



**платформа аутентификации и управления
доступом**

Руководство разработчика

Часть 12

Модуль для работы со СКЗИ

Листов 13

Содержание

Перечень сокращений	3
Перечень терминов.....	4
1. Получение данных из ЭП.....	5
1.1. Данные в запросе	5
1.2. Данные в ответе на запрос	5
1.3. Пример выполнения запроса	6
2. Проверка подлинности ЭП	8
2.1. Данные в запросе	8
2.2. Возможные ошибки.....	8
2.3. Пример выполнения запроса	8
3. Создание отсоединенной ЭП.....	11
3.1. Данные в запросе	11
3.2. Данные в ответе на запрос	11
3.3. Пример выполнения запроса	12

Перечень сокращений

ИНН	–	идентификационный номер налогоплательщика
СКЗИ	–	средство криптографической защиты информации
СНИЛС	–	страховой номер индивидуального лицевого счёта
УЦ	–	удостоверяющий центр
ЭП	–	электронная подпись

Перечень терминов

- Удостоверяющий центр – юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ
- Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию

1. Получение данных из ЭП

Имя ресурса: /crypto/api/v1/cryptos/get-signature-info

Метод: POST

HTTP-заголовки:

– Content-Type: application/json

1.1. Данные в запросе

Описание данных в запросе приведено в таблице 1.

Таблица 1 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
ЭП в формате base64	signature	Строка	Да	ЭП в формате base64

1.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 2.

Таблица 2 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Наименование УЦ	publisher	Строка	Да	Наименование УЦ, который выдал сертификат
Серийный номер сертификата	serialNumber	Целое число	Да	Серийный номер сертификата в десятичной системе счисления
ИНН	inn	Строка	Нет	ИНН владельца сертификата
СНИЛС	snils	Строка	Нет	СНИЛС владельца сертификата
Цепочка УЦ сертификата	parentCertificationAuthoritiesInfos	Массив	Нет	Цепочка УЦ сертификата

Параметр	Название параметра	Тип данных	Обязательность	Описание
Наименование УЦ	publisher	Строка	Да	Наименование УЦ, который выдал сертификат, из цепочки сертификатов
Серийный номер УЦ сертификата	serialNumber	Целое число	Да	Серийный номер УЦ сертификата в десятичной системе счисления

1.3. Пример выполнения запроса

Запрос:

```
POST http://{host}/crypto/api/v1/cryptos/get-  
signature-info
```

```
Content-Type: application/json
```

```
{  
  "signature":  
  "MIICzTCCAnqgAwIBAgITIgAAY1bCqnMX+VcBhAAAAABjVjAKBgggq  
hQMHAEQEDAJARMQ8wDQYDVQQDEwZDQS1EQ1MwHhcNMjQwNDI0MTIyN  
jMxWhcNMjUwNzI0MTIzNjMxWjBVMR8wHQYDVQQDHhYEHwQ1BEIEQA  
AgBB8ENQRCBEAEPgQyMRowGAYIKoUDA4EDAQESDDcxNjQyMDQ2ODc  
wNDEWMBQGBSsqFA2QDEgs4NTczMTI1NjIxOTBmMB8GCCqFAwcBAQEBA  
MBMGBYqFAwICJAAGCCqFAwcBAQICA0MABECTKmatZ/NOatknhTi+D  
uIDyD9CSS2tMJRqYZBa2bRdNC7RlNseX+KZX+EvBsbSoSZPFICNNw  
mk1jKlbqzhnYW3o4IBXjCCAVowEwYDVR0lBAwwCgYIKwYBBQUHAWI  
wCwYDVR0PBAQDAgTwMB0GA1UdDgQWBBTm5Eh6L6LFyGpmr7ToPPsm  
0T/yajAfBgNVHSMEGDAWgBQF08gVLikzeC5WFybn3bHf5GCM/DBsB  
gNVHR8EZTBjMGGgX6Bdhi5odHRwOi8vY2EuZGNzLmluZm9zZWUucn  
UvQ2VydeEVucm9sbC9DQS1EQ1MuY3JshitodHRwOi8vY2FkY3MuaXR  
zb2MucnUvQ2VydeEVucm9sbC9DQS1EQ1MuY3JSMIGHBggrBgEFBQcB  
AQR7MHkwTAYIKwYBBQUHMAKGQGH0dHA6Ly9jYS5kY3MuaW5mb3NlY  
y5ydS9DZXJ0RW5yb2xsL2NhLmRjcY5pbmZvc2VjLnJ1X0NBLURDUy  
5jcnQwKQYIKwYBBQUHMAGGHWh0dHA6Ly9jYS5kY3MuaW5mb3NlYy5  
ydS9vY3NwMAoGCCqFAwcBAQMCA0EACmcWTQvTqRoeAyNw9sCg1SZJ  
4TnXspUwDXkzilui3yF7qFYUQ104b0nPnamz7nMizuXlu+Lvg++HO  
OiD7Ta5Vg=="
```

```
}
```

Ответ:

Content-Type: application/json

```
{
  "publisher": "CA-DCS",
  "serialNumber":
758225468794098591223375761336203232212443990,
  "certValidTo": "2025-07-24T12:36:31Z",
  "certOwner": "Петр Петров",
  "inn": "716420468704",
  "snils": "85731256219",
  "parentCertificationAuthoritiesInfos": [
    {
      "publisher": "CA-DCS",
      "serialNumber":
139722319546893040937772127543483520135
    }
  ]
}
```

2. Проверка подлинности ЭП

Имя ресурса: /crypto/api/v1/cryptos/validate-signature

Метод: POST

HTTP-заголовки:

– Content-Type: application/json

2.1. Данные в запросе

Описание данных в запросе приведено в таблице 3.

Таблица 3 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Данные в формате base64	data	Строка	Да	Данные в формате base64, которые были подписаны
ЭП в формате base64	signature	Строка	Да	ЭП в формате base64

2.2. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 4.

Таблица 4 – Данные ошибки выполнения запроса

Параметр	Название параметра	Тип данных	Описание
Тип ошибки	type	Строка	Тип ошибки
Информация об ошибке	message	Строка	Информация об ошибке

2.3. Пример выполнения запроса

Запрос:

POST http://{{host}}/crypto/api/v1/cryptos/validate-signature

Content-Type: application/json

```
{  
  "data": "MjAyMS0wNi0wMlQxNDozOTozMS4xODI3ODRa",  
  "signature":  
    "MIIIIJAYJKoZIhvcNAQcCoIIIFTCCCBCECAQExDDAKBggqhQMHAQEC  
    AjALBgkqhkiG9w0BBwGgggV8MIICczCCAiKgAwIBAgIQN0GIgvU5p  
    ZJK1E494ALqPDAIBgYqhQMCAGMwfzEjMCEGCSqGSIB3DQEJARYUc3  
    VwcG9ydEBjcmlwdG9wcm8ucnUxCzAJBgNVBAYTAlJVMQ8wDQYDVQQQ  
    HEwZNB3Njb3cxZzAVBgNVBAoTDkNSWVBUTy1QUk8gTEwDMSEwHwYD  
    VQQDEzhDU1lQVE8tUFJPIFRlc3QgQ2VudGVyIDlwHhcNMtkwNTI3M  
    DcyNDI2WhcNMjQwNTI2MDczNDA1WjB/MSMwIQYJKoZIhvcNAQkBFh  
    RzdxBwb3J0QGNyeXB0b3Byby5ydTELMakGA1UEBhMCU1UxDzANBgN  
    VBACtBk1vc2NvdzEXMBUGA1UEChMOQ1JZUFRPLVBSTyBMTEMxITAf  
    BgNVBAMTGENSWVBUTy1QUk8gVGVzdCBDZW50ZXIgmjBjMBwGBiqFA  
    wICEzASBgqhQMCAiMBBgqhQMCAh4BA0MABEAUnxYEqKt2UTufYj  
    uRXLy8yaxgLd6w0UF7uaoyi7V63vC9ImBM1KzK8fK4G3KBNYrs9c  
    R/sPD1I28Gxvze8OSo3gwdjALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/  
    BAUwAwEB/zAdBgNVHQ4EFgQUToM+FGnv7F16lStfEf43MhZJVSswE  
    gYJKwYBBAGCNxUBBAUCAwEAATAjBgkrBgEEAYI3FQIEFgQUBGJVkQ  
    sOsc3ReX2auMgfaZ42h/MwCAYGKoUDAgIDA0EAXMwy1be7f6EoKoP  
    uc3PyatD2aI4dXxF1Wnt1EU8Dnxb17j4lWCFSnD7t/E4GQ/H1QV4p  
    GWcCJLsj3eSuWEpaSDCCAwEwggKwoAMCAQICEXIAVDIWXpkZYqjAZ  
    9gAAQBUMhYwCAYGKoUDAgIDMH8xIzAhBgkqhkiG9w0BCQEFHFN1cH  
    BvcnRAY3J5cHRvcHJvLnJlMQswCQYDVQQGEwJSVTEPMA0GA1UEBxM  
    GTW9zY293MRcwFQYDVQQKEw5DU1lQVE8tUFJPIEXMQzEhMB8GA1UE  
    AxMYQ1JZUFRPLVBSTyBUZXN0IENlbnRlcjA5MB4XDTEwMDUyNzE0M  
    TUwNFoXDTIxMDgyNzE0MjUwNFowGzEZMBcGA1UEAwwQVGVzdCBDZX  
    J0aWZpY2F0ZTBmMB8GCCqFAwCBAQEBAQEBMBByqFAwICJAAGCCqFAwC  
    BAQICA0MABEDh/POfTcZ7cv2oGk8rMvEZ0FkTkrsDzT87hsgH39o+  
    sw74FFP2NEUnCw/pKAmiWyzB5EhR6EwInBrTkCYZn2IIo4IBYjCCA  
    V4wDwYDVR0PAQH/BAUDAwfWADAdBgNVHQ4EFgQUlAMG+JT3WDb2i9  
    HY7EImWTO3QdcwHwYDVR0jBBgwFoAUTOM+FGnv7F16lStfEf43MhZ  
    JVSswXAYDVR0fBFUwUzBRoE+gTYZLaHR0cDovL3Rlc3RjYS5jcmlw  
    dG9wcm8ucnUvQ2VydEVucm9sbC9DU1lQVE8tUFJPIJTIwVGVzdCUyM  
    ENlbnRlcjA5YUyMDIoMSkuY3J5SjMIGSBggrBgEFBQcBAQSBnzCBnDBkBg  
    grBgEFBQcwAoZYaHR0cDovL3Rlc3RjYS5jcmlwdG9wcm8ucnUvQ2V  
    ydEVucm9sbC90ZXN0LWNhLTlwMTIwMTRfQ1JZUFRPLVBSTyUyMFRlc3Q1  
    MjBDZW50ZXIlMjAyKDEpLmNydDA0BggrBgEFBQcwAYYoaHR0cDovL  
    3Rlc3RjYS5jcmlwdG9wcm8ucnUvbn2NzcC9vY3NwLnNyZjAIBgYqhQ  
    MCAgMDQqDxkObS1FidWXPEk+8AImU/JJFnjp3PVKSpEZnX7lUSE8S  
    DejqlcRu4sgtiEtGjtQDFkxp6BOCikjm+UwiCnys9MYICbzCCAMsC
```

```
AQEwgZYwFzEjMCEGCSqGSib3DQEJARYUc3VwcG9ydEBjcmlwdG9wc
m8ucnUxCzAJBgNVBAYTA1JVMQ8wDQYDVQQHEwZNb3Njb3cxZzAVBg
NVBAoTDkNSWVBUTy1QUk8gTEExDMSEwHwYDVQQDEzhDU1lQVE8tUFJ
PIFRlc3QgQ2VudGVyIDICEyIAVDIWXpkZyqjAZ9gAAQBUMhYwCgYI
KoUDBwEBAgKgggFxmBgGCSqGSib3DQEJAZELBgkqhkiG9w0BBwEwH
AYJKoZIhvcNAQkFMQ8XDTEyMDYwMjE0Mzk0N1owHQYKKwYBBAGCN1
gCATEPBA1Eb2N1bWVudCBOYW1lMC8GCSqGSib3DQEJBDEiBCCjYbo
QMi4hKC1DIUab8uXI+5ejpYUiPQsjFGXv9JnFZzCB5gYLKoZIhvcN
AQkQAi8xgdYwgdMwgdAwgc0wCgYIKoUDBwEBAgIEIMqxGqzGP2BMA
JkgzkciyPNEH14r4TrnL/WQ/h5lj1DoMIGcMIGEpIGBMH8xIzAhBg
kqhkiG9w0BCQEFHFN1cHBvcnRAY3J5cHRvcHJvLnJlMQswCQYDVQQ
GEwJSVTEPMA0GA1UEBxMGTW9zY293MRcwFQYDVQQKEw5DU1lQVE8t
UFJPIExMQzEhMB8GA1UEAxMYQ1JZUFRRPLVBSTyBUZXN0IENlbmRlc
iAyAhMSAFQyFl6ZGWKowGfYAAEAVDIWMAoGCCqFAwCBAQEBA64r
Z1+1mWLzltavt7knydJyFVdtH5ahlwIshQaJKH2fMWn3dUaLLAzx/
JnPapriGKE4Z3Cprm/vC7QD8NZMsw"
}
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "type": "SignatureNotVerifiedException",
  "message": "signature invalid"
}
```

3. Создание отсоединенной ЭП

Имя ресурса: /crypto/api/v1/cryptos/sign

Метод: POST

HTTP-заголовки:

– Content-Type: application/json

3.1. Данные в запросе

Описание данных в запросе приведено в таблице 5.

Таблица 5 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Данные, которые необходимо подписать	data	Строка	Да	Данные, которые необходимо подписать
Идентификатор сертификата	certificateAlias	Строка	Нет	Идентификатор сертификата, которым необходимо произвести подпись. Если не указывается, то используется сертификат по умолчанию, который определяется сервисом, реализующим СКЗИ

3.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 6.

Таблица 6 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
ЭП в формате base64	signature	Строка	Да	Созданная ЭП в формате base64

3.3. Пример выполнения запроса

Запрос:

```
POST http://{{host}}/crypto/api/v1/cryptos/sign
Content-Type: application/json
```

```
{
  "data": "Я хочу отозвать сертификат" ,
  "certificateAlias": "te-d9427172-de30-442b-98c1-13258007374a"
}
```

Ответ:

```
Content-Type: application/json
```

```
{
  "signature":
  "MIAGCSqGSIB3DQEHAqCAMIACAQExDjAMBggqhQMHAQECAGUAMIAG
  CSqGSIB3DQEHAaCAJIAEMdCv\r\nINGF0L7Rh9GDINC+0YLQvtC30
  LLQsNGC0Ywg0YHQtdGA0YLQuNGE0LjQutCw0YIAAAAAAACggDCC\r
  \nA0wwggL5oAMCAQICEyIAAGSwynqRhse1kZkAAAAAZLAWCgYIKoU
  DBwEBAwIwETEPMA0GA1UEAxMG\r\nQ0EtRENTMB4XDTI0MDQyNzEx
  MjI1OVoxDTI1MDcyNzExMzI1OVowgdMxZDASBgNVBAMTC3Rlc3Qg\r
  \r\nY2VydCAzMjRwGgYJKoZIhvcNAQkBFglpc2ZrQGVtYWlsLnJlMQ
  0wCwYDVQQJEwR0ZXN0MQ0wCwYD\r\nVQQKEwR0ZXN0MQ0wCwYDVQQ
  LEwR0ZXN0MRUwEwYDVQQHhgEHAQ+BEEOgQyBDAXGzAZBgNVBAge
  \r\nEgA3ADcAIAQcBD4EQQQ6BDIEMDELMakGA1UEBhMCU1UxFTATB
  gUqhQNkBBIKNzcXMDU2ODc2MDEY\r\nMBYGBSsqFA2QBEg0xMDQ3Nz
  k3MDE5ODMwMGYwHwYIKoUDBwEBAQEwEwYHKOUDAgIkAAAYIKoUDBwE
  B\r\nAgIDQwAEQLGGm+zMP+uDSOCOJ8dpVm46BsmMUYhSDM4OppaQ
  0Gi/BECOauDAKoIkUHsZkJiu27s9\r\nnrncOifcicn7m47sWk5ajg
  gFeMIIBWjATBgNVHSUEDDAKBggrBgEFBQcDAZALBgNVHQ8EBAMCBP
  Aw\r\nhQYDVR0OBByEFfEzMCPhHW1XaUcTidq6DAoy0+NkPMB8GA1U
```

```
dIwQYMBaAFAXTyBUuKTN4LlYXJs3d\r\nsd/kYIz8MGwGA1UdHwRl
MGMwYaBfoF2GLmh0dHA6Ly9jYS5kY3MuaW5mb3NlYy5ydS9DZXJ0R
W5y\r\nb2xsL0NBLURDUy5jcmyGK2h0dHA6Ly9jYWRjcy5pdHNvYy
5ydS9DZXJ0RW5yb2xsL0NBLURDUy5j\r\nncmwwgYcGCCsGAQUFBwE
BBHsweTBMBggrBgEFBQcwAoZAaHR0cDovL2NhLmRjcy5pbmZvc2Vj
LnJl\r\nL0NlcnRFbnJvbGwvY2EuZGNzLmluZm9zZWZmucnVfQ0EtR
ENTLmNydDApBggrBgEFBQcwAYYdaHR0\r\nncDovL2NhLmRjcy5pbm
Zvc2VjLnJlL29jc3AwCgYIKoUDBwEBAwIDQQBC5xIi0FaNuyQEUEj
kKbAW\r\nL6DzDyJt56lw7DY7J6yUT+zreOqI2qKgo7nN29QAZFCP
H55lm69+btACTqsEzubIAAAxggF5MIIB\r\nndQIBATAoMBExDzANB
gNVBAMTBkNBLURDUwITIGAAZLDKpGGx7WRmQAAAABksDAMBggqhQ
MHAQEC\r\nnAgUAoIHpMBgGCSqGSIB3DQEJAzELBgkqhkiG9w0BBwE
wKQYJKoZIhvcNAQk0MRwwGjAMBggqhQMh\r\nnAQECAGUAoQoGCCqF
AwcBAQEBCMC8GCSqGSIB3DQEJBDEiBCDk2DF6AzNeLXWeYxs//B6XG
mU4Wegb\r\nncDuZ2xnP6prqMjBxBgsqhkiG9w0BCRACLzFiMGAwXj
BcMAoGCCqFAwcBAQICBCBJ819RP63zE8Uc\r\nnK+3a3miYWFftv+q
T6D3PsuZyh80lRjAsMBWkEzARMQ8wDQYDVQQDEwZDQS1EQ1MCEyIA
AGSwynqR\r\nnhse1kZkAAAAAZLAWCgYIKoUDBwEBAQEEOHlp9GKHe
/3FKy5+aGbv+L7YaHAb34JtGTZ1AOSsovzE\r\nnnIQhD72Gl2kH4B
hyM0eUnXlZwU856jRAYInKyZ/rsR0AAAAAAA="
}
```