Криптография

1. Получите **КУЦ** ресурс **/v1/crypto/eio**
https://edupirfintech.sberbank.ru:9443/fintech/api/v1/crypto/eio

Выполнить запрос в Swagger
https://edupirfintech.sberbank.ru:9443/fintech/api/swagger-ui.html#!/Crypto/getEioCryptoInfoUsingGET

GET /v1/crypto/eio Получение криптоинформации для ЕИО (КУЦ, пользователи и т.д.)

КАК?
Отправляется запрос на получение **КУЦ** - Код Удостоверяющего Центра
В запросе заполните параметр Authorization – введите **Access Token**

Parameters

Parameter	Value	Description	Parameter Type	Data Type
Authorization	f63f8ba7-a4ad-4e92-b461-2735a1c0bc88-1	Access token организации-клиента, полученный через SSO	header	string

ЧТО?
Из ответа возьмите **ваши** значения certCenterCode – (пример: **A005LT)** и certCenterNum – (пример: **05,** далее по процессу потребуется увеличить на +1)

Response Body


```
{
  "certCenterCode": "A005LT",
  "certCenterNum": "05",
  "certBank": "-----BEGIN CERTIFICATE
```

Криптография

2. Работа со скриптом

Откройте файл - create_windows.txt.

2.1 Сформируйте BICRYPTID
Склейте КУЦ - A005LT, текущий номер сертификата 05 + 1 = 06, ФИО пользователя для которого создаётся сертификат, в итоге получаем - **BICRYPTID="A005LT06sФам66202ИО**".

2.2 Далее для команд необходимо указать верные пути:

"C:\Program Files\OpenSSL-Win64\bin\openssl" - расположение openssl.exe

" C:/Users/CryptoPro/Windows/dev1.ext " - путь до файла из которого сформируется файл ext1

dev1.ext	27.09.2022 13:00
dev2.ext	08.09.2021 17:58
dev3.ext	08.09.2021 17:58
dev4.ext	17.02.2022 10:24

* в файле dev1.ext требуется изменить значение на наш сформированный BICRYPTID

```
asn1=SEQUENCE:ext1
[ext1]
field1=OID:1.2.643.3.123.3.1
field2=OCTWRAP,FORMAT:UTF8,UTF8:A005LT06sФам66202ИО
```

Криптография

2.3 "C:/Users/20266754/Desktop/Aleksandr/Crypto/Crypto-3/CryptoPro/Windows/ext1"" - указываем путь, куда требуется разместить сформированный файл расположения файлов на сервере(dev1 - dev4)

В итоге получаем пример строки:

"C:\Program Files\Openssl\openssl.exe" asn1parse -genconf "C:/Users/20266754/Desktop/Aleksandr/Crypto/Crypto-3/CryptoPro/Windows/**dev1.ext**" -out "C:/Users/20266754/Desktop/Aleksandr/Crypto/Crypto-3/CryptoPro/Windows/**ext1**" -dump

2.4 Дублируем строку 4 раза - меняем **dev1.ext dev2.ext dev3.ext dev4.ext** и в конце строки **ext1 ext2 ext3 ext4:**

"C:\Program Files\Openssl\openssl.exe" asn1parse -genconf "C:/Users/20266754/Desktop/Aleksandr/Crypto/Crypto-3/CryptoPro/Windows/**dev1.ext**" -out "C:/Users/20266754/Desktop/Aleksandr/Crypto/Crypto-3/CryptoPro/Windows/**ext1**" -dump

"C:\Program Files\Openssl\openssl.exe" asn1parse -genconf "C:/Users/20266754/Desktop/Aleksandr/Crypto/Crypto-3/CryptoPro/Windows/**dev2.ext**" -out "C:/Users/20266754/Desktop/Aleksandr/Crypto/Crypto-3/CryptoPro/Windows/**ext2**" -dump

"C:\Program Files\Openssl\openssl.exe" asn1parse -genconf "C:/Users/20266754/Desktop/Aleksandr/Crypto/Crypto-3/CryptoPro/Windows/**dev3.ext**" -out "C:/Users/20266754/Desktop/Aleksandr/Crypto/Crypto-3/CryptoPro/Windows/**ext3**" -dump

"C:\Program Files\Openssl\openssl.exe" asn1parse -genconf "C:/Users/20266754/Desktop/Aleksandr/Crypto/Crypto-3/CryptoPro/Windows/**dev4.ext**" -out "C:/Users/20266754/Desktop/Aleksandr/Crypto/Crypto-3/CryptoPro/Windows/**ext4**" -dump

Криптография

Далее

"C:\Users\20266754\Documents\CSP**cryptcp.exe**" - указать корректный путь до exe файла утилиты командной строки для подписи и шифрования файлов.

2.5. Далее формируем строку:

-dn "CN=Фам66202 Имя66202 Отч66202, C=RU, O="ООО ""ПАРТНЕР- 662""", 2.5.4.11=partner662, T=partner662, E=test_user@sberbank.ru“

- CN=Фам66202 Имя66202 Отч66202 - **ФИО**
- C=RU - **код страны**
- O= ООО ПАРТНЕР-662 - **название организации**
- 2.5.4.11=partner662 - **Подразделение Обозначение: OU**
- T=partner662 - **Должность**
- E=test_user@sberbank.ru - **п\я**

Итоговая команда выглядит следующим образом (**это строка**):

C:\Users\20266754\Documents\CSP\cryptcp.exe" -creatrqst -provtype 80 -dn "CN=Фам66202 Имя66202 Отч66202,C=RU,O=ООО ПАРТНЕР-662,2.5.4.11=partner662,T=partner662,E=test_user@sberbank.ru" -cont "container-test1" -ku -both -pin 11111 -exprt -ext "C:/Users/20266754/Desktop/Aleksandr/Crypto/Crypto-3/CryptoPro/Windows/ext1" -ext "C:/Users/20266754/Desktop/Aleksandr/Crypto/Crypto-3/CryptoPro/Windows/ext2" -ext "C:/Users/20266754/Desktop/Aleksandr/Crypto/Crypto-3/CryptoPro/Windows/ext3" -ext "C:/Users/20266754/Desktop/Aleksandr/Crypto/Crypto-3/CryptoPro/Windows/ext4" "C:/Users/20266754/Desktop/Aleksandr/Crypto/Crypto-3/CryptoPro/Windows/request_6_cms.der"

Криптография

2.6 После формирования результирующего файла-запроса *******.der в нем нужно будет поправить:**

request_6_cms.der

- Удалите слово NEW в начале и конце файла, если есть.
- Замените все переносы строк Windows в файле, в результате получится файл, с содержимым **в виде строки**)

КАК: Notepad++ Команда Replace

Find what: “\r\n”

Replace with: “\\n“

- Вставьте в начало -----BEGIN CERTIFICATE REQUEST-----
- Вставьте в конец -----END CERTIFICATE REQUEST-----

Криптография

Подготовленный файл запроса сертификата.

request_6_cms.der

Должен получиться такой файл.der:

-----BEGIN CERTIFICATE REQUEST-----\nMIIDQzCCAvACAQAwgbUxKjAoBgkqhkiG9w0BCQEWG0FsVmlrdEt1em5ldHNvdkBz
\nYmVyYmFuay5ydTETMBEGA1UEDAwKcGFydG5lcjY2MjETMBEGA1UECwwKcGFydG5l
\ncjY2MjEiMCAGA1UECgwZ0J7QntCeINCf0JDQoNCi0J3QldCgLTY2MjELMAkGA1UE
\nBhMCUlUxLDAqBgNVBAMMI9Ck0LDQvDY2MjAyINCY0LzRjzY2MjAyINCe0YLRhzY2
\nMjAyMGYwHwYIKoUDBwEBAQEwEwYHKoUDAgIkAAYIKoUDBwEBAgIDQwAEQG9aFM78
\nCAhj7IE+fIiivKlgnCKwlEDuV90wiRN0O5C5oDTRntVYZsnguQOCf31vbpFijJLl\n3ADz1FlfUFmotF+gggHJMBoGCisGAQQBgjcNAgMxDBYKNi4yLjkyMDAuMjBOBgkr
\nBgEEAYI3FRQxQTA/AgEFDB1DQUItV1NOLTAwMTU1MDguc2lnbWEuc2JyZi5ydQwO
\nU0lHTUFcMjAyNjY3NTQMC2NyeXB0Y3AuZXhlMIGPBgorBgEEAYI3DQICMYGAMH4C
\nAQEedgBDAHIAeQBwAHQAbwAtAFAAcgBvACAARwBPAFMAVAAgAFIAIAAzADQALgAx
\nADAALQAyADAAMQAyACAAQwByAHkAcAB0AG8AZwByAGEAcABoAGkAYwAgAFMAZQBy
\nAHYAaQBjAGUAIABQAHIAbwB2AGkAZABlAHIDAQAwgcgGCSqGSIb3DQEJDjGBujCB
\ntzATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMCBPAwJQYHKoUDA3sD
\nAQQaDBhBMDA1TFQwNHPQpNCw0Lw2NjIwMtCY0J4wEgYDVR0TAQH/BAgwBgEBAAIB
\nADAUBgcqhQMDewMEBAkGByqFAwN7BQQwIAYIKoUDBwEBAQEEFDASBgcqhQMCAh8B
\nBgcqhQMCAiMCMB0GA1UdDgQWBBSZhRD5DPVqh6deoXRk2CMyv6H2wzAKBggqhQMH
\nAQEDAgNBAFYNlXKIgsqSFM1M01XAGA6t1Ld35UjcoP4DzIFi6VIFCnIXK6c8rPwX\niFqK2hBnYEI1bmM14mX5Hg67WYEyWu8=\n-----END CERTIFICATE REQUEST-----

Криптография

Сформируйте запрос на создание нового сертификата.

3. Формируем json запрос для отправки:

*Параметр externalID "32a6dd81-103a-4d3a-8e9b-0ba4b528f5f6" – формируется вами самостоятельно.


```
{
  "email": "test_user@sberbank.ru",
  "externalId": "32a6dd81-103a-4d3a-8e9b-0ba4b528f5f6",
  "login": "User662-00-02",
  "number": "06",
  "orgName": "ООО \"ПАРТНЕР-662\"",
  "pkcs10": {
    "bicryptId": "A005LT06sФам66202ИО",
    "cms": "-----BEGIN CERTIFICATE REQUEST-----
\nMIIDQzCCAvACAQAwgbUxKjAoBgkqhkiG9w0BCQEWG0FsVmlrdEt1em5ldHNvdkBz\nYmVyYmFuay5ydTETMBEGA1UEDAwKcGFydG5lcjY2MjETMBEGA1UECwwKcGFydG5l\ncjY
2MjEiMCAGA1UECgwZ0J7QntCeINCf0JDQoNCi0J3QldCgLTY2MjELMAkGA1UE\nBhMCUlUxLDAqBgNVBAMMI9Ck0LDQvDY2MjAyINCY0LzRjzY2MjAyINCe0YLRhzY2\nMjAyMGYwH
wYIKoUDBwEBAQEwEwYHKoUDAgIkAAYIKoUDBwEBAgIDQwAEQG9aFM78\nCAhj7IE+fIiivKlgnCKwlEDuV90wiRN0O5C5oDTRntVYZsnguQOCf31vbpFijJLI\n3ADz1FlfUFmotF+gg
gHJMBoGCisGAQQBgjcNAgMxDBYKNi4yLjkyMDAuMjBOBgkr\nBgEEAYI3FRQxQTA/AgEFDB1DQUItV1NOLTAwMTU1MDguc2lnbWEuc2JyZi5ydQwO\nU0lHTUFcMjAyNjY3NTQMC
2NyeXB0Y3AuZXhlMIGPBgorBgEEAYI3DQICMYGAMH4C\nAQEedgBDAHIAeQBwAHQAbwAtAFAAcgBvACAARwBPAFMAVAAgAFIAIAAzADQALgAx\nADAALQAyADAAMQAyACAAQ
wByAHkAcAB0AG8AZwByAGEAcABoAGkAYwAgAFMAZQBy\nAHYAaQBjAGUAIABQAHIAbwB2AGkAZABlAHIDAQAwgcgGCSqGSIb3DQEJDjGBujCB\ntzATBgNVHSUEDDAKBggrBgE
FBQcDBDAOBgNVHQ8BAf8EBAMCBPAwJQYHKoUDA3sD\nAQQaDBhBMDA1TFQwNHPQpNCw0Lw2NjIwMtCY0J4wEgYDVR0TAQH/BAgwBgEBAAIB\nADAUBgcqhQMDewMEBAkG
ByqFAwN7BQQwIAYIKoUDBwEBAQEEFDASBgcqhQMCAh8B\nBgcqhQMCAiMCMB0GA1UdDgQWBBSZhRD5DPVqh6deoXRk2CMyv6H2wzAKBggqhQMH\nAQEDAgNBAFYNlXKIgsq
SFM1M01XAGA6t1Ld35UjcoP4DzIFi6VIFCnIXK6c8rPwX\niFqK2hBnYEI1bmM14mX5Hg67WYEyWu8=\n-----END CERTIFICATE REQUEST-----"
  },
  "userName": "Фам66202 Имя66202 Отч66202",
  "userPosition": "partner662"
}
```

Криптография

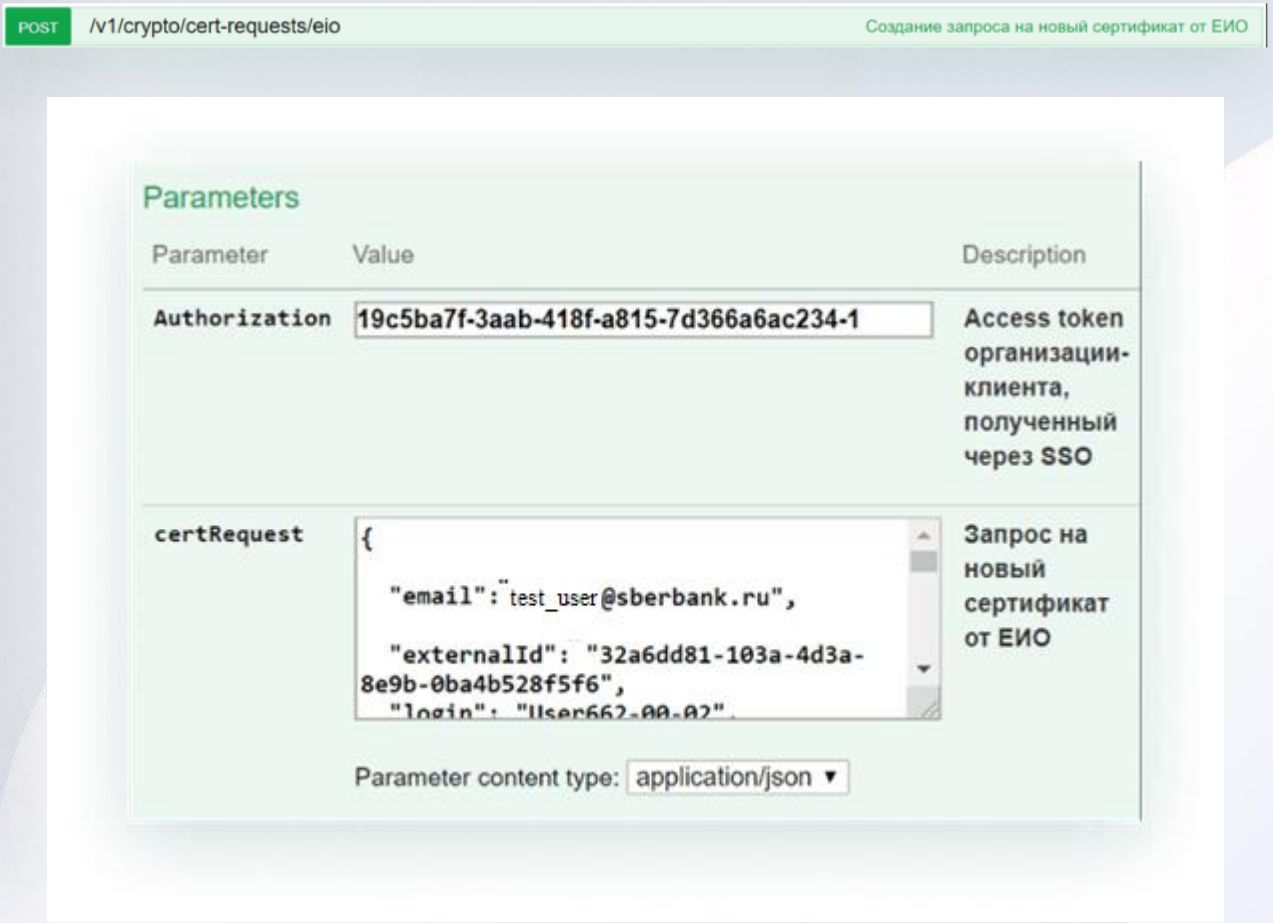
3.1 Отправка запроса в Swagger

КАК?

- Ресурс v1/crypto/cert-request/eio

https://edupirfintech.sberbank.ru:9443/fintech/api/swagger-ui.html#!/Crypto/createCertRequestEioUsingPOST

- Для отправки запроса на создание сертификата ранее сформированный json запрос поместите в поле certRequest



Криптография

Получаем ответ:

Response Body


```
{
  "externalId": "32a6dd81-103a-4d3a-8e9b-0ba4b528f5f6",
  "userName": "Фам66202 Имя66202 Отч66202",
  "userPosition": "partner662",
  "orgName": "ООО \"ПАРТНЕР-662\"",
  "email": "test_user@sberbank.ru",
  "pkcs10": {
    "cms": "-----BEGIN CERTIFICATE REQUEST-----\nMIIDQzCCAvACAQAwgbUxKjAoBgkqhkiG9w0BCQEWG0FsVmlrdEt1em5ldHNvdkBz\nYmVyYmFuay5y
    "bicryptId": "A005LT06s0am66202MO"
  },
  "bankStatus": "DELIVERED",
  "bankComment": "Public Key DS: 6f5a14cefc080863ec813e7c88a2bca9609c22b09440ee57dd308913743b90b9\na034d19ed55866c9e0b903827f7d
  "number": "06",
  "login": "User662-00-02"
}
```

Криптография

4. Получите статус сертификата.
КАК?

- Ресурс GET /v1/crypto/cert-requests/eio/{externalId}/state
- Swagger https://edupirfintech.sberbank.ru:9443/fintech/api/swagger-ui.html#!/Crypto/getStatusEioUsingGET

GET /v1/crypto/cert-requests/eio/{externalId}/state — Получение статуса запроса на новый сертификат для ЕИО

Authorization - Access Token

externalID - придумали ранее сами

Parameters

Parameter	Value	Description	Parameter Type	Data Type
Authorization	19c5ba7f-3aab-418f-a815-7d366a6ac234-1	Access token организации-клиента, полученный через SSO	header	string
externalId	32a6dd81-103a-4d3a-8e9b-0ba4b528f5f6	Внешний UUID запроса на новый сертификат	path	string

Response Body


```
{
  "bankStatus": "ACCEPTED",
  "bankComment": "Public Key DS: 6f5a14cefc080863ec813e7c88a2bca9609c22b09440ee57dd308913743b90b9\na034d19ed55866c9e0b903827f7d
  "channelInfo": null
}
```


ВАЖНО! Только после статуса ACCEPTED можно запрашивать печатную форму (заявление на выпуск сертификата)!

Криптография

5. Скачайте заявление на выпуск сертификата.
КАК?

- Ресурс GET /v1/crypto/cert-requests/eio/{externalId}/print
- Swagger https://edupirfintech.sberbank.ru:9443/fintech/api/swagger-ui.html#!/Crypto/printEioUsingGET

GET	/v1/crypto/cert-requests/eio/{externalId}/print	Получение печатной формы запроса на новый сертификат для ЕИО

Authorization - Access Token

externalId - придумали ранее сами

Parameters

Parameter	Value	Description	Parameter Type	Data Type
Authorization	fa87bb1e-51db-4ccd-a318-620a38b01f8e-1	Access token организации-клиента, полученный через SSO	header	string
externalId	32a6dd81-103a-4d3a-8e9b-0ba4b528f5f6	Внешний UUID запроса на новый сертификат	path	string

Response Body

```
no content
```

Response Code

```
0
```

Response Headers

```
{
  "error": "no response from server"
}
```

*Если метод **вернул** ошибку, то необходимо воспользоваться обходным решением

Криптография

5.1 Обходное решение, если метод вернул ошибку.

КАК?

Направьте запрос на ящик supportdbo2@sberbank.ru по следующему шаблону:

Коллеги, привет!

Просьба выпустить сертификат.

Тест
Client_id 111322
BICRYPTID="A005LT06sФам66202ИО"
externalId": "32a6dd81-103a-4d3a-8e9b-0ba4b528f5f6"
ООО ПАРТНЕР-662

После того, как заявка будет отработана, вам будет направлен ответ, что печатная форма сертификата сформирована и запрос отправлен в Удостоверяющий центр для подготовки сертификата

Криптография

5.2 Получите статус сертификата

КАК?

- Ресурс GET /v1/crypto/cert-requests/eio/{externalId}/state
- https://edupirfintech.sberbank.ru:9443/fintech/api/swagger-ui.html#!/Crypto/getStatusEioUsingGET

GET	/v1/crypto/cert-requests/eio/{externalId}/state	Получение статуса запроса на новый сертификат для ЕИО

Если статус PUBLISHED_BY_BANK - перейдите к следующему шагу

Response Body


```
{
  "bankStatus": "PUBLISHED_BY_BANK",
  "bankComment": "Public Key DS: 6f5a14cefc080863ec813e7c88a2bca9609c22b09440ee57dd308913743b90b9\na034d19ed55866c9e0b903827f7d
  "channelInfo": null
}
```

Криптография

6. Активируйте сертификат POST /v1/crypto/cert-requests/eio/{externalId}/activate

POST	/v1/crypto/cert-requests/eio/{externalId}/activate	Активация сертификата для ЕИО

https://edupirfintech.sberbank.ru:9443/fintech/api/swagger-ui.html#!/Crypto/activateEioUsingPOST
Получаем успешный код ответа - 200

Response Code

```
200
```

7. Скачайте выпущенный сертификат GET /v1/crypto/eio

GET	/v1/crypto/eio	Получение криптоинформации для ЕИО (КУЦ, пользователи и т.д.)

https://edupirfintech.sberbank.ru:9443/fintech/api/swagger-ui.html#!/Crypto/getEioCryptoInfoUsingGET

Response Code

```
200
```

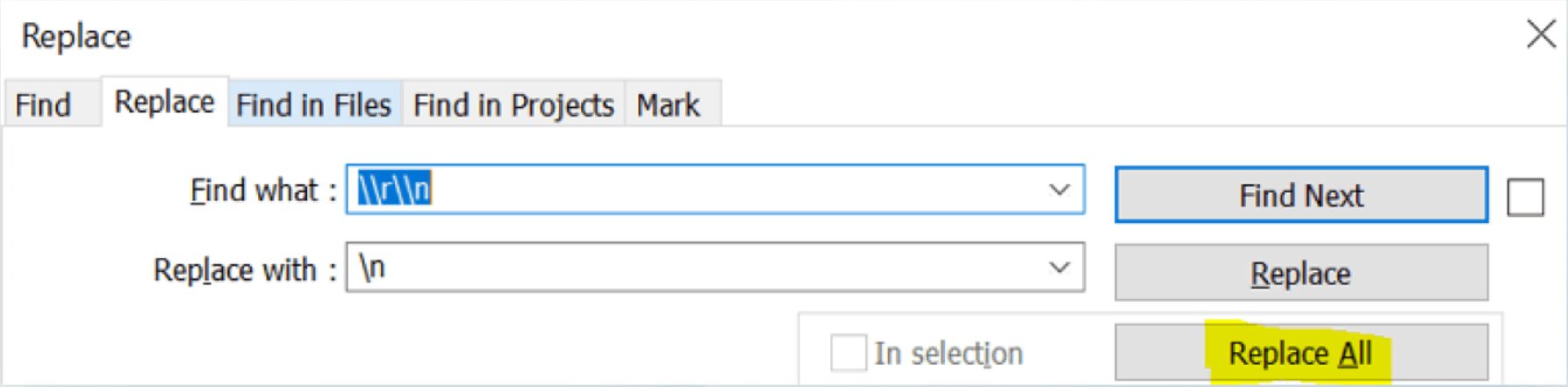
В ответе Response Body получаем массив данных

Криптография

8. Скачайте (скопируйте) сертификат открытого ключа (блок «certificateInfos», поле «cert») в текстовый файл.


```
"certificateInfos": [
  {
    "issuer": "EMAILADDRESS=casbrf@sberbank.ru, CN=ПАО Сбербанк УЦ (ТЕСТ Q), OU=Департамент безопасности (ТЕСТ), O=
    "serialNumber": "7A8F20A728A14E29A9F8",
    "uuid": "2716bd9a-1583-46fd-a385-8e42168f6bef",
    "active": true,
    "cert": "-----BEGIN CERTIFICATE-----\r\nMIIEPjCCA+ugAwIBAgIKeo8gpyihTimp+DAKBggqhQMHAQEDAjCCAWsxGzAZBgNV\r\nBAg
  }
]
```


8.1 Преобразуйте строку значения сертификата в столбец.
КАК?
Notepad++ Команда Replace
Find what: “\\r\\n”
Replace with: “\n“



Криптография

После добавления символов переноса строк, содержимое сертификата выглядит, как столбец.

Сохраняем полученный файл с расширением *.cer


```
-----BEGIN CERTIFICATE-----
MIIEPjCCA+ugAwIBAgIKeo8gpyihTimp+DAKBggqhQMHAQEDAjCCAWsxGzAZBgNV
BAgMEjc3INCzLtCc0L7RgdC60LLQsDEYMBYGA1UEBwwP0LMu0JzQvtGB0LrQstCw
MRowGAYIKoUDA4EDAQESDDAwNzcwNzA4Mzg5MzEmMCQGA1UECQwd0YPQuy4g0JLQ
sNCy0LjQu9C+0LLQsCwg0LQuMTkxGDAWBgUqhQNkARINMTAyNzcwMDEzMjE5NTEL
MAkGA1UEBhMCUlUxKzApBgNVBAoMItCf0JDQniDQodCx0LXRgNCx0LDQvdC6ICjQ
otCV0KHQoikxQzBBBgNVBAsMOtCU0LXQv9Cw0YDRgtCw0LzQtdC90YIg0LHQtdC3
0L7Qv9Cw0YHQvdC+0YHRgtC4ICjQotCV0KHQoikxMjAwBgNVBAMMKdCf0JDQniDQ
odCx0LXRgNCx0LDQvdC6INCj0KYgKNCi0JXQodCiIFEpMSEwHwYJKoZIhvcNAQkB
FhJjYXNicmZAc2JlcmJhbmsucnUwHhcNMjIwOTMwMDgwNTAwWhcNMjMxMjMwMDgx
MDI4WjCBtTEqMCgGCSqGSIb3DQEJARYbQWxWaWt0S3V6bmV0c292QHNiZXJiYW5r
LnJ1MRMwEQYDVQQMDApwYXJ0bmVyNjYyMRMwEQYDVQQLDApwYXJ0bmVyNjYyMSIw
IAYDVQQKDBnQntCe0J4g0J/QkNCg0KLQndCV0KAtNjYyMQswCQYDVQQGEwJSVTEs
MCoGA1UEAwwj0KTQsNC8NjYyMDIg0JjQvNGPNjYyMDIg0J7RgtGHNjYyMDIwZjAf
BggqhQMHAQEBATATBgcqhQMCAiQABggqhQMHAQECAgNDAARAb1oUzvwICGPsgT58
iKK8qWCcIrCUQO5X3TCJE3Q7kLmgNNGe1VhmyeC5A4J/fW9ukWKMksjcAPPUWV9Q
Wai0X6OCARswggEXMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIE
8DAlBgcqhQMDewMBBBoMGEEwMDVMVDA0c9Ck0LDQvDY2MjAy0JjQnjASBgNVHRMB
Af8ECDAGAQEAAgEAMBQGByqFAwN7AwQECQYHKoUDA3sFBDAgBggqhQMHAQEBAQQU
MBIGByqFAwICHwEGByqFAwICIwIwHQYDVR0OBBYEFJmFEPkM9WqHp16hdGTYIzK/
ofbDMD0GA1UdHwQ2MDQwMqAwoC6GLGh0dHA6Ly93d3dsLnNiZXJiYW5rLnJ1L2Nh
L3Rlc3RfMjAxMng1MDkuY3JsMB8GA1UdIwQYMBaAFER+sfJUNI8vPMx8c81kE7Fa
tnguMAoGCCqFAwcBAQMCA0EAfixHIv2Ohwwq89LpNPgsXI//tFC4vCuj2dwXTHFp
RUcLLYFUfsVsOP9nxJKJgXzO+b9ZUPVT4UoifnLMnuB/QA==
-----END CERTIFICATE-----
```

Криптография

8.2 Далее (скопируйте) скачайте цепочку корневых и промежуточных сертификатов банка. Используем значения из блока certsCA).


```
"certsCA": [
  "-----BEGIN CERTIFICATE-----\r\nMIIEFTCCA8SgAwIBAgIIMDBDQTAxNTkwCAYGKoUDAgIDMIIBEjELMAkGA1UEBhMC\r\nUlUxLzAtBgNVBAoMJtCe
  "-----BEGIN CERTIFICATE-----\r\nMIIENTCCA+SgAwIBAgIIMDBDQTAxNjAwCAYGKoUDAgIDMIIBEjELMAkGA1UEBhMC\r\nUlUxLzAtBgNVBAoMJtCe
  "-----BEGIN CERTIFICATE-----\r\nMIIENzCCA+agAwIBAgIIMDBDQTAxNjEwCAYGKoUDAgIDMIIBEjELMAkGA1UEBhMC\r\nUlUxLzAtBgNVBAoMJtCe
  "-----BEGIN CERTIFICATE-----\nMIIE7TCCBJqgAwIBAgIKdo4eLjUUTAsXvzAKBggqhQMHAQEDAjCCAXcxGzAZBgNV\nBAgMEjc3INCzLtCc0L7RgdC6
  "-----BEGIN CERTIFICATE-----\nMIIFEDCCBL2gAwIBAgIKdo4gnesMRx3/sjAKBggqhQMHAQEDAjCCAXcxGzAZBgNV\nBAgMEjc3INCzLtCc0L7RgdC6
  "-----BEGIN CERTIFICATE-----\r\nMIIHdDCCByGgAwIBAgIKdrQ86xS2EePCzDAKBggqhQMHAQEDAjCCAWQxGzAZBgNV\r\nBAgMEjc3INCzLtCc0L7R
```


8.2 Аналогично сертификату пользователя, преобразуйте каждую строку в столбец и сохраните в раширением *.cer :
КАК?
Notepad++ Команда Replace

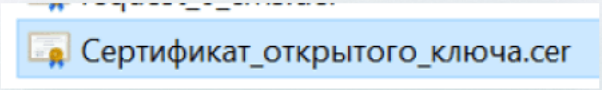
Включите отображение скрытых\непечатных символов.
Там, где строка начинается с \r\n – сделайте замену
Find what: “\\r\\n”
Replace with: “\n“

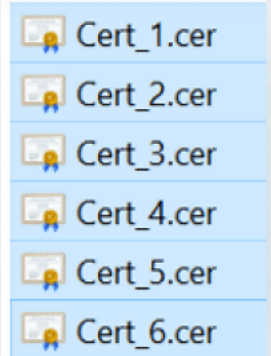
Там, где строка начинается с \n – сделайте замену
Find what: “\\n”
Replace with: “\n“

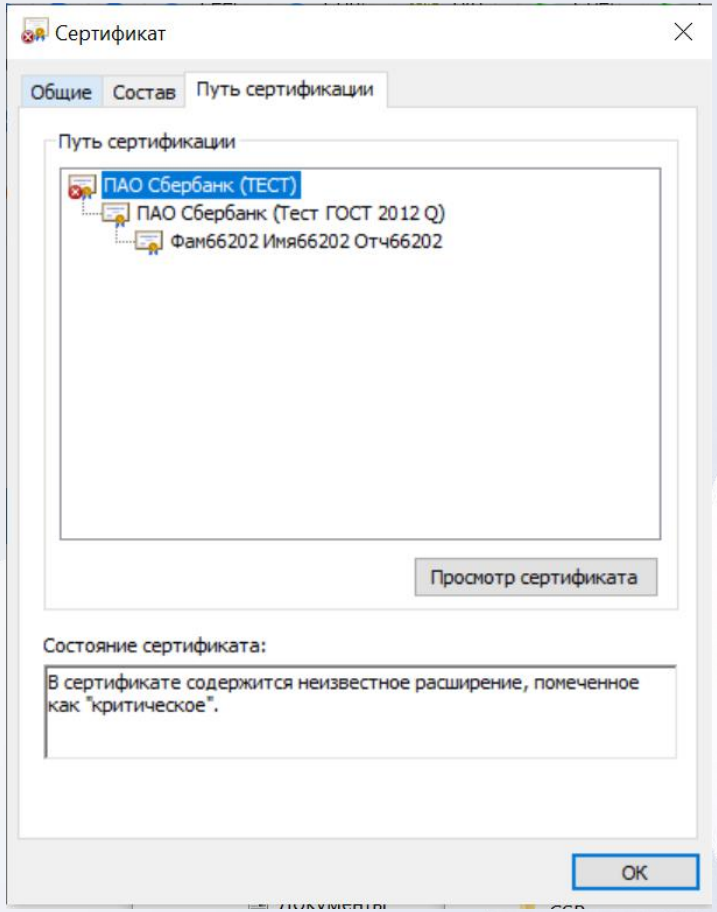
Криптография

9. Установите полученные сертификаты.

9.1 Откройте сертификат (пользователя) открытого ключа и убедитесь, что на вкладке «Путь сертификации» отсутсвуют какие-либо ошибки, а не как на скрине и так же присутствует полная цепочка.

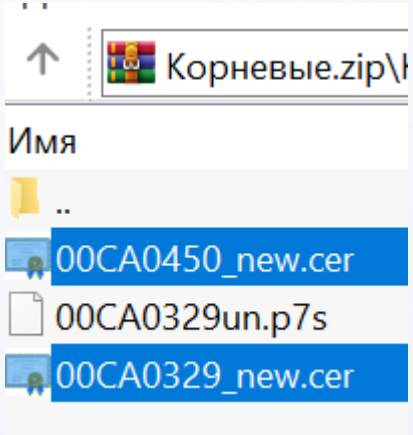


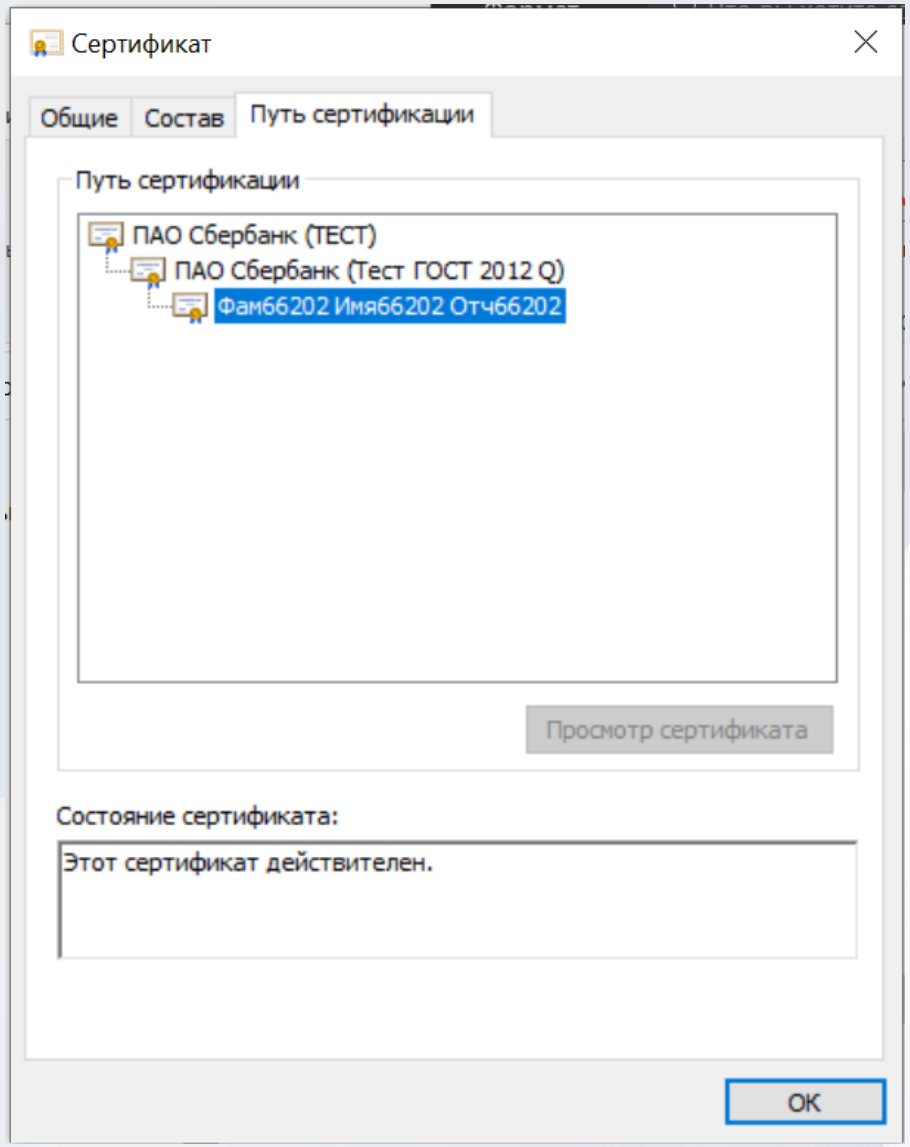




Криптография

10. Для устранения ошибки корневого сертификата установите на ваш ПК сертификаты из архива во вложении «Корневые.zip».

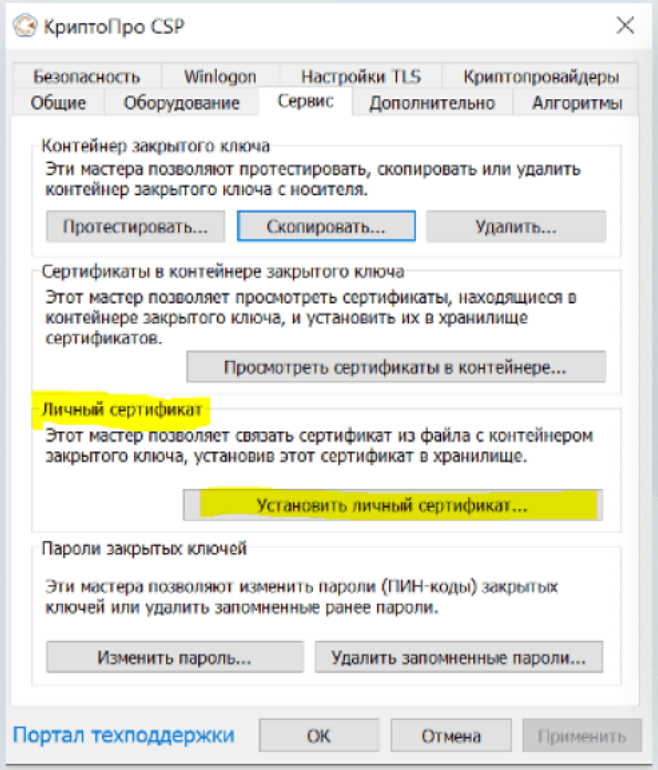


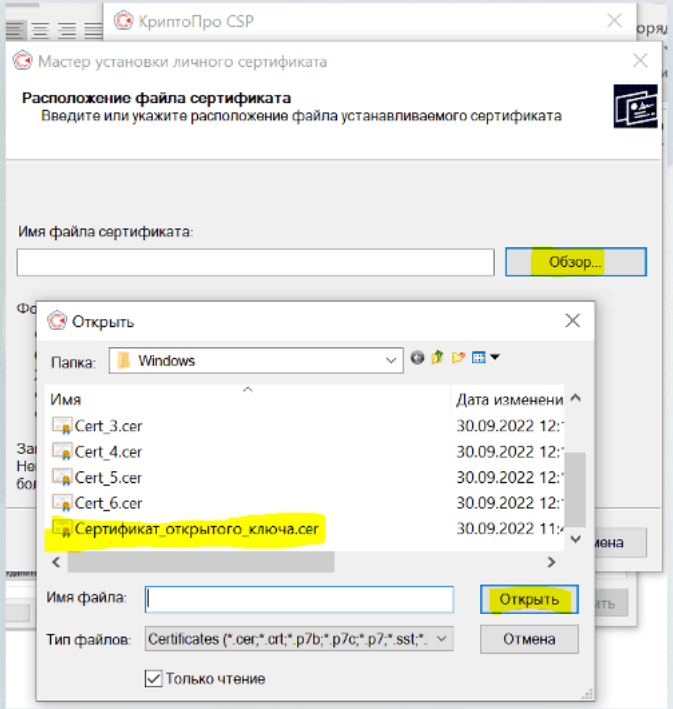


Криптография

11. Добавьте сертификат пользователя в CryptoPro

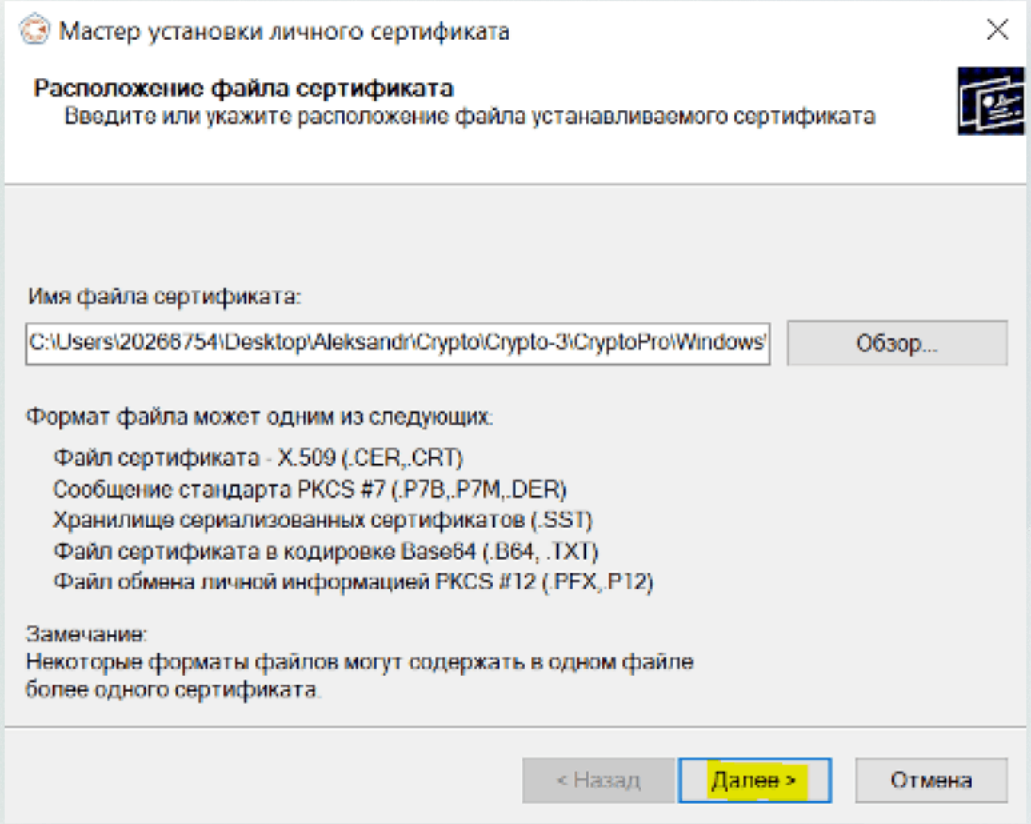
- Запустите CryptoPro
- Вкладка Сервис
- Нажмите «Установить Личный сертификат… » – выберите сформированный ранее Сертификат открытого ключа.

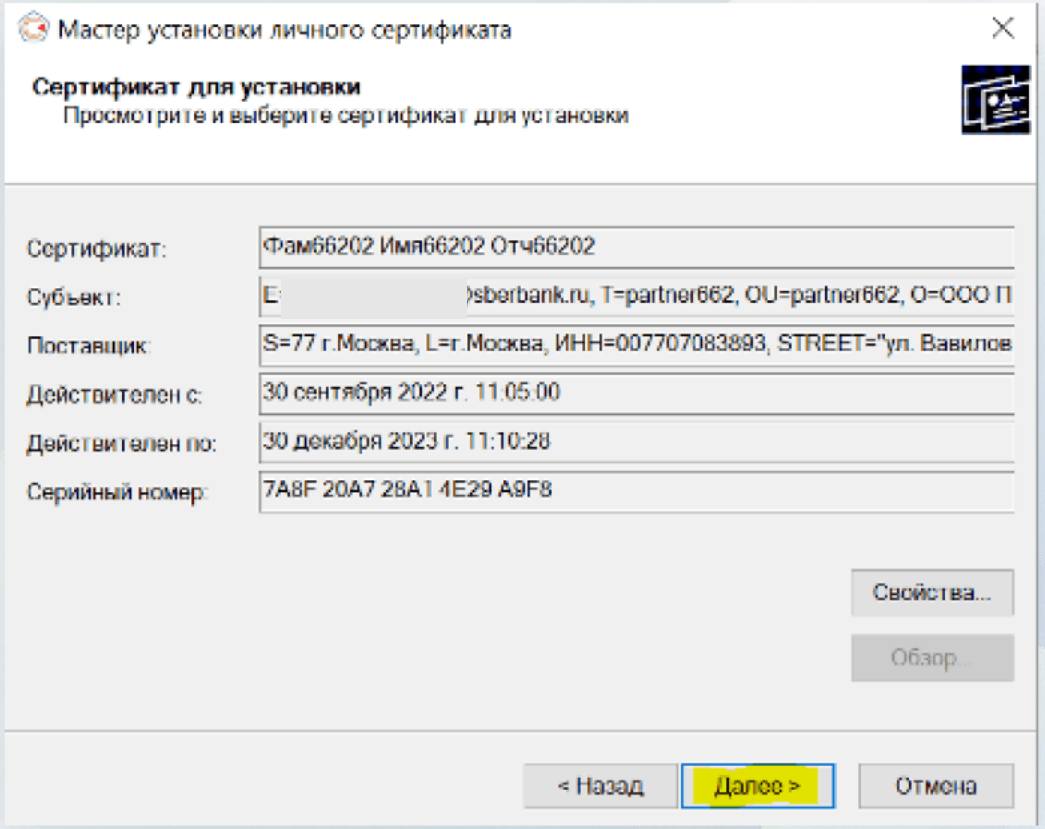




Криптография

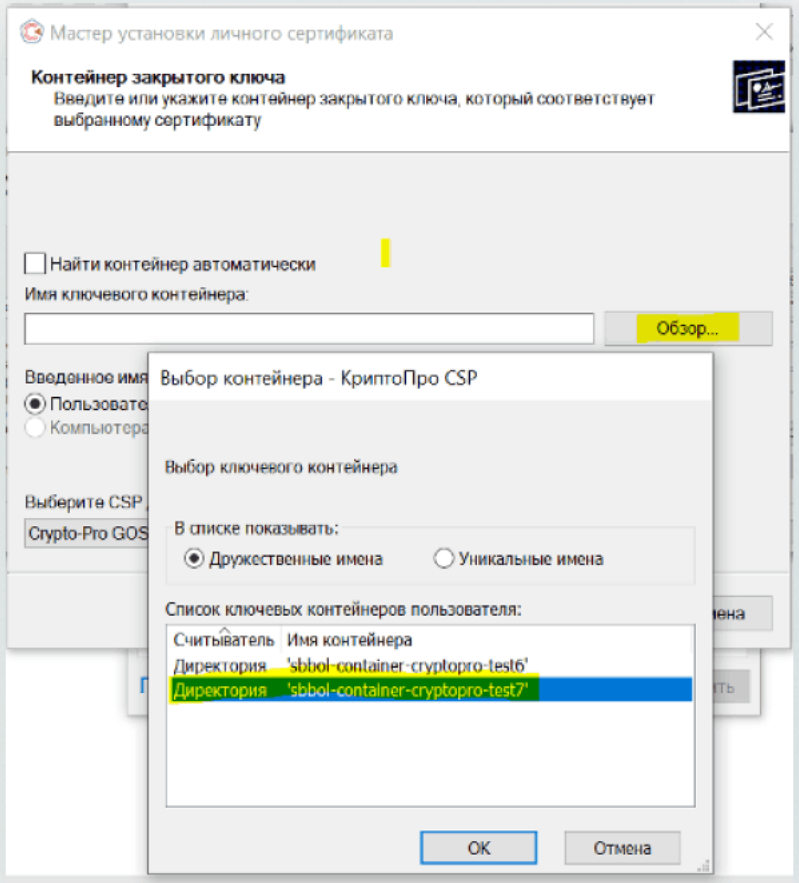
Далее

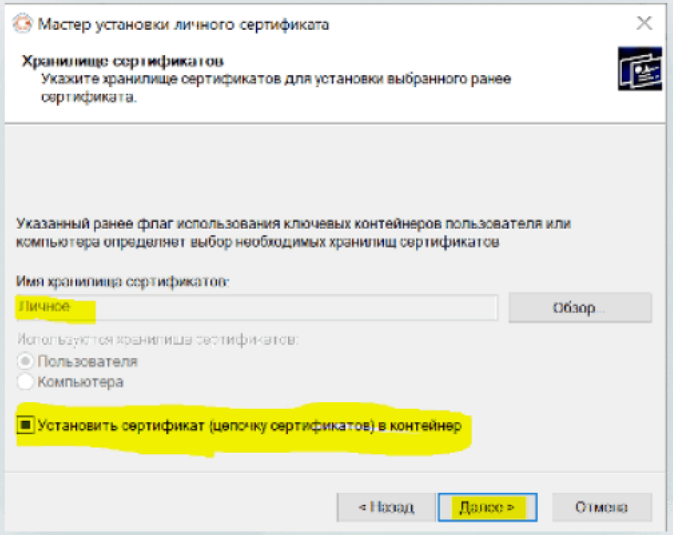


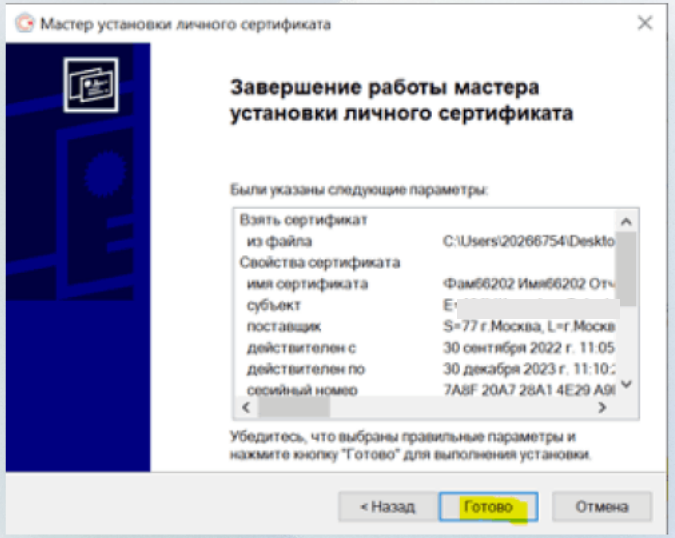


Криптография

Контейнер закрытого ключа

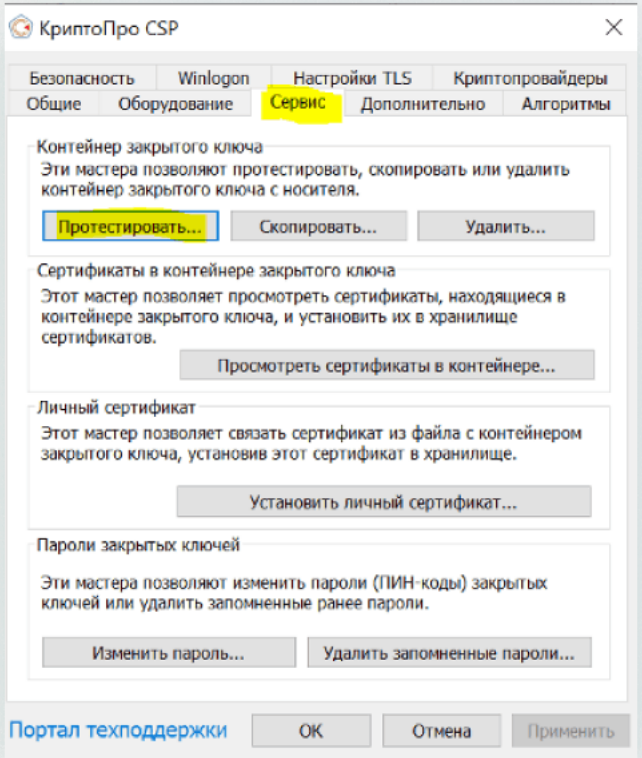


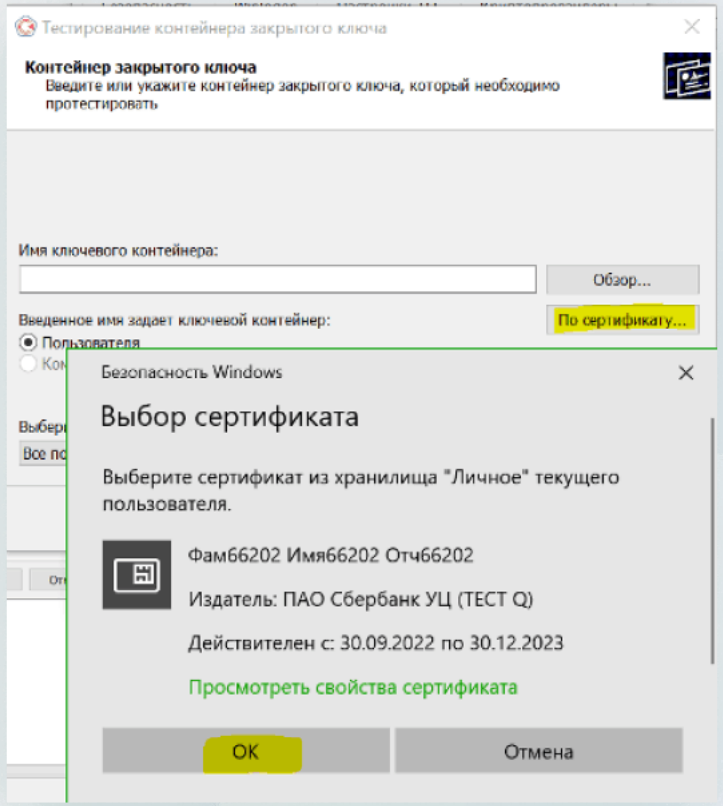


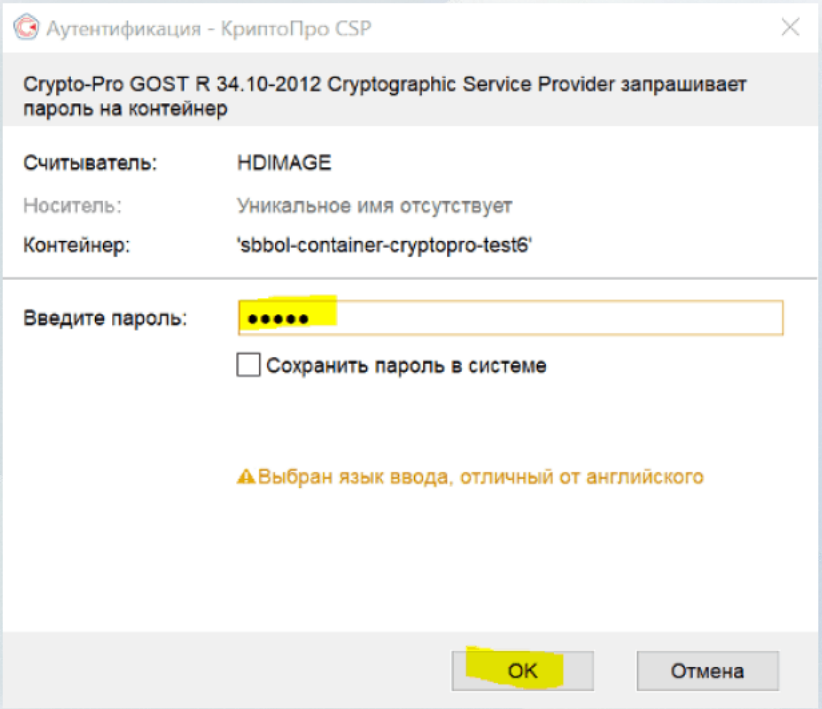


Криптография

Протестируйте

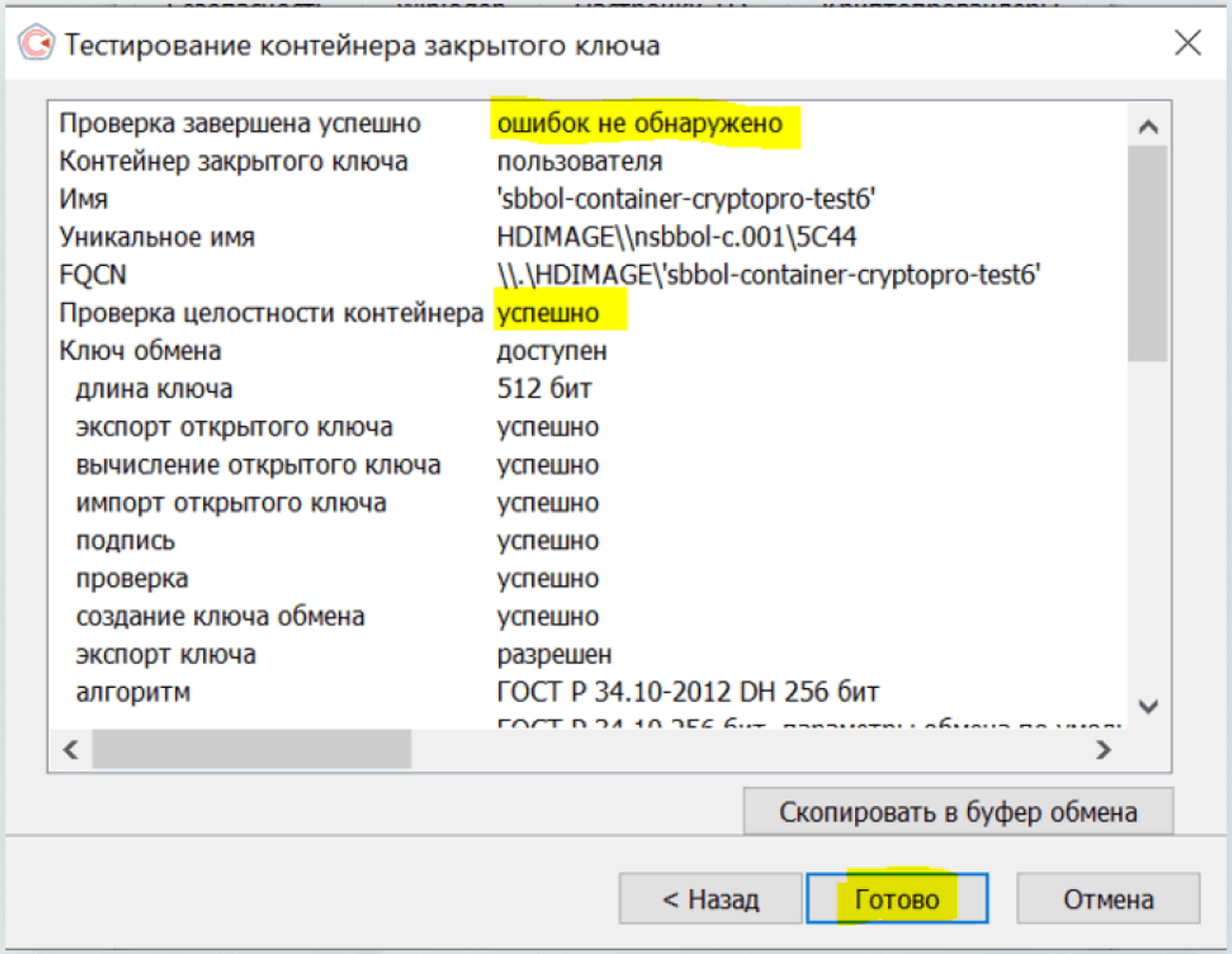






Криптография

Проверка выполнена успешно.



Криптография

Формирование дайджеста документа

1) Формирование дайджеста отправляемого документа (рублёвое платёжное поручение).

Файл digest_rpp.txt

https://developers.sber.ru/docs/ru/sberbusinessapi/host/rpp/payments#format-daydzhesta-rpp4

Сформированный дайджест сохраните на компьютере в файле (далее понадобится для команды формирования Электронной Подписи).

amount=1.21
date=2023-01-17
externalId=ee17342c-1232-4320-aca9-e736e49c8d3f
operationCode=01
payeeAccount=40702810038363663755
payeeBankBic=044525225
payeeBankCorrAccount=30101810400000000225
payeeInn=7709730320
payeeKpp=583501001
payeeName=Общество с ограниченной ответственностью ООО "РОМАШКА“
payerAccount=40702810940303423014
payerBankBic=044525225
payerBankCorrAccount=30101810400000000225
payerInn=5051775164
payerKpp=770701001
payerName=ООО "ПАРТНЕР-662“
priority=5
purpose=Оплата заказа №123. НДС нет.

Криптография

2) Подписание дайджеста документа ЭЦП пользователя
Электронная подпись создаётся по дайджесту следующей командой:

"C:\Users\20266754\Documents\CSP\cryptcp.exe" -signf -detached -dir "C:\Users\20266754\Desktop\Aleksandr\Crypto\Crypto-3\CryptoPro\Windows\Materials\SBER_API_2" -dn "CN=Фам66202 Имя66202 Отч66202" "C:\Users\20266754\Desktop\Aleksandr\Crypto\Crypto-3\CryptoPro\Windows\Materials\SBER_API_2\digest.txt" -hashalg 1.2.643.7.1.1.2.2 -pin 11111

Описание команды:

"C:\Users\20266754\Documents\CSP\cryptcp.exe“ – путь до исполняемого файла cryptcp.
"C:\Users\20266754\Desktop\Aleksandr\Crypto\Crypto-3\CryptoPro\Windows\Materials\SBER_API_2" – путь до создаваемых файлов
"CN=Фам66202 Имя66202 Отч66202" - именной отпечаток сертификата
"C:\Users\20266754\Desktop\Aleksandr\Crypto\Crypto-3\CryptoPro\Windows\Materials\SBER_API_2\digest.txt" - путь до сформированного дайджеста документа.
-hashalg 1.2.643.7.1.1.2.2 -pin 11111 – указание алгоритма шифрования и пин кода для крипто контейнера.

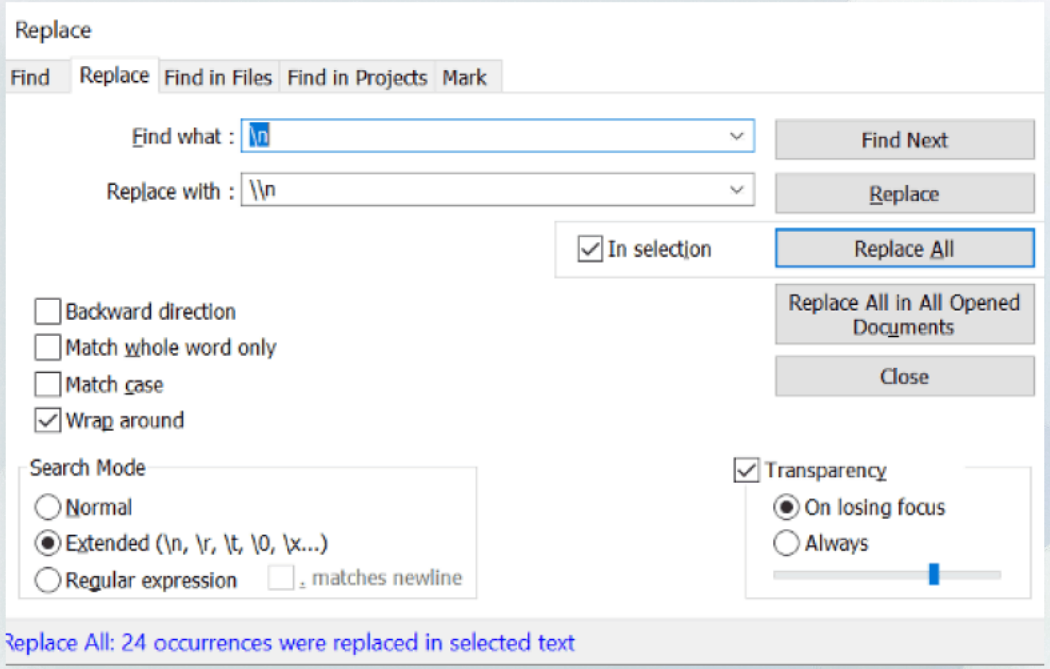
Криптография

В результате получаем дайджест ЭП, результирующий файл подписи пользователя digest_rpp.txt.sgn

Ниже представлено содержимое с демонстрацией скрытых символов переноса строк.


```
MIAGCSqGSIb3DQEHAqCAMIACAQExDjAMBggqhQMHAQECAgUAMIAGCSqGSIb3DQEH
AQAAMYIEJTCCBCECAQEwggF7MIIBazEbMBkGA1UECAwSNzcg0LMu0JzQvtGB0LrQ
stCwMRgwFgYDVQQHDA/Qsy7QnNC+0YHQutCy0LAxGjAYBggqhQMDgQMBARIMMDA3
NzA3MDgzODkzMSYwJAYDVQQJDB3Rg9C7LiDQktCw0LLQuNC70L7QstCwLCDQtC4x
OTEYMBYGBSqFA2QBEg0xMDI3NzAwMTMyMTk1MQswCQYDVQQGEwJSVTErMCkGA1UE
Cgwi0J/QkNCeINCh0LHQtdGA0LHQsNC90LogKNCi0JXQodCiKTFDMEEGA1UECww6
0JTQtdC/0LDRgNGC0LDQvNC10L3RgiDQsdC10LfQvtC/0LDRgdC90L7RgdGC0Lgg
KNCi0JXQodCiKTEyMDAGA1UEAwwp0J/QkNCeINCh0LHQtdGA0LHQsNC90Log0KPQ
piAo0KLQldCh0KIgUSkxITAfBgkqhkiG9w0BCQEWEmNhc2JyZkBzYmVyYmFuay5y
dQIKeo8gpyihTimp+DAMBggqhQMHAQECAgUAoIICPzAYBgkqhkiG9w0BCQMxCwYJ
KoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0yMjEwMTAxMzI3MzFaMC8GCSqGSIb3
DQEJBDEiBCB+shaDtXrlF82j/tWoZNOPpg9WuRYrE9EDlwghOQ8IdjCCAdIGCyqG
SIb3DQEJEAIvMYIBwTCCAb0wggG5MIIBtTAKBggqhQMHAQECAgQgQeEh9Npfx8wm
gSTIgmm/tjT5wZalRa0zV8vboZKxXX4wggGDMIIBc6SCAW8wggFrMRswGQYDVQQI
DBI3NyDQsy7QnNC+0YHQutCy0LAxGDAWBgNVBAcMD9CzLtCc0L7RgdC60LLQsDEa
MBgGCCqFAwOBAwEBEgwwMDc3MDcwODM4OTMxJjAkBgNVBAkMHdGD0LsuINCS0LDQ
stC40LvQvtCy0LAsINC0LjE5MRgwFgYFKoUDZAESDTEwMjc3MDAxMzIxOTUxCzAJ
BgNVBAYTAlJVMSswKQYDVQQKDCLQn9CQ0J4g0KHQsdC10YDQsdCw0L3QuiAo0KLQ
ldCh0KIpMUMwQQYDVQQLDDrQlNC10L/QsNGA0YLQsNC80LXQvdGCINCx0LXQt9C+
0L/QsNGB0L3QvtGB0YLQuCAo0KLQldCh0KIpMTIwMAYDVQQDDCnQn9CQ0J4g0KHQ
sdC10YDQsdCw0L3QuiDQo9CmICjQotCV0KHQoiBRKTEhMB8GCSqGSIb3DQEJARYS
Y2FzYnJmQHNiZXJiYW5rLnJ1Agp6jyCnKKFOKan4MAoGCCqFAwcBAQEBBEB1NOEg
hRnKAUBz8K/Pn93ohbMlf2q1GbNkRjc2v7HXAyrj9tei/AW/7cBSr79x9L9eOqHn
5X4Vu5HwSS9vuE0KAAAAAAAA
```


Требуется заменить перенос строк командой \n на \\n



В итоге получаем подпись в строку (string). В конце строки удалите \n – если осталось.

Криптография

3) Формирование запроса в банк:
https://developers.sber.ru/docs/ru/sberbusinessapi/host/rpp/payments#primer-zaprosa84

Раннее сформированную ЭП требуется прописать в запрос в секции:
"digestSignatures":[{ "base64Encoded": “**вставить Электронную Подпись**”

Далее требуется объединить дайджест РПП и полученный дайджест ЭЦП, весь полученный запрос требуется перевести в строку, убрав перенос строк - **\r\n заменить на пусто**)
Получаем тело запроса:

{ "amount": 1.21, "date": "2023-01-17", "externalId": "ee17342c-1232-4320-aca9-e736e49c8d3f", "operationCode": "01", "payeeAccount": "40702810038363663755", "payeeBankBic": "044525225", "payeeBankCorrAccount": "30101810400000000225", "payeeInn": "7709730320", "payeeKpp": "583501001", "payeeName": "Общество с ограниченной ответственностью **ООО \"РОМАШКА\"**", "payerAccount": "40702810940303423014", "payerBankBic": "044525225", "payerBankCorrAccount": "30101810400000000225", "payerInn": "5051775164", "payerKpp": "770701001", "payerName": "**ООО \"ПАРТНЕР-662\"**", "priority": "5", "purpose": "Оплата заказа №123. НДС нет.", "digestSignatures":[{ "**base64Encoded**":
"MIAGCSqGSIb3DQEHAqCAMIACAQExDjAMBggqhQMHAQECAgUAMIAGCSqGSIb3DQEH\nAQAAMYIELzCCBCsCAQEwggGAMIIBcDELMAkGA1UEBhMCUlUxGDAWBgNVBAgMDzc3\nINCc0L7RgdC60LLQsDEZMBcGA1UEBwwQ0LMuINCc0L7RgdC60LLQsDEnMCUGA1UE\nCQwe0YPQuy4g0JLQsNCy0LjQu9C+0LLQsCwg0LQuIDE5MTswOQYDVQQDDDLQn9CQ\n0J4g0KHQsdC10YDQsdCw0L3QuiAo0KLQtdGB0YIg0JPQntCh0KIgMjAxMiBRKTE7\nMDkGA1UECgwy0J/QkNCeINCh0LHQtdGA0LHQsNC90LogKNCi0LXRgdGCINCT0J7Q\nodCiIDIwMTIgUSkxMDAuBgNVBAsMJ9Cj0LTQvtGB0YLQvtCy0LXRgNGP0Y7RidC4\n0Lkg0YbQtdC90YLRgDEaMBgGCCqFAwOBAwEBEgwwMDc3MDcwODM4OTMxGDAWBgUq\nhQNkARINMTAyNzcwMDEzMjE5NTEhMB8GCSqGSIb3DQEJARYSY2FzYnJmQHNiZXJi\nYW5rLnJ1Agp7BrBxDq0HI9FyMAwGCCqFAwcBAQICBQCgggJEMBgGCSqGSIb3DQEJ\nAzELBgkqhkiG9w0BBwEwHAYJKoZIhvcNAQkFMQ8XDTIzMDExNzE2MDI0OVowLwYJ\nKoZIhvcNAQkEMSIEIDs3pii7ZzqWwRdlWn7omdx2XGwvvWAwUlRptCRzQR7EMIIB\n1wYLKoZIhvcNAQkQAi8xggHGMIIBwjCCAb4wggG6MAoGCCqFAwcBAQICBCBSHZdD\nC5B3X9tN6+9YWRNLzd02OQxOf0+2f3EjNH5MnTCCAYgwggF4pIIBdDCCAXAxCzAJ\nBgNVBAYTAlJVMRgwFgYDVQQIDA83NyDQnNC+0YHQutCy0LAxGTAXBgNVBAcMENCz\nLiDQnNC+0YHQutCy0LAxJzAlBgNVBAkMHtGD0LsuINCS0LDQstC40LvQvtCy0LAs\nINC0LiAxOTE7MDkGA1UEAwwy0J/QkNCeINCh0LHQtdGA0LHQsNC90LogKNCi0LXR\ngdGCINCT0J7QodCiIDIwMTIgUSkxOzA5BgNVBAoMMtCf0JDQniDQodCx0LXRgNCx\n0LDQvdC6ICjQotC10YHRgiDQk9Ce0KHQoiAyMDEyIFEpMTAwLgYDVQQLDCfQo9C0\n0L7RgdGC0L7QstC10YDRj9GO0YnQuNC5INGG0LXQvdGC0YAxGjAYBggqhQMDgQMB\nARIMMDA3NzA3MDgzODkzMRgwFgYFKoUDZAESDTEwMjc3MDAxMzIxOTUxITAfBgkq\nhkiG9w0BCQEWEmNhc2JyZkBzYmVyYmFuay5ydQIKewawcQ6tByPRcjAKBggqhQMH\nAQEBAQRAp6Ko8Sni39LMHpsqN3gUEehVq+pNKlIlhJu3eQzoMWb8yDumkpOkV8Cm\nIyZh02GxlPOkgsMoWIbsEHk+f5dx7QAAAAAAAA==\n", "**certificateUuid**":"167398cb-edf8-401d-aa7d-c6f3b19c724e" }]}

Криптография

4) Отправка подписанного документа РПП в банк (рублёвого платёжного поручения)

Swagger https://edupirfintech.sberbank.ru:9443/fintech/api/swagger-ui.html#!/

Payments : Рублёвые платёжные поручения

Show/Hide | List Operations | Expand Operations

POST /v1/payments — Создание рублёвого платёжного поручения

Parameters

Parameter	Value	Description	Parameter Type	Data Type
Authorization	285ddb81-d1e0-4a12-8bea-06ca07c983b2-1	Access token организации-клиента, полученный через SSO	header	string
payment	{"amount":"301.00","date":"2022-10-07","externalId":"22b33456-91e9-4b10-a093-cddfbf24fc22","operationCode":"01","payeeAccount":"40702810938000035759","payeeBankBic":"044525225","payeeBankCorrAccount":"30101810400000000225","payee	Платёжное поручение	body	Model | Example Value

Parameter content type: application/json


```
],
"externalId": "22a6dd81-103a-4d3a-8e9b-0ba4b527f5f6",
"incomeTypeCode": "2",
"number": "1",
"operationCode": "02",
"payeeAccount": "40802810600000200000",
"payeeBankBic": "044525225",
"payeeBankCorrAccount": "30101810400000000225",
"payeeInn": "7707083893",
"payeeKpp": "222201001",
"payeeName": "Общество с ограниченной ответственностью
"payerAccount": "40802810600000200000"
```

Криптография

Получаем ответ:
Статус **DELIVERED** не конечный, ожидаем обработку документа.

Response Body


```
{
  "number": "53",
  "date": "2022-10-07",
  "digestSignatures": [
    {
      "certificateUuid": "2716bd9a-1583-46fd-a385-8e42168f6bef",
      "base64Encoded": "MIAGCSqGSIb3DQEHAqCAMIACAQExDjAMBggqhQMHAQECAgUAMIAGCSqGSIb3DQEH\nAQAAMYI
    }
  ],
  "bankStatus": "DELIVERED",
  "bankComment": null,
  "externalId": "22b33456-91e9-4b10-a093-cddfbf24fc22",
  "amount": "301.00",
  "operationCode": "01",
  "deliveryKind": null,
  "priority": "5",
  "urgencyCode": "NORMAL",
  "voCode": null,
  "purpose": "В том числе НДС 20 % - 58.83 рублей.",
```


Response Code

```
201
```

Криптография

5) Проверяем статус отправленного документа. Используем метод

GET	/v1/payments/{externalId}/state	Получение статуса рублёвого платёжного поручения

Заполняем параметры и отправляем запрос:

Parameters

Parameter	Value	Description	Parameter Type	Data Type
Authorization	285ddb81-d1e0-4a12-8bea-06ca07c983b2-1	Access token организации-клиента, полученный через SSO	header	string
externalId	22b33456-91e9-4b10-a093-cddfbf24fc22	Внешний UUID платежного поручения	path	string

Получаем успешный ответ – ACCEPTED

Response Body


```
{
  "bankStatus": "ACCEPTED",
  "bankComment": null,
  "channelInfo": null,
  "crucialFieldsHash": "1e876294c0e6a653b8ea6433d67702ba"
}
```


Response Code

```
200
```

Рублёвое Платёжное Поручение подписано ЭП и отправлено в банк.