

Инструкция по генерации личного ключа и запроса на технологический сертификат КПСИС

Для генерации личного ключа и запроса на выпуск технологического сертификата необходимо направить http-запрос на сервис генерации личного ключа и выпуска запроса на ТСОК по адресу сервиса вида «<http://host:port/api/v1/gencertreq>». Адрес размещения сервиса генерации личного ключа КПСИС и выпуска запроса на ТСОК указывается при настройке КПСИС. Для получения сведений о том, на каком именно порте запущен сервис, необходимо находясь в каталоге с `docker-compose.yml` ввести в терминал команду:

```
# docker-compose ps.
```

1.1. Запрос:

Endpoint: <http://host:port/api/v1/gencertreq>.

Method: POST.

Content-Type: application/json

Parameters:

Описание параметров запроса приведено в таблице 30 Руководства системного программиста КПСИС.

Состав параметра «`cert_req_param.cert_info`» для сервиса приведен в таблице 31 Руководства системного программиста КПСИС.

1.2. Сервис возвращает следующий ответ:

Content-Type: application/json

Parameters.

Описание параметров ответа приведено в таблице 32 Руководства системного программиста КПСИС

1.3. Пример запроса:

```
{
  "key_param": {
    "security_level": 128,
    "iteration_count": 10000,
    "users_num": 5,
    "threshold_num": 3,
    "passwords": [
      "12345678",
      "87654321",
      "12345678",
      "87654321",
      "12345678"
    ]
  },
  "cert_req_param": {
```

```

    "type": "service_and_tls",
    "cert_info": {
        "common_name": "*.example.org",
        "description": "Какой-то сервис",
        "organization": "ООО Организация",
        "state": "Минский район",
        "locality": "Минск",
        "street": "ул. Улица, 322, 212212",
        "email": "org@example.com",
        "subject_alt_name": ["*.example.org", "www.example.org"]
    },
    "save_to_file": true
}

```

1.4. Пример ответа:

```

{ "cert_request": "<запрос на СОК в формате BASE64>",
  "error": "0",
  "key": "<личный ключ в ключевом контейнере в формате BASE64>",
  "secret_shards": [
    "-----BEGIN ENCRYPTED PRIVATE KEY-----<значение
частичного секрета 1 в формате BASE64> -----END
ENCRYPTED PRIVATE KEY-----",
    "-----BEGIN ENCRYPTED PRIVATE KEY-----<значение
частичного секрета 2 в формате BASE64> -----END
ENCRYPTED PRIVATE KEY-----",
    "-----BEGIN ENCRYPTED PRIVATE KEY-----<значение
частичного секрета 3 в формате BASE64> -----END
ENCRYPTED PRIVATE KEY-----",
    "-----BEGIN ENCRYPTED PRIVATE KEY-----<значение
частичного секрета 4 в формате BASE64> -----END
ENCRYPTED PRIVATE KEY-----",
    "-----BEGIN ENCRYPTED PRIVATE KEY-----<значение
частичного секрета 1 в формате BASE64> -----END
ENCRYPTED PRIVATE KEY-----" ] }

```

1.5. Сформированный запрос на ТСОК КПСИС (cert_req.req), личный ключ (key.pem) и частичные секреты (shard*.pem) будут находиться в каталоге «esiful-kpsis/data/keygensrvc/».

1.6. Файл запроса на ТСОК КПСИС «cert_req.req» необходимо направить в НЦЭУ вместе с копией заявки на получение услуги посредством Системы технической поддержки (<https://support.nces.by>).