срок действия клиентского сертификата – не более 1 года
5. При работе по HTTPS обязательно использование протокола TLS v1.3
6. При установлении канала связи и после его установления по HTTPS должны использоваться криптостойкие протоколы шифрования, исключая такие протоколы, как: MD5, SHA-1, 3DES, DES или AES-CBC
7. Все WEB запросы (API) должны выполняться в формате POST. Ссылка на ресурс при обращении не должна содержать параметры запроса

# Создание клиентского сертификата

Пример команды openSSL:

openssl req -newkey rsa:4096 -days 1000 -nodes -keyout client1.pem > client1-req.pem

После чего необходимо заполнить данные сертификата, ответив на вопросы утилиты, пример:

Ignoring -days; not generating a certificate

Generating a RSA private key

................................................................................................................................++++

......................................................................................................................................++++

writing new private key to 'client1.pem'

-----

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]:RU

State or Province Name (full name) [Some-State]:Moscow

Locality Name (eg, city) []:Moscow

Organization Name (eg, company) [Internet Widgits Pty Ltd]:Parter Ltd

Organizational Unit Name (eg, section) []:IT

Common Name (e.g. server FQDN or YOUR name) []:client1.partner.invalid

Email Address []:noreply@partner.invalid

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

An optional company name []

# Подпись клиентского сертификата

Пример команды openSSL:

openssl x509 -req -in client1-req.pem -days 365 -CA rootCA.crt -CAkey rootCA.key -set\_serial 01 > client1-cert.pem

# Примеры использования

## Использование отдельно ключа и сертификата

curl --cert client1-cert.pem --key client1.pem <https://sso.nl-dev.ru:8443>

## Пример использования одного файла, с ключом и сертификатом

Необходимо объединить ключ и сертификат вместе, командой

cat client1.pem client1-cert.pem > client1-combined.pem

После чего можно воспользоваться командой

curl --cert client1-combined.pem https://sso.nl-dev.ru:8443

## Пример ответа сервера на запрос без использования сертификата

curl https://sso.nl-dev.ru:8443

curl: (56) OpenSSL SSL\_read: error:1409445C:SSL routines:ssl3\_read\_bytes:tlsv13 alert certificate required, errno 0

# Меры по предотвращению компрометации

Оба участника взаимодействия должны обеспечить защиту от атак захвата DNS запросов и возможной подмены злоумышленниками DNS серверов или ответов при разрешении имен, в том числе, при разрешении имен серверов из сертификатов

Запрещается копировать или передавать куда-либо актуальные закрытые ключи шифрования

При компрометации центров сертификации или ключей, необходимо выполнить взаимное оповещение и выполнить мероприятия по восстановлению доверия центрам сертификации, смену закрытых ключей шифрования и сертификатов между партнерами

Должна обеспечиваться поддержка сервиса партнером и эксплуатационными службами ИТ Группы компаний. Своевременно устраняться уязвимости, устанавливаться обновления безопасности

Партнер должен на регулярной основе (не реже 2-х раз в год) проводить Pentest клиентской части приложения и сообщать о найденных уязвимостях которые косвенно или напрямую зависят от ответной части на стороне API

Передача сертификата осуществляется на физическом, шифрованном носителе